IBM Communications Server für Linux

# Einstieg

*Version 6.2.2*

GC12-3362-01

IBM Communications Server für Linux

# Einstieg

*Version 6.2.2*

GC12-3362-01

**Hinweis:**
Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die allgemeinen Hinweise unter „Bemerkungen", auf Seite 113 gelesen werden.

**Zweite Ausgabe (Juli 2006)**

Diese Ausgabe bezieht sich auf Communications Server für Linux Version 6.2.2 und, sofern in neuen Ausgaben nichts anderes angegeben ist, auf alle folgenden Releases und Änderungen.

Veröffentlichungen können über den zuständigen IBM Ansprechpartner oder die zuständige IBM Geschäftsstelle bezogen werden.

Am Ende dieser Veröffentlichung befindet sich ein Vordruck für ein Antwortschreiben.

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
*IBM Communication Server for Linux Version 6.2.2, Quick Beginnings,*
IBM Form GC31-6768-01,
herausgegeben von International Business Machines Corporation, USA



Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:
SW TSC Germany
Kst. 2877
Juli 2006

# Inhaltsverzeichnis

# Tabellen

# Abbildungsverzeichnis

# Willkommen bei IBM Communications Server für Linux

Das vorliegende Handbuch gibt eine Einführung in das Softwareprodukt IBM Communications Server für Linux, mit dessen Hilfe ein Linux-Computer Daten mit anderen Knoten in einem SNA-Netz (Systemnetzwerkarchitektur) austauschen kann.

Die Installationsvariante für IBM Communications Server für Linux richtet sich nach der Hardware, auf der das Produkt ausgeführt wird:

**Communications Server für Linux**
Communications Server für Linux, Lizenzprogrammnummer 5724-i33, kann auf folgenden Systemen ausgeführt werden:

- 32-Bit Intel-Workstations mit Linux (i686)
- 64-Bit-AMD64/Intel-EM64T-Workstations mit Linux (x86_64)
- IBM pSeries-Computer mit Linux (ppc64)

**Communications Server für Linux auf System z**
Communications Server für Linux auf System z, Lizenzprogrammnummer 5724-i34, wird auf System-z-Großrechnern mit Linux für System z (s390 oder s390x) ausgeführt.

Das Handbuch *Einstieg in Communications Server für Linux* gibt es in zwei verschiedenen Versionen, jeweils eine für jede der beiden Installationsvarianten. Vergewissern Sie sich, dass Ihnen die richtige Version dieses Handbuchs für Ihre Installation von Communications Server für Linux vorliegt. Das vorliegende Handbuch gilt für Communications Server für Linux auf den Plattformen i686, x86_64 und ppc64.

Communications Server für Linux stellt Basiskomponenten für die verschiedensten Anforderungen an den Netzbetrieb und für ein breites Spektrum von Lösungen bereit. Das Produkt kann für den Austausch von Informationen mit Knoten in SNA-Netzen oder für den Hostzugriff von Telnet-Programmen, die über TCP/IP kommunizieren, eingesetzt werden.

## Benutzung des Handbuchs

In den folgenden Abschnitten ist erläutert, wie das vorliegende Handbuch aufgebaut ist.

### Orientierungshilfe

Dieses Handbuch ist für Administratoren und technisches Personal im Bereich der Netzplanung sowie für alle Personen bestimmt, die sich für Communications Server für das Betriebssystem Linux interessieren.

Tabelle 1 auf Seite xii können Sie entnehmen, wo Sie die gewünschten Informationen zu Communications Server für Linux finden.

*Tabelle 1. Orientierungshilfe für die ersten Schritte*

| Sie möchten ... | Lesen Sie ... |
|---|---|
| sich über Communications Server für Linux informieren | Kapitel 1, „Informationen zu IBM Communications Server für Linux", auf Seite 1 |
| die Verwendung von Communications Server für Linux in Ihrem Netz planen | Kapitel 2, „Netz mit IBM Communications Server für Linux planen", auf Seite 19 |
| Communications Server für Linux auf Linux-Servern installieren | Kapitel 3, „Communications Server für Linux auf Linux-Servern installieren", auf Seite 27 |
| Remote API Clients unter Linux (32-Bit Intel, 64-Bit-Intel/ AMD oder pSeries) installieren | Kapitel 4, „IBM Remote API Clients unter Linux installieren", auf Seite 41 |
| Remote API Clients unter Linux auf System z installieren | Kapitel 5, „IBM Remote API Clients unter Linux für System z installieren", auf Seite 47 |
| Remote API Clients unter AIX installieren | Kapitel 6, „IBM Remote API Clients auf AIX-Systemen installieren", auf Seite 53 |
| Remote API Clients unter Windows installieren | Kapitel 7, „Installation von Remote API Client unter Windows vorbereiten und ausführen", auf Seite 57 |
| Communications Server für Linux konfigurieren | Kapitel 8, „Communications Server für Linux konfigurieren und verwenden", auf Seite 71 |
| Hinweise zur Dokumentation für Communications Server für Linux und zu anderen Publikationen, einschließlich Onlineinformationen, erhalten | Kapitel 9, „Informationsquellen für Communications Server für Linux und SNA", auf Seite 111 |
| die Bemerkungen und Informationen zu Marken lesen | „Bemerkungen", auf Seite 113 |

## Typografische Konventionen

Tabelle 2 gibt einen Überblick über die in diesem Handbuch verwendeten typografischen Darstellungen.

*Tabelle 2. Typografische Konventionen*

| Element | Typografiebeispiel |
|---|---|
| Hervorgehobene Wörter | **Sichern Sie Dateien vor dem Löschen** |
| Handbuchtitel | *Communications Server für Linux Verwaltungshandbuch* |
| Datei- oder Pfadname | **/usr/spool/uucp/myfile.bkp** |
| Programm oder Anwendung | **snaadmin** |
| Benutzereingabe | **0p1** |
| Computerausgabe | **CLOSE** |

## Verwendete Abkürzungen

Im vorliegenden Handbuch werden die folgenden Abkürzungen verwendet:

| | |
|---|---|
| AIX | Advanced Interactive Executive |
| API | Application Programming Interface (Anwendungsprogrammierschnittstelle) |
| APPC | Advanced Program-to-Program Communication |
| APPN | Advanced Peer-to-Peer Networking |
| COS | Class of Service (Serviceklasse) |
| CPI-C | Common Programming Interface for Communications |
| CSV | Common Service Verb |
| DDDLU | Dynamic Definition of Dependent LUs (dynamisches Definieren unabhängiger LUs) |
| DES | Data Encryption Standard (Standard für Datenverschlüsselung) |
| DLC | Data Link Control (Datenübertragungssteuerung) |
| DLUR | Dependent LU Requester |
| DLUS | Dependent LU Server |
| FTP | File Transfer Protocol |
| HPR | High-Performance Routing |
| IETF | Internet Engineering Task Force |
| ISO | International Organization for Standards |
| ISR | Intermediate Session Routing (Weitervermittlung einer Sitzungsroute) |
| LAN | Local Area Network (lokales Netz) |
| LDAP | Lightweight Directory Access Protocol |
| LEN | Low-Entry Networking |
| LLC2 | Logical Link Control 2 (Protokoll zur Steuerung logischer Verbindungen) |
| LU | Logical Unit (logische Einheit) |
| LUA | Konventionelle LU-Anwendungsprogrammierschnittstelle |
| MDS-NMVT | Multiple Domain Support - Network Management Vector Transport |
| MPC | MultiPath Channel |
| MS | Management Services (Verwaltungsdienste) |
| NMVT | Network Management Vector Transport |
| NOF | Node Operator Facility |
| OSI | Open Systems Interconnection |
| PU | Physical Unit (physische Einheit) |
| RFC | Request For Comments |
| RLE | Run-Length Encoding (Verschlüsselung für Ausführungshäufigkeit) |
| SAA | Systems Application Architecture (Systemanwendungsarchitektur) |
| SAP | Service Access Point |
| SNA | Systems Network Architecture (Systemnetzwerkarchitektur) |
| SSL | Secure Sockets Layer |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| TN | Telnet |
| TP | Transaction Program (Transaktionsprogramm) |
| VT | Virtual Terminal (Virtuelles Terminal) |
| WAN | Wide Area Network (Weitverkehrsnetz) |
| ZNK | Zweignetzknoten |

# Neuerungen

Communications Server für Linux Version 6.2.2 ersetzt Communications Server für Linux Version 6.2 und Communications Server für Linux Version 6.2.1.

Folgende Releases dieses Produkts werden noch unterstützt:

- Communications Server für Linux Version 6.2
- Communications Server für Linux Version 6.2.1

Folgende Releases des Produkts werden nicht mehr unterstützt:

- Communications Server für Linux Version 6.0.1, verfügbar als PRPQ 5799-RQA.

## Neue Funktionen

In diesem Release wurde Communications Server für Linux um folgende Funktionen erweitert:

- Die Client/Server-Unterstützung deckt jetzt ein breiteres Spektrum von Server- und Client-Computern ab.
  - Folgende Server werden unterstützt:
    - 32-Bit Intel-Workstations mit Linux (i686)
    - 64-Bit-AMD64/Intel-EM64T-Workstations mit Linux (x86_64)
    - IBM pSeries-Computer mit Linux (ppc64)
  - Unterstützte Clients sind i686-, x86_64-, ppc64-, s390- oder s390x-Systeme, AIX-Workstations oder PCs mit einer 32-Bit-Version von Microsoft Windows (Microsoft Windows 2000, 2003 oder XP) bzw. einer x64-Version von Microsoft Windows (Microsoft Windows Server 2003 x64 Edition oder Microsoft Windows XP Professional x64 Edition). Diese Clients können über TCP/IP mit dem CS-Linux-Server (oder einem CS/AIX-Server) und mit HTTPS über einen WebSphere-Server kommunizieren.
    - Linux-Clients, Clients mit Linux auf System z und AIX-Clients unterstützen alle API-Bibliotheken, die auf Linux-Servern oder Servern mit Linux auf System z verfügbar sind. (Die im früheren Produkt CS/AIX Version 4.2 enthaltenen APIs werden in dieser Version nicht unterstützt.)
    - Windows-Clients (mit einer 32-Bit- oder x64-Version von Microsoft Windows) unterstützen die APIs APPC, CPI-C, CSV, LUA (einschließlich LUA RUI und LUA SLI) und NOF.
    - Die Client-Unterstützung für die API NOF erstreckt sich (für alle Client-Typen) nur auf die Abfragefunktionen. Aufrufe zum Definieren, Löschen, Starten oder Stoppen von Ressourcen sind nicht verfügbar.
    - Windows-Clients können in der WTS-Umgebung (Windows Terminal Server) ausgeführt werden, in der mehrere Benutzer einen Client gemeinsam nutzen können, deren Anwendungen jedoch unabhängig voneinander ausgeführt werden.
- Die Linux-Distribution SLES10 wird jetzt (für Server und Clients) unterstützt.
- Communications Server für Linux unterstützt jetzt mit WAN-Adaptern auf Linux-Servern SDLC- und X.25-Konnektivität (QLLC). Der Adapteranbieter muss hierfür Einheitentreibercode und DLC-Code bereitstellen. IBM stellt weder diese Adapter noch die Einheitentreiber zur Verfügung. Details zu Anbietern geeigneter WAN-Adapter finden Sie auf der Unterstützungswebseite zu Communications Server für Linux.

- In TN Server und TN Redirector können Sie jetzt eine bestimmte lokale Adresse angeben, an der der TN-Durchgriffsdienst auf den Empfang von Client-Verbindungen warten soll. Dieses Feature ist optional. Sie können den Dienst so konfigurieren, dass er die Verbindung von TN3270-Clients zu einer beliebigen lokalen Adresse unterstützt, oder den Dienst auf eine angegebene Adresse beschränken.

## Nicht mehr unterstützte Funktionen

Unter Red Hat Advanced Server 2.1 wird der Client- und Servercode nicht mehr unterstützt.

# Kapitel 1. Informationen zu IBM Communications Server für Linux

Dieses Kapitel enthält Informationen zu den CS-Linux-Programmpaketen. Darüber hinaus werden die Funktionen, Features und Vorteile von Communications Server für Linux beschrieben.

## IBM Communications Server für Linux - Features und Programmpakete

Communications Server für Linux ist DFV-Software, die unter dem Betriebssystem Linux ausgeführt wird. Zum Lieferumfang der Software gehören die in den Abschnitten „IBM Communications Server für Linux" und „Erweiterte Features für den Netzbetrieb" auf Seite 6 beschriebenen Features.

### IBM Communications Server für Linux

IBM Communications Server für Linux verbindet Anwendungen in SNA- und TCP/IP-Netzen miteinander. Dieses Softwareprodukt macht aus einer Workstation mit dem Betriebssystem Linux einen SNA-Knoten, indem es für die Workstation SNA-Ressourcen und -Protokolle bereitstellt. Die so ausgestattete Workstation kann mit anderen Workstations und Hosts in einem SNA-Netz kommunizieren. Darüber hinaus bietet die Software TCP/IP-Funktionen, so dass Sie IBM Communications Server für Linux innerhalb Ihres TCP/IP-Netzes oder auch an der Nahtstelle zwischen einem TCP/IP- und einem SNA-Netz verwenden können.

Communications Server für Linux stellt die folgenden Dienste bereit:

**Netzunterstützung**

Communications Server für Linux unterstützt Unterbereichsnetze und Peer-zu-Peer-Netze:

**SNA-Unterbereichsnetze**

Diese Netze (auch bekannt als hostvermittelte Netze) sind hierarchisch aufgebaut, wobei die Steuerung der Kommunikation zwischen den Computern, die Netzverwaltung und die Bereitstellung von Verarbeitungsdiensten sowie die Speicherung von großen Datenmengen von einem oder mehreren Hosts übernommen werden. Alle anderen Knoten im Netz sind von der Steuerung durch einen Host abhängig.

Linux-Computer können als hostabhängige Knoten konfiguriert werden und so Teil eines Unterbereichsnetzes sein.

**Peer-zu-Peer-Netze**

In Umgebungen für verteilte Verarbeitung unterstützt Communications Server für Linux APPN-Netze. In diesen Peer-zu-Peer-Netzen nehmen Linux-Computer ihre Verarbeitungsfunktion wahr und kommunizieren direkt als Peers miteinander. Peer-zu-Peer-Netze nutzen in vollem Umfang die Fähigkeiten des Linux-Computers, der in zunehmendem Maße kostspielige Hosts ersetzt.

Ein APPN-Netz besteht aus Peer-Knoten der folgenden Arten:

- APPN-Netzknoten (zuständig für Übertragungssteuerung, dynamische Routenberechnung und Auswahldienste sowie Netzverwaltungsdienste)

- APPN-Endknoten (verwendet APPN-Netzknotendienste für die Kommunikation mit Peer-Knoten)
- LEN-Knoten (kommuniziert direkt mit Nachbarknoten oder als Scheinnachbarknoten konfigurierten Knoten)

**Anmerkung:** Hosts können als Peer-Knoten in einem APPN-Netz fungieren, wenn für die Kommunikation mit Linux-Computern und anderen Hosts im Netz eine unabhängige LU 6.2 verwendet wird.

**Bereitstellung von Unterbereichsfunktionen in einem APPN-Netz**
Die DLUR-Funktion (Dependent LU Requester) ermöglicht den Transport des Datenverkehrs zwischen Hosts und hostabhängigen Knoten über ein APPN-Netz.

**Optionen für Datenübertragungssteuerung**
Auf Verbindungsebene bietet Communications Server für Linux verschiedene Konnektivitätsoptionen, die helfen sollen, Ihre Anforderungen an Größe, Geschwindigkeit, Sicherheit und Kosten des Netzes zu erfüllen. (Eine ausführliche Liste der unterstützten Verbindungsarten finden Sie im Abschnitt „Installationsvoraussetzungen" auf Seite 22.) CS Linux unterstützt wie folgt Datenübertragungsverbindungen für verschiedene Netztypen:

**Lokale Netze**
Für LAN-Konnektivität können Sie die entsprechenden Verbindungen für die Kommunikation über Token-Ring-, Standard-Ethernet- und 802.3-Ethernet-Protokolle installieren.

**Weitverkehrsnetze**
Communications Server für Linux unterstützt SDLC- und X.25-Konnektivität (QLLC). Diese Unterstützung ist von der OEM-Adapterunterstützung auf der jeweiligen Plattform abhängig.

**Lokaler Anschluss**
Für den lokalen Anschluss unterstützt Communications Server für Linux MPC-Konnektivität (Multipath Channel). (Dies gilt nur für Communications Server für Linux auf System z.)

**IP-Integration**
Falls Ihr zentrales Unternehmensnetz auf IP basiert, können Sie das Netz mit dem Feature Enterprise Extender (HPR/IP) von Communications Server für Linux in die SNA integrieren, so dass Ihre SNA-Anwendungen über das IP-Netz kommunizieren können.

**LU-Unterstützung**
Logische Einheiten (LUs) sind anwendungsspezifische Netzressourcen, die auf jedem Knoten eines SNA-Netzes vorhanden sind. Jede LU fungiert als Schnittstelle, mit der Anwendungen auf Verbindungen zugreifen, um über das Netz mit Partneranwendungen auf anderen Knoten zu kommunizieren.

Communications Server für Linux unterstützt verschiedene LU-Typen für verschiedene Anwendungsklassen.

- In einem Unterbereichsnetz unterstützt Communications Server für Linux abhängige LUs der folgenden Typen:
  - LU 0
  - LU 1
  - LU 2

– LU 3
– LU 6.2

LU 0 unterstützt die einfache Kommunikation zwischen Programmen und wird normalerweise für Transaktionen in den Geschäftsstellen des Einzelhandels und Bankenwesens verwendet. LU 2 unterstützt Terminalemulationsanwendungen, mit denen der Linux-Computer ein IBM Terminal der 3270-Produktfamilie emulieren kann. Über die anderen LU-Typen können Anwendungen an der verteilten Verarbeitung teilnehmen oder mit verschiedenen Druckern oder interaktiven Workstations kommunizieren.

Communications Server für Linux unterstützt Hostsysteme, die DDDLU (Dynamic Definition of Dependent LUs, dynamische Definition abhängiger LUs) verwenden. Dies ist ein Hostfeature, mit dem abhängige LUs des SNA-Systems zur Hostkonfiguration hinzugefügt werden können, wenn die DFV-Verbindung vom SNA-System zum Host hergestellt ist. Bei Verwendung von DDDLU müssen LUs nicht mehr statisch auf dem Host konfiguriert werden. (Abhängige LUs auf dem CS-Linux-Knoten müssen dennoch definiert werden.) Auf diese Weise wird der Aufwand für die Erstkonfiguration auf dem Host verringert und eine spätere Erweiterung vereinfacht.

Communications Server für Linux kann sowohl mit DDDLU-fähigen als auch mit nicht DDDLU-fähigen Hosts kommunizieren, ohne dass die Konfiguration geändert werden muss. Wenn die DFV-Verbindung vom CS-Linux-Knoten zum Host hergestellt ist, informiert ein DDDLU-fähiger Host den Knoten, damit dieser DDDLU unterstützt. Der Knoten sendet daraufhin die erforderlichen Informationen, um die abhängigen LUs zu definieren, die die Verbindung verwenden. Ist der Host nicht DDDLU-fähig, sendet Communications Server für Linux diese Informationen nicht und geht davon aus, dass die LUs bereits statisch auf dem Host definiert wurden.

- Unabhängige LUs 6.2 unterstützen den unabhängigen Datenverkehr in APPN-Netzen. Sie unterstützen die autonome Kommunikation und Netzverwaltung sowie die verteilte Verarbeitung.

  Die DLUR-Funktion von Communications Server für Linux gestattet darüber hinaus den Transport des Datenverkehrs von abhängigen LUs über ein APPN-Netz.
- Mit der Primary-RUI-Unterstützung kann eine CS-Linux-Anwendung untergeordnete abhängige LU-Einheiten, die mit einem LAN/WAN verbunden sind, wie ein Großrechner verwalten. Diese Funktion zieht einige Konnektivitätseinschränkungen nach sich, ermöglicht Anwendungen jedoch, Daten zwischen abhängigen LU-Einheiten ohne eine komplette Großrechneranwendung zu übergeben.

**Sitzungsunterstützung**

Eine Sitzung ist ein temporärer logischer Kanal zwischen Partner-LUs. Normalerweise kommunizieren Partneranwendungen, die den LUs zugeordnet sind, über die Sitzung. Communications Server für Linux kann Tausende von Sitzungen unterstützen. Communications Server für Linux bietet auch Unterstützung für U-förmige Sitzungen (die als „Transparenz zwischen lokalem und fernen Sitzungspartner" bezeichnet wird), bei denen sich die primären und sekundären LUs auf demselben Linux-Computer befinden. Dadurch können Sie ein Paar aus Quellen- und Zieltransaktionsprogramm auf einem Computer entwickeln und testen, ohne dass es einer Verbindung bedarf.

Die Daten, die während einer Sitzung zwischen zwei Partner-LUs ausgetauscht werden, können komprimiert werden, um die erforderliche Bandbreite zu verringern.

- Für LUs des Typs 6.2 können Sie in Communications Server für Linux die Anwendung der Komprimierung in der Konfiguration des von der Sitzung verwendeten Modus angeben. Sie können verschiedene Komprimierungsalgorithmen angeben, die jeweils einen anderen Grad der Komprimierung ermöglichen (RLE, LZ9 oder LZ10). Unterschiedliche Komprimierungsstufen können Sie auch für die verschiedenen Richtungen des Datenflusses in der Sitzung angeben. Es ist möglich, die in eine Richtung fließenden Daten zu komprimieren und die in die andere Richtung fließenden Daten nicht.
- Für LUs der Typen 0-3 können Sie in Communications Server für Linux die Anwendung der Komprimierung in der Konfiguration der von der Sitzung verwendeten Verbindungsstation oder PU angeben. Für die Komprimierung ankommender Daten wird RLE und für die Komprimierung abgehender Daten LZ9 verwendet.

**API-Unterstützung**

Communications Server für Linux bietet Anwendungsprogrammierschnittstellen (APIs) für die Entwicklung von Anwendungen für bestimmte LU-Typen, für verteilte Verarbeitung, für Netzverwaltung und für die Verwaltung von Communications Server für Linux selbst. Communications Server für Linux stellt ein Reihe von APIs bereit, die mit den APIs der CS-Systemfamilie für andere Betriebssysteme kompatibel sind.

Eine API ist eine Schnittstelle, über die ein Transaktionsprogramm (TP) mit der unterstützenden LU kommunizieren kann. Die Schnittstelle besteht aus einer Bibliothek von Verben (die auch als Funktionen, Aufrufe oder Unterroutinen bezeichnet werden). Aus diesen Verben wählt das TP diejenigen aus, mit denen die Anforderung einer Aktion (z. B. SEND_DATA) an die zugeordnete LU weitergeleitet werden kann. Die LU wiederum verarbeitet die Verben und gemäß dem entsprechenden Protokoll einen Datenstrom, fügt einen Header mit der Zieladresse an und sendet die Daten über die Verbindung an Partner-LUs.

Common Programming Interface for Communications (CPI-C) ist aufgrund ihrer Übertragbarkeit eine der leistungsfähigsten APIs. CPI-C wurde zur Unterstützung abgängiger und unabhängiger LUs 6.2 eingeführt und wird der SAA-Forderung nach Vereinigung verschiedener Plattformen und Betriebssysteme gerecht. CPI-C verwendet Syntaxregeln, die allen Systemen gemeinsam sind, und ist dadurch zum Standard geworden.

Neben der Standard-API der Programmiersprache C, CPI-C, stellt Communications Server für Linux auch eine CPI-C-Anwendungsprogrammierschnittstelle für Java-Anwendungen bereit. Weitere Informationen hierzu finden Sie im *Communications Server for Linux CPI-C Programmer's Guide*. Sofern nichts anderes angegeben ist, beziehen sich alle Hinweise auf CPI-C in den Handbüchern zu Communications Server für Linux auch auf CPI-C für Java.

Weitere für Communications Server für Linux verfügbare APIs sind:

- API APPC für Peer-zu-Peer-Kommunikation zwischen Anwendungsprogrammen unter Verwendung von LUs 6.2. Die API kann optional im nicht gesperrten Modus verwendet werden. Wenn ein TP nicht gesperrte Verben verwendet, kann die API die Steuerung an das TP zurückgeben, bevor die angeforderte Aktion abgeschlossen ist. Das TP wird später informiert, wenn die Aktion beendet ist.

- API LUA für die Kommunikation mit Hostanwendungen.
- API CSV (Common Service Verb) für Dienstprogrammfunktionen wie die Steuerung der Zeichenumsetzung und des Anwendungs-Trace.

Im Lieferumfang von Communications Server für Linux sind außerdem die folgenden privaten Programmierschnittstellen enthalten:

- API MS (Management Services) für Netznachrichtenübertragungsdienste
- API NOF (Node Operator Facility) für Anwendungen zum Konfigurieren und Verwalten der CS-Linux-Ressourcen.

Weitere Informationen zu APIs finden Sie im Programmierungshandbuch zur jeweiligen API.

**Client/Server-Unterstützung**

Computer, auf denen Communications Server für Linux ausgeführt wird, können für die Kommunikation mit Client/Server-Protokollen konfiguriert werden. Wenn in einem Netz Client/Server-Protokolle verwendet werden, bilden alle Computer, die für die Kommunikation in diesem Netz Client/Server-Protokolle nutzen, eine Domäne.

Computer mit Communications Server für Linux können in einer Client/Server-Konfiguration die folgenden Aufgabenbereiche übernehmen:

- Ein Server enthält einen SNA-Knoten und dessen Konnektivitätskomponenten. Der Server stellt SNA-Konnektivität für Anwendungen auf dem lokalen System oder auf anderen Computern in der CS-Linux-Domäne bereit. Server müssen Linux-Systeme sein.
- Ein Remote API Client enthält keine SNA-Knotenkomponenten, sondern greift über einen Server auf diese zu. Ein Client kann bei Bedarf gleichzeitig auf mehrere Server zugreifen und Anwendungen parallel ausführen. Clients können AIX, Linux oder Windows ausführen. (Ein Linux-Computer kann der Server oder der Client sein, jedoch nicht beides. Sie können Server und Client nicht auf demselben Computer installieren.)

Server und Clients kommunizieren mit TCP/IP innerhalb der CS-Linux-Domäne. Alternativ können sie mit HTTPS über einen WebSphere-Server kommunizieren, der die Client-Verbindungen mit Sicherheitszertifikaten authentifiziert. Normalerweise wird HTTPS verwendet, wenn die Clients ihre Verbindung über ein öffentliches Netz herstellen.

In einer Domäne mit mehreren CS-Linux-Servern befindet sich auf einem Server die Master-Kopie der Konfigurationsdatei für die CS-Linux-Domäne. Dieser Server ist der Hauptserver. Die anderen Server in der Domäne können als Ausweichserver definiert werden oder Peer-Server bleiben. Die Domänenkonfigurationsdatei wird auf die Ausweichserver kopiert, wenn diese gestartet werden oder wenn sich die Master-Kopie ändert, so dass sich auf allen Ausweichservern eine Kopie mit den aktuellen Informationen befindet. Ein Peer-Server erhält bei Bedarf Domänenkonfigurationsdaten vom Hauptserver, kann jedoch nicht als Ausweichserver agieren.

Fällt der Hauptserver aus, übernimmt der erste Ausweichserver in der Liste der für die Domäne definierten Server die Aufgaben des Hauptservers. Die Domänenkonfigurationsdatei auf diesem Server wird nun als Master-Kopie verwendet und, wenn notwendig, auf andere Server kopiert. Wird der Hauptserver erneut gestartet, empfängt er von dem Ausweichserver, der gegenwärtig als Hauptserver agiert, eine Kopie der Domänenkonfiguration und übernimmt dann wieder seine Rolle als Hauptserver.

**Unterstützung für verteilte Anwendungen**

In einem Client/Server-System mit Communications Server für Linux kooperieren die auf Remote API Clients ausgeführten Anwendungen für die Ausführung einer Task mit Konnektivitätsressourcen auf Servern. Anwendungen, die auf anderen Computern (ohne Communications Server für Linux) ausgeführt werden, können für die verteilte Verarbeitung ebenfalls mit Anwendungen auf CS-Linux-Computern kooperieren.

Communications Server für Linux unterstützt verteilte Anwendungen mittels APPC (auch bekannt als LU 6.2).

## Erweiterte Features für den Netzbetrieb

Zum Basisprodukt Communications Server für Linux gehören eine Reihe von Features, die das Produkt durch eine erweiterte Funktionalität für den Netzbetrieb ergänzen. Zu diesen Features gehören unter anderem:

- SNA Gateway verbindet LANs mit SNA-Unterbereichsnetzen.
- Durch die Unterstützung für primäre LUs können untergeordnete abhängige LU-Einheiten wie von einer Großrechneranwendung (Hostanwendung) gesteuert werden.
- Branch Extender vereinfacht große APPN-Netze durch Auslagerung von Ressourcen an verschiedene Standorte (z. B. an unterschiedliche Zweigstellen einer großen Organisation). Dadurch wird die Anzahl der zu speichernden Topologiedaten reduziert, die Möglichkeit der effizienten Lokalisierung von Ressourcen jedoch nicht eingeschränkt.
- APPC Application Suite stellt ausgewählte Anwendungen für APPN-Netze bereit.
- Enterprise Extender (EE, auch bekannt als HPR/IP) ermöglicht den Transport von SNA-Datenverkehr in unveränderter Form über IP-Netze.
- TN Server bietet über SNA Hostzugriff auf TN3270- und TN3270E-Clients, die unter der Bezeichnung TN3270-Clients zusammengefasst werden.
- TN Redirector bietet TCP/IP-Hostdurchgriff auf TN3270-, TN3270E-, TN5250- und VT-Clients, die unter der Bezeichnung Telnet-Clients zusammengefasst werden.

## SNA Gateway

Ein Gateway ist eine benutzertransparente Einheit zur Verbindung unterschiedlicher Netze oder Datenverarbeitungssysteme, die die beiden Systeme, die sie verbindet, unterstützt. Endbenutzer nehmen sich gegenseitig als Benutzer desselben Netzes wahr.

Mit Hilfe von SNA Gateway kann ein CS-Linux-Computer als Gateway fungieren, der mehrere untergeordnete Computer in einem SNA-Netz mit einer oder mehreren Host-PUs verbindet (siehe Abb. 1). Zur Vereinfachung der Hostkonnektivität und zur Vermeidung einer übermäßigen Anzahl von Verbindungen wird SNA Gateway als PU-Konzentrator verwendet, d. h., mehrere Computer werden wie eine (scheinbar auf dem SNA-Gateway-Knoten befindliche) PU behandelt, die über eine physische Verbindung mit dem Host kommuniziert.

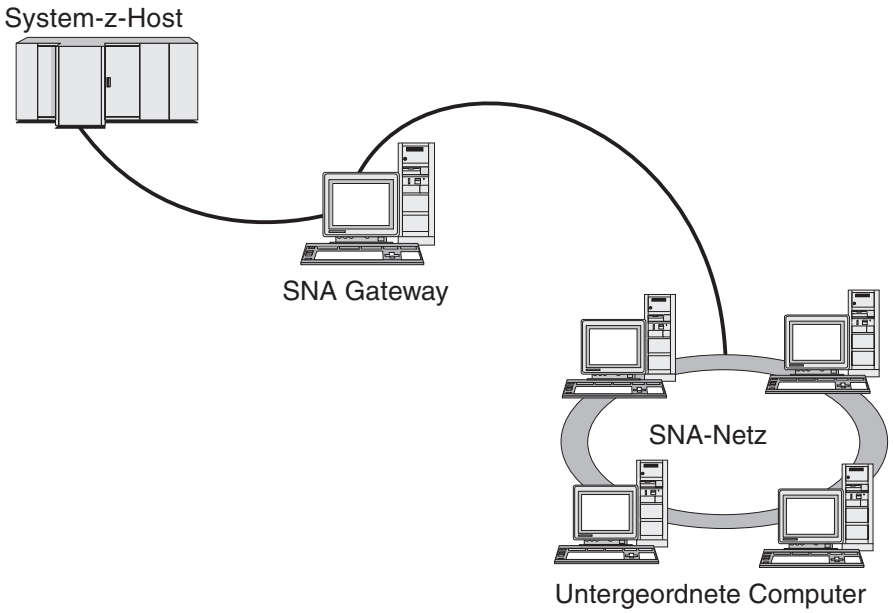


*Abbildung 1. Verbindung mehrerer untergeordneter Linux-Computer mit einem Host über SNA Gateway*

## Unterstützung für primäre LU

Durch die Unterstützung für primäre LU kann eine Linux-Anwendung untergeordnete abhängige LU-Einheiten steuern, als wäre sie eine Großrechneranwendung (Hostanwendung).

LUA-Anwendungen stellen in der Regel als sekundäre LUs eine Verbindung zu Großrechnern (Hosts) her, so dass die Hostanwendung die Definition für die Sitzungen steuert und für das Senden des BIND zu Beginn einer Sitzung verantwortlich ist. Communications Server für Linux kann mit Hilfe der Schnittstelle Primary RUI über ein LAN für untergeordnete abhängige SNA-Einheiten die Aufgabe einer primären LU übernehmen. Über diese Schnittstelle kann eine Anwendung ohne einen Großrechner (Host) eine Verbindung für Sitzungen mit untergeordneten abhängigen LUs herstellen.

Für die Verwendung von Anwendungen für primäre LU muss der Knoten mit untergeordneten LUs (oder einer Schablone für untergeordnete PU) konfiguriert sein (Host-LU-Name #PRIRUI#). Damit wird dem Server signalisiert, dass die Anwendungen, die Primary RUI verwenden, diese PUs und die ihnen zugeordneten LU-Ressourcen steuern. Die PUs können nur an LAN-Ports verwendet werden. Im *Communications Server for Linux LUA Programmer's Guide* erfahren Sie, wie Sie Anwendungen für die Verwendung von Primary RUI programmieren können.

## Branch Extender

Netzknoten in einem APPN-Netz müssen Topologiedaten (zur Position anderer Knoten im Netz und den zwischen diesen bestehenden DFV-Verbindungen) verwalten und diese Daten im Netz weiterleiten, sobald sich die Topologie ändert. Wächst das Netz, nehmen auch die Anzahl der gespeicherten Daten und der topologiebezogene Datenaustausch im Netz zu. Dies erschwert die Verwaltung der Daten.

Diese Probleme können umgangen werden, indem das Netz in Teilnetze gegliedert wird. Jeder Endknoten muss dann nur die Topologiedaten der Knoten in seinem eigenen Teilnetz verwalten. Der Versuch, Ressourcen in anderen Teilnetzen zu lokalisieren, führt dann allerdings zu einem vermehrten Datenaustausch im Netz.

Das in Abb. 2 auf Seite 9 dargestellte APPN-Feature Branch Extender bietet eine Lösung für diese Probleme an.

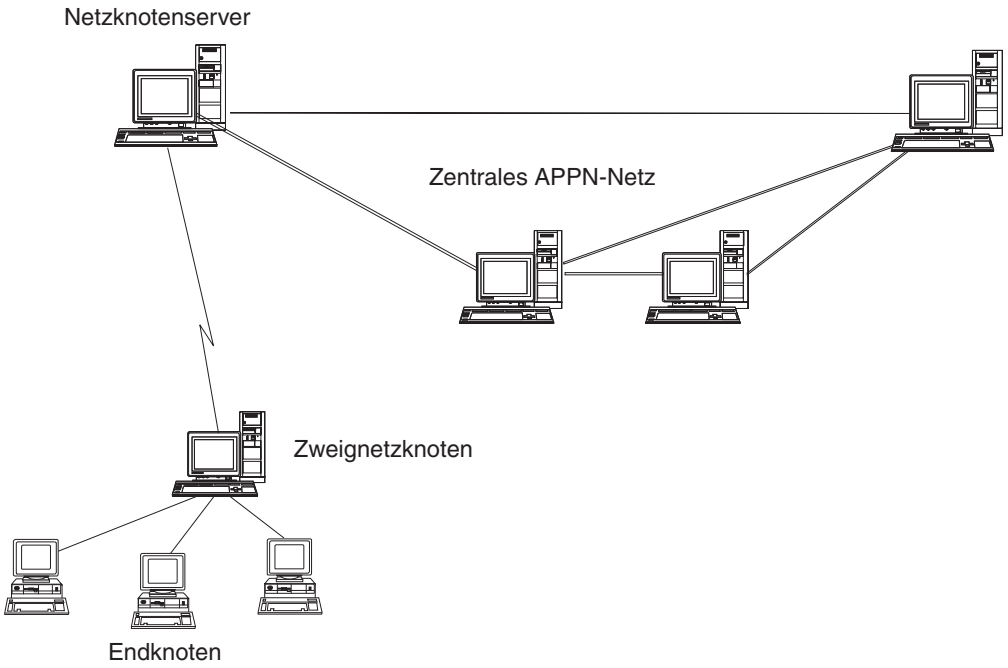


*Abbildung 2. Branch Extender*

Wie der Name bereits nahe legt, wurde Branch Extender für Netze entwickelt, die in bestimmte Bereiche, z. B. die verschiedenen Zweigstellen einer großen Organisation, unterteilt werden können. Branch Extender gliedert Zweignetze aus dem zentralen APPN-Netz (z. B. dem Netz am Hauptsitz der Organisation) aus.

Jedes Zweignetz enthält einen neuen Knotentyp, den Zweignetzknoten, der mit einem Netzknoten im zentralen APPN-Netz verbunden ist. Der Zweignetzknoten vereint in sich die Funktionen eines APPN-Netzknotens und eines APPN-Endknotens.

- Aus Sicht des zentralen Netzes ist der Zweignetzknoten ein Endknoten, der mit dem zugehörigen Netzknotenserver im zentralen Netz verbunden ist.
  - Die Knoten im zentralen Netz haben keine Kenntnis von den Knoten innerhalb des Zweignetzes, so dass weniger Topologiedaten gespeichert werden müssen.
  - Weil der Zweignetzknoten als Endknoten erscheint, empfängt er keine Topologiedaten vom zentralen Netz. (Topologiedaten werden nur zwischen Netzknoten übertragen.)
  - Der Zweignetzknoten registriert alle Ressourcen im Zweignetz auf seinem Netzknotenserver, als würden sie sich auf dem Zweignetzknoten selbst befinden. Die Knoten im zentralen Netz können somit Ressourcen im Zweignetz suchen, ohne Kenntnis davon zu haben, dass zu diesem Zweignetz verschiedene Knoten gehören.
- Aus Sicht des Zweignetzes ist der Zweignetzknoten ein Netzknoten, der für Endknoten im Zweignetz die Funktion eines Netzknotenservers übernimmt. Für alle Knoten im Zweignetz stellt sich ihre Verbindung zum übrigen Netz so dar, als wäre sie eine Verbindung über ihren Netzknotenserver, so wie es bei Standardnetzknotenservern der Fall ist.

## APPC Application Suite

Die APPC Application Suite ist eine Gruppe von Anwendungen zum Darstellen der Möglichkeiten der verteilten Verarbeitung von APPN-Netzen. Diese Anwendungen können die Konfigurationsprüfung und Fehlerbestimmung unterstützen. Mit der APPC Application Suite können Sie Unterstützung für häufig in Netzen ausgeführte Operationen, z. B. die Dateiübertragung, bereitstellen.

Zur APPC Application Suite gehören die folgenden Anwendungen:

- **ACOPY** (APPC COPY)
- **AFTP** (APPC File Transfer Protocol)
- **ANAME** (APPC Name Server)
- **APING** (APPC Ping)
- **AREXEC** (APPC Remote EXECution)
- **ATELL** (APPC TELL)

Auf diese Anwendungen kann ein Server oder ein Linux- bzw. ein Windows-Client zugreifen.

## Enterprise Extender

Enterprise Extender (auch bekannt als HPR/IP) stellt Mechanismen für die Integration von SNA-Anwendungen in ein IP-Netz bereit.

SNA-Anwendungen sind so konzipiert, dass sie für die Kommunikation mit anderen SNA-Anwendungen über SNA-Netze SNA-Protokolle verwenden. Werden SNA-Anwendungen in einem TCP/IP-Netz installiert, gewährleistet Enterprise Extender, dass die Anwendungen weiterhin kommunizieren können. Die Funktion Enterprise Extender stellt einen Mechanismus für den Transport von SNA-Protokollen über das IP-Netz bereit. Insbesondere stellt Enterprise Extender APPN-HPR-Funktionalität (High-Performance Routing) zur Verfügung, so dass die Anwendungen die Vorzüge der APPN- und der IP-Konnektivität nutzen können.

Enterprise Extender wird in Communications Server für Linux einfach als DFV-Verbindung implementiert. Wenn Sie zwei SNA-Anwendungen über IP verbinden möchten, müssen Sie eine Enterprise-Extender-Verbindung definieren, so wie Sie eine SDLC- oder Ethernet-Verbindung definieren würden.

## TN Server

3270-Emulationsprogramme, die über TCP/IP (und nicht über ein SNA-Netz) kommunizieren, werden als TN3270-Programme (Telnet-3270-Emulationsprogramme) bezeichnet.

Einige TN3270-Programme bieten Unterstützung für TN3270E (Standarderweiterungen für Telnet 3270). TN3270E unterstützt über Telnet die Emulation von 3270-Einheiten (sowohl von Terminals als auch von Druckern). Dies ermöglicht dem Telnet-Client, eine bestimmte Einheit auszuwählen (durch Angabe des LU-Namens oder des Namens eines LU-Pools), und bietet erweiterte Unterstützung für verschiedene Funktionen wie für die Schlüssel ATTN und SYSREQ und die SNA-Antwortbearbeitung.

**Anmerkung:** Im vorliegenden Handbuch wird die Bezeichnung TN3270 für Informationen verwendet, die sich auf die Protokolle TN3270, TN3287 und TN3270E beziehen.

TN Server von Communications Server für Linux ermöglicht TN3270-Benutzern den Zugriff auf 3270-Hosts. Über TN Server können TN3270-Benutzer eine Hostverbindung gemeinsam mit Communications Server für Linux oder anderen TN3270-Benutzern verwenden und benötigen keine Direktverbindung. Mit TN Server können TN3270-Benutzer auch auf Hosts ohne TCP/IP zugreifen.

Die Funktion TN Server von Communications Server für Linux ist in Abb. 3 veranschaulicht.

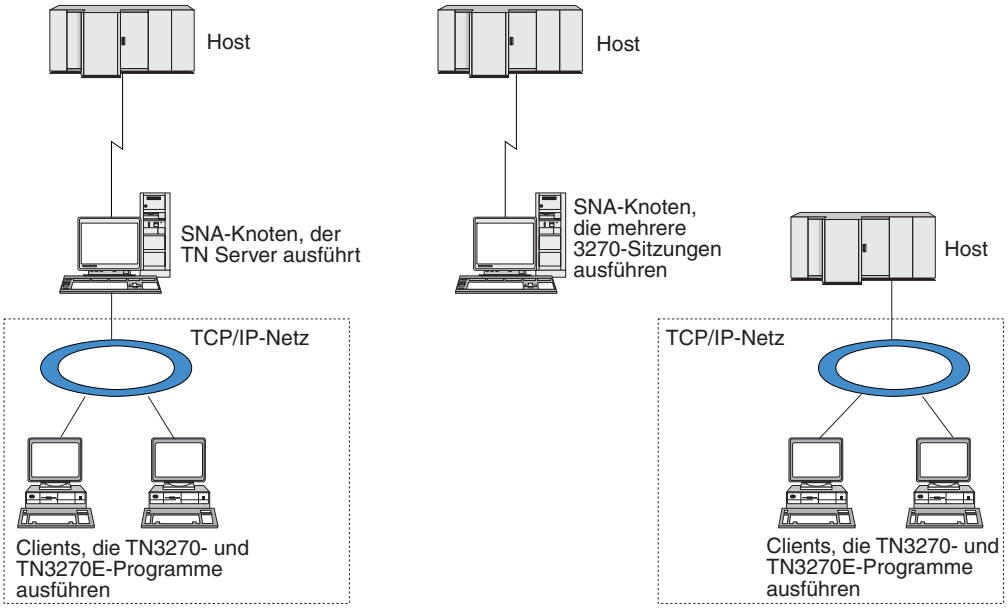


*Abbildung 3. TN Server*

Das Feature TN Server von Communications Server für Linux ermöglicht die Zuordnung eines TN3270-Benutzers zu einer 3270-LU unter Communications Server für Linux. Alle Daten des TN3270-Benutzers werden an die LU weitergeleitet. Dies bedeutet, dass die Konfiguration für den Host und den TN3270-Benutzer so ist, als wären sie direkt miteinander verbunden. Keiner von beiden muss wissen, dass die Daten über TN Server weitergeleitet werden.

TN Server von Communications Server für Linux unterstützt alle TN3270-Client-Emulationsprogramme, die die in den IETF-RFCs 1123, 1576, 1646, 1647 und 2355 definierten Protokolle richtig implementieren.

**Sicherheitsfeatures:** TN Server von Communications Server für Linux unterstützt mit der SSL-Software (Secure Sockets Layer) die Datenverschlüsselung, die Server- und Client-Authentifizierung sowie das Express Logon.

- Datenverschlüsselung bedeutet, dass die zwischen dem TN-Server und dem TN3270-Emulator ausgetauschten Daten in verschlüsselter Form transportiert werden.
- Mit der Serverauthentifizierung kann ein TN3270-Client sicherstellen, dass er eine Verbindung zum erwarteten TN-Server aufbaut.
- Mit der Client-Authentifizierung kann ein TN-Server überprüfen, ob der TN3270-Client, der eine Verbindung zum Server herstellt, der erwartete Client ist. Außerdem kann der TN-Server anhand einer Liste auf einem externen Verzeichnisserver feststellen, ob die Berechtigung des Clients in der Zwischenzeit widerrufen wurde.
- Das Express Logon wird im Zusammenhang mit der Client-Authentifizierung verwendet. Bei aktiviertem Express Logon müssen TN3270-Clients keine Benutzer-ID und kein Kennwort angeben, wenn Sie eine Verbindung zum Host herstellen. Die erforderlichen Angaben (Benutzer-ID und Kennwort) werden aus dem Sicherheitszertifikat des Clients abgerufen.

## TN Redirector

Das Feature TN Redirector von Communications Server für Linux stellt Durchgriffsdienste für 3270-, 5250- oder VT-Sitzungen über TCP/IP bereit. Der Telnet-Benutzer kommuniziert über eine TCP/IP-Verbindung mit Communications Server für Linux und Communications Server für Linux wiederum über eine weitere TCP/IP-Verbindung mit dem Host.

TN Redirector von Communications Server für Linux unterstützt mit der SSL-Software (Secure Sockets Layer) die Datenverschlüsselung sowie die Server- und die Client-Authentifizierung, wie TN Server diese Unterstützung für 3270 zur Verfügung stellt. Auf diese Weise kann bei Bedarf eine SSL-Sicherheitsprüfung (Secure Sockets Layer) durchgeführt werden, ohne diese auf die gesamte Benutzerhostverbindung zu erstrecken. Beispiele:

- Wenn Clients zu Communications Server für Linux eine Verbindung über ein TCP/IP-LAN ohne erforderliche Überprüfung herstellen, jedoch eine Verbindung zu einem fernen Host herstellen, der SSL erfordert, können Sie SSL für die TCP/IP-Verbindung zwischen Communications Server für Linux und dem Host verwenden. Auf diese Weise wird die Sicherheit für alle Clients überprüft. Die einzelnen Clients müssen keine Sicherheitsangaben machen.
- Wenn Communications Server für Linux an demselben Standort wie der Host installiert ist, die Clients die Verbindung jedoch von externen Standorten aus aufbauen, können Sie SSL für die Client-Verbindungen zu Communications Server für Linux verwenden und müssen die SSL-Software nicht auf dem Host installieren.

# Features und Vorteile

Die Features und Vorzüge von Communications Server für Linux reichen von der vereinfachten Konfiguration über die verbesserte Problemanalyse bis hin zur erhöhten Netzleistung.

## Flexible Komponenten

Communications Server für Linux unterstützt die meisten Umgebungen und Knotenfunktionen. Mit Communications Server für Linux kann der Linux-Computer in einem Netz beliebigen Typs (Unterbereichsnetz oder APPN-Netz) eine oder mehrere der folgenden Funktionen übernehmen:

- hostabhängiger Knoten
- Peer-Knoten (eine Beschreibung der APPN-Peer-Knoten finden Sie in den Erläuterungen für Peer-zu-Peer-Netze im Abschnitt „IBM Communications Server für Linux" auf Seite 1)
- Partner (Quelle oder Ziel) in verteilten Anwendungen
- Gateway-Knoten zur Verbindung von SNA-Netzen

Durch APIs für Netzverwaltung kann der Linux-Computer als MS-Eingangspunkt konfiguriert werden und bietet dann Unterstützung für die verteilte Netzverwaltung. Auf Verbindungsebene kann der Linux-Computer mit einer der unterstützten Verbindungsarten mit verschiedenen LANs und WANs verbunden werden. (Eine Beschreibung der Verbindungsarten finden Sie in den Abschnitten „IBM Communications Server für Linux" auf Seite 1 und „Installationsvoraussetzungen" auf Seite 22.)

## Client/Server-Betrieb

Die Client/Server-Konfiguration bietet die folgenden Vorteile:

- Die Konzentration von SNA-Ressourcen auf Servern verringert die Auslastung auf Clients, erhöht den Client-Durchsatz und erfordert weniger Speicher für die Bereitstellung von SNA-Diensten für Clients.
- Mehrere Benutzer an verschiedenen Maschinen können eine Datenverbindung gemeinsam nutzen, so dass nicht für jede Maschine eine physische SNA-Netzverbindung notwendig ist.
- Mehrere Server können eine redundante Konnektivität gewährleisten (z. B., wenn mehrere Server Zugriff auf einen Host ermöglichen). Das Vorhandensein mehrere Pfade zu einer SNA-Ressource macht eine Lastverteilung auf verschiedene Server möglich und bietet eine sofortige Ausweichlösung, falls ein bestimmter Server oder eine bestimmte Verbindung ausfällt.
- Werden mehrere Server übergreifende LU-Pools verwendet, kann der Administrator auf einfache Weise Server und Benutzer konfigurieren und hinzufügen.
- Durch die verringerte Anzahl von Verbindungen und PUs für die Hostkonnektivität reduziert sich die Größe der Host-VTAM-Definition.
- Mit den Verwaltungsdienstprogrammen können Knotenressourcen (für jeden Computer in der Domäne) und gemeinsam genutzte Ressourcen konfiguriert und verwaltet werden. Die Client/Server-Unterstützung der Verwaltungs-Tools von Communications Server für Linux ermöglicht eine transparente Verwaltung aller Domänenressourcen von jedem Computer in der Domäne.
- SNA-Anwendungen können über Internet-Protokolle miteinander verbunden werden, die für die Überwindung von Firewalls sowie für Authentifizierung und Sicherheit TCP/IP und HTTPS verwenden.

## Problemlose Konfiguration

Communications Server für Linux wurde mit Konfigurationsoptionen und Funktionen entwickelt, die die für die Konfiguration erforderliche Zeit und die Komplexität des Netzes reduzieren. Beispiele:

**Motif-Verwaltungsprogramm**
Der einfachste Weg, die CS-Linux-Konfiguration zu definieren und zu ändern, ist die Verwendung des Motif-Verwaltungsprogramms (**xsnaadmin**). Dieses Programm stellt eine grafische Benutzerschnittstelle bereit, über die Sie die CS-Linux-Ressourcen anzeigen und verwalten können. Darüber hinaus vereinfacht dieses Programm die Konfiguration dadurch, dass nur die Felder angezeigt werden, deren Werte bei den verschiedenen Installationen normalerweise variieren, und für andere Felder Standardwerte verwendet werden.

Das Motif-Verwaltungsprogramm stellt Hilfeanzeigen mit übersichtlichen Informationen zu SNA und Communications Server für Linux, Referenzinformationen zu CS-Linux-Dialoganzeigen und Anleitungen zur Ausführung bestimmter Aufgaben bereit.

**Dynamische Konfiguration in APPN-Netzen**
Durch die dynamische Konfiguration von APPN-Netzen wird zusätzlich das Konfigurieren von Knoten oder Netzen erleichtert. APPN-Endknoten und -Anwendungen tragen beispielsweise dynamische Konfigurationsdaten zur Unterstützung von LU-6.2-Sitzungen ein, wodurch die Sitzungskonfiguration optional wird. Dadurch, dass der Knotensteuerpunkt standardmäßig als lokale LU fungiert, können Sie die LU-6.2-Konfiguration ganz umgehen.

APPN unterstützt die dynamische Konfiguration von Verbindungsstationen auch, wenn keine konfigurierten Verbindungsstationen vorhanden sind.

## Zusätzliche Benutzerschnittstellen für die Verwaltung

Das Motif-Verwaltungsprogramm wird als Schnittstelle für die Konfiguration und Verwaltung von Communications Server für Linux empfohlen. Für Communications Server für Linux stehen Ihnen zusätzliche Schnittstellen zur Verfügung, die Sie entsprechend Ihrer Ausrüstung und Ihren Anforderungen auswählen können.

**Befehlszeilenverwaltungsprogramm**
Das Befehlszeilenverwaltungsprogramm (**snaadmin**) kann zum Erstellen von Befehlen für die Verwaltung einzelner CS-Linux-Ressourcen verwendet werden. Sie können **snaadmin** direkt an einer Linux-Eingabeaufforderung ausführen oder in eine Shell-Prozedur integrieren.

**API NOF**
Die API NOF für Communications Server für Linux bietet dieselben Verwaltungsfunktionen wie das Befehlszeilenverwaltungsprogramm an, stellt jedoch eine Schnittstelle bereit, die eher für die Verwendung innerhalb eines Programms als für ein Befehls-Script geeignet ist. Mit der API NOF können Sie eigene Anwendungsprogramme für die Verwaltung von Communications Server für Linux schreiben.

## Verbesserte Leistung

Communications Server für Linux verbessert die ohnehin hohe Leistungsfähigkeit von SNA-Netzen und verwendet Serviceklassen. Darüber hinaus optimiert Communications Server für Linux die Netzgeschwindigkeit durch die SNA-Datenkomprimierung für Sitzungsdaten von LUs 0-3 und durch verschiedene Methoden der Übertragungsverwaltung, die den Übertragungsfluss entsprechend der Netzgröße ausgleichen:

- In APPN-Netzen unterstützt Communications Server für Linux sowohl HPR (High-Performance Routing) als auch ISR (Intermediate Session Routing) und stellt Verbindungsnetzoptionen bereit. ISR bietet Effizienz für kleine Netze, kann bei größeren Netzen jedoch die Leistung verschlechtern.
- In größeren Netzen mit LAN-Konnektivitätsoptionen (wie Token-Ring oder Ethernet) bzw. bei Verwendung von Enterprise Extender kann mit der Verbindungsnetzoption die Effizienz der Übertragung erhöht werden. Die Verbindungsnetzoption erstellt einen direkten Kommunikationspfad zwischen den Knoten, so dass der Datenverkehr Zwischennetzknoten umgehen kann.
- Ein weiterer Mechanismus zur Steuerung des Datenverkehrs, die angepasste Nachrichtendosierung auf Sitzungsebene, reguliert die Auslastung automatisch durch Steuerung der Geschwindigkeit, mit der LUs Nachrichteneinheiten an Partner-LUs senden können.

## Sicherheitsoptionen

Da Netze immer komplexer werden und die Architektur immer offener wird, steht auch das Thema Sicherheit mehr im Vordergrund. Bei SNA-Netzen mit Communications Server für Linux können Sie Ihre Daten durch die Definition verschiedener Sicherheitsstufen in der Konfiguration und durch Implementieren bestimmter Verbindungstypen schützen. Beispiele:

- In einem Client/Server-System können Sie einen WebSphere-Server konfigurieren, der Remote API Clients den HTTPS-Zugriff auf die Server ermöglicht. Bei dieser Art des Zugriffs werden Client-Verbindungen mit Sicherheitszertifikaten authentifiziert. (Dieses Feature erfordert neben dem Standardprodukt Communications Server für Linux zusätzliche Software. Weitere Informationen hierzu finden Sie im Abschnitt „Installationsvoraussetzungen" auf Seite 22.)
- LU-6.2-Benutzer können bis zu drei Sicherheitsstufen definieren: Sitzungssicherheit, Ressourcenschutz und Dialogsicherheit. So stellt der Benutzer sicher, dass die richtigen LUs an einer Sitzung beteiligt sind und dass der Zugriff auf alle einer bestimmten LU zugeordneten Anwendungen bzw. auf eine spezifische Anwendung eingeschränkt wird. Zusätzliche Sicherheit ist durch Datenverschlüsselungsroutinen möglich.
- TN Server und TN Redirector von Communications Server für Linux unterstützen mit der SSL-Software (Secure Sockets Layer) die Datenverschlüsselung sowie die Server- und die Client-Authentifizierung zwischen dem CS-Linux-Server und TN3270- oder Telnet-Clients. (Dieses Feature erfordert neben dem Standardprodukt Communications Server für Linux zusätzliche Software. Weitere Informationen hierzu finden Sie im Abschnitt „Installationsvoraussetzungen" auf Seite 22.)

## Flexibilität bei der Netzverwaltung

Communications Server für Linux unterstützt das Netzverwaltungsschema MDS-NMVT (Multiple Domain Support-Network Management Vector Transport) für eine zentralisierte, verteilte oder hierarchische Verwaltung. Diese Art der Verwaltung basiert auf einer Architektur mit Sammelpunkten/Eingangspunkten und ermöglicht so ein hohes Maß an Flexibilität.

Sammelpunkte sind Steuerknoten, die das Netz entsprechend den von Eingangspunkten (Verwaltungsanwendungen auf allen anderen Knoten im Netz) gesammelten Daten verwalten.

- Bei der zentralen Verwaltung hat ein einzelner Sammelpunkt die Funktion des Steuerpunkts für das gesamte Netz.
- Bei der verteilten Verwaltung teilen sich mehrere Sammelpunkte die Verwaltung des Netzes.
- Bei der hierarchischen Verwaltung sind die Sammelpunkte entsprechend ihren Funktionen verschachtelt.

MDS-NMVT kann daher an die Verwaltung von Unterbereichsnetzen, Standard-APPN-Netzen und sehr großen APPN-Netzen angepasst werden.

## Zuverlässigkeit, Verfügbarkeit und Wartungsfreundlichkeit

Zur Aufrechterhaltung eines zuverlässigen Systembetriebs stellt Communications Server für Linux eine Reihe von Anzeigefunktionen und Fehlerbestimmungs-Tools bereit.

- Das Motif-Verwaltungsprogramm bietet erweiterte Tools für Konfiguration und Verwaltung an. Dazu gehören unter anderem:
  - sofortige Aktualisierung von Konfigurationsdaten
  - Statusinformationen zu Verbindungen, Sitzungen und Knotenressourcen
- Abfrage- und Statusbefehle rufen Informationen zu folgenden Bereichen ab:
  - LU-LU-Sitzungen
  - APPN-Zwischensitzungen
  - aktive Verbindungen
  - APPN-Technologiedatenbanken, in denen Verbindungsinformationen gespeichert sind
- Tools für Fehlerdiagnose unterstützen die verschiedenen Phasen der Konfiguration und des Betriebs. Zu diesen Tools gehören unter anderem:
  - Tool zum Erfassen von Diagnoseinformationen (**snagetpd**), das Ihnen die Erfassung von Serviceinformationen erleichtert
  - Status- und Fehlernachrichten, die Sie bei der Fehlerbehebung für Konfigurationsroutinen und für den Systembetrieb unterstützen
  - Protokolle, in denen Informationen zu Netzfehlern, Störungen und Prüfungen erfasst werden
  - Trace-Funktionen für die Zusammenstellung und Formatierung ausführlicher Fehlerdaten

Weitere Dienstprogramme bieten Ihnen Hilfe beim Testen der Verbindungskonnektivität und der Kommunikation zwischen Anwendungen.

Zu Communications Server für Linux gehört außerdem die API MS (Management Services) für die Entwicklung von Tools, mit denen Netz-Alerts und Fehlermeldungen gesendet und empfangen werden können.

Alle genannten Tools für Verwaltung und Fehlerdiagnose sind vollständig in das Client/Server-Modell von Communications Server für Linux integriert, so dass Sie die gesamte CS-Linux-Domäne verwalten oder Diagnoseinformationen von einem einzelnen Punkt im Netz erfassen können.

## Netzintegration, Wachstum und Veränderungen

Zur Unterstützung der Netzintegration, -erweiterung und -änderung können mit den APIs von Communications Server für Linux Anwendungen für eine bestimmte LU, Plattform oder ein bestimmtes Betriebssystem entwickelt werden, wenn im Unternehmen entsprechender Bedarf besteht. CPI-C ist eine besonders wichtige API, da sie für die verschiedenen Plattformen und Betriebssysteme einheitlich ist. Diese API wird zur Entwicklung von Anwendungen verwendet, die auf einem beliebigen System ausgeführt werden können.

Enterprise Extender bietet außerdem einen Mechanismus für die Integration von SNA- und TCP/IP-Netzen an.

# Kapitel 2. Netz mit IBM Communications Server für Linux planen

Dieses Kapitel bietet einen Überblick über die Schritte bei der Planung eines Netzes, in dem Communications Server für Linux ausgeführt wird. Darüber hinaus finden Sie hier eine Zusammenfassung der Funktionen, die Sie für einen Linux-Computer konfigurieren können, und Richtlinien für die Kalkulation der für die Unterstützung der Funktionen erforderlichen Ressourcen.

## Schritte bei der Netzplanung

Dieser Abschnitt enthält einige allgemeine Richtlinien für die Planung, Konfiguration und Verwaltung von Netzen mit verschiedenen Dienstprogrammen von Communications Server für Linux und Linux.

Zur Planung eines Netzes gehört das Abwägen von Funktion, Leistung, Ressourcen und Kosten. Es gibt keinen idealen Plan für ein Netz, jedoch einige allgemeine Richtlinien und Techniken, mit denen sichergestellt werden kann, dass der Plan Ihren Anforderungen entspricht. Zum Planen eines Netzes führen Sie folgende Schritte aus:

- Bestimmen Sie die Funktionen, die das Netz bieten soll (z. B. Dateiübertragung oder 3270-Emulation), und die Leistungsanforderungen.
- Bestimmen Sie, wie Communications Server für Linux konfiguriert werden kann, um die von Ihnen gewünschten Funktionen bereitzustellen.
- Kalkulieren Sie die erforderlichen Ressourcen und die damit zusammenhängenden Kosten für die Installation von Communications Server für Linux zur Unterstützung Ihrer Leistungs- und Kapazitätsanforderungen und von CS-Linux-Funktionen.

### Funktionsanforderungen für das Netz

Bei der Bestimmung der Funktionen, die das Netz anbieten soll, sollten Sie folgende Fragen berücksichtigen:

- Soll das Netz ein APPN-Netz sein?
- Wird Communications Server für Linux als Client/Server-System ausgeführt? Wenn ja, werden alle Computer in einer CS-Linux-Domäne arbeiten oder müssen mehrere separate Domänen definiert werden?
- Wird in der CS-Linux-Domäne mehr als ein Server benötigt, um den Lastausgleich für Konnektivitätsressourcen zu ermöglichen? Wenn ja, welcher Server soll dann der Konfigurationshauptserver sein? Müssen Ausweichkonfigurationsserver bereitgestellt werden?
- Wird HTTPS-Unterstützung für die Verbindung von Remote API Clients zu CS-Linux-Servern benötigt?
- Werden Benutzeranwendungen auf dem Server oder auf Linux-Client-Computern ausgeführt?
- Soll der Server Konnektivitätsressourcen für Windows-Anwendungen (wie API-Transaktionsprogramme), die auf Windows-Clients ausgeführt werden, bereitstellen?
- Soll jeder Server ein Endpunkt für Sitzungen oder einer der folgenden Gateway-Typen sein?

  - APPN
  - LU 0
  - LU 2
  - TN Server oder TN Redirector
- Welche LUs werden im Netz verwendet?

Die Beantwortung dieser Art von Fragen hilft Ihnen bei der Bestimmung der für das Netz erforderlichen CS-Linux-Funktionen.

## Konfiguration von Communications Server für Linux planen

Wie Communications Server für Linux arbeiten soll, können Sie erst genau definieren, wenn Sie den Arbeitsfluss im Netz kennen. Dazu sollten Sie sich die folgenden Fragen stellen:

- Welche Ressourcen (z. B. Anwendungen) sollen über das Netz verfügbar sein?
- Wie viele Benutzer müssen auf ferne Ressourcen zugreifen?
- Wie häufig wird auf jede Ressource zugegriffen?
- Wie erhalten Benutzer Zugang zum Netz?
- Wie werden Benutzeranfragen im Netz weitergeleitet?

Sie können Communications Server für Linux für die Unterstützung von zahlreichen Funktionen wie die nachfolgend genannten konfigurieren:

- APPN-Netzknoten für ISR (Intermediate Session Routing)
- APPN-Endknoten (die autonom mit Nachbarknoten kommunizieren, aber APPN-Netzknotendienste verwenden, um mit nicht benachbarten Peer-Knoten zu kommunizieren)
- LEN-Knoten (die direkt mit Nachbarknoten oder als Scheinnachbarknoten konfigurierten Knoten kommunizieren)
- Verwendung von LU 0, LU 1, LU 2, LU 3 und LU 6.2 (abhängig und unabhängig)
- SNA-Gateway-Verbindung zu einem Host

Abhängig von Ihren Anforderungen können Sie für einen bestimmten Knoten eine oder mehrere Funktion(en) konfigurieren. Sie können Communications Server für Linux beispielsweise als APPN-Netzknoten konfigurieren, der Routing-Dienste und ISR anbietet, und denselben Knoten für SNA Gateway zur Weiterleitung abhängiger LU-Sitzungen (wie LU 0 und LU 2) verwenden. In ähnlicher Weise können Sie Communications Server für Linux für die Ausführung von TN Server und die Unterstützung einer gemeinsam verwendeten Datenbank sowie einer unabhängigen LU-6.2-Verbindung zu MQSeries auf dem Host konfigurieren.

## Ressourcenanforderungen für Installation und Betrieb

Zur Bestimmung der Unterstützung für die CS-Linux-Funktionen müssen folgende Fragen beantwortet werden:

- Welche Qualifikation müssen die Mitarbeiter haben?
- Welches Übertragungsmedium wird voraussichtlich verwendet?
- Welches sind die Installationsvoraussetzungen für die ausgewählte Konfiguration?
- Wie viel Hauptspeicher und Seitenwechselbereich ist für die Verarbeitung erforderlich?

Die Beantwortung dieser Fragen hilft Ihnen bei der Festlegung der Ressourcenarten, die Communications Server für Linux verwendet, wenn das Produkt für die Unterstützung einer oder mehrerer der im Abschnitt „Funktionsanforderungen für das Netz" auf Seite 19 beschriebenen Funktionen konfiguriert wird. Die Beantwortung der Fragen hilft Ihnen darüber hinaus, das Verhältnis zwischen CS-Linux-Funktionen, Linux-Ressourcen und Netzressourcen besser zu verstehen.

Die Zuordnung der Ressourcen zu Knoten bestimmt die Leistung des Netzes.

## Personalanforderungen

Zum Installieren, Ausführen und Optimieren von Communications Server für Linux ist folgendes Personal erforderlich:

- Netzadministratoren, die das Netz planen, neue Einheiten hinzufügen und die Gesamtnetzleistung gewährleisten und verbessern
- Systemadministratoren, die Communications Server für Linux und die zugrunde liegende Hardware installieren bzw. warten und Systeme für die Netzverbindung konfigurieren
- Programmierer, die angepasste Anwendungen wie Transaktionsprogramme und Netzverwaltungsroutinen entwickeln

Die Netz- und Systemadministratoren müssen mit der Hardware, auf der Communications Server für Linux ausgeführt wird, und mit dem Betriebssystem Linux vertraut sein. Sie müssen die Netze gut kennen, mit denen die verschiedenen Systeme verbunden sind, und mit den allgemeinen SNA-Konzepten vertraut sein. Darüber hinaus müssen Sie Kenntnisse zu folgenden Themen haben:

- Motif-Schnittstelle
- Installations-Tool **rpm** für Linux
- TCP/IP, falls die Verwendung von Client/Server-Funktionen, TN Server oder Enterprise Extender geplant ist
- Betriebssystem Windows 2000, Windows XP oder Windows Server 2003, falls zum CS-Linux-System Remote API Clients für Windows gehören
- WebSphere Application Server, falls zum CS-Linux-System Remote API Clients gehören, die HTTPS für die Verbindung zu Servern verwenden

Programmierer, die angepasste Anwendungen für SNA entwickeln, müssen die Programmiersprache C (oder Java, falls sie Java CPI-C verwenden) kennen sowie mit den APIs, die in Communications Server für Linux verfügbar sind, vertraut sein.

## Übertragungsmedien

Communications Server für Linux wird möglicherweise neben anderen Übertragungsprotokollen auf demselben Übertragungsmedium (wie SDLC oder Token-Ring) ausgeführt. Aus diesem Grund muss die Bandbreite der Bitübertragungsschicht für alle Protokolle und Anwendungen, die auf demselben Übertragungsmedium ausgeführt werden, ausreichend sein.

**Anmerkung:** Communications Server für Linux kann die Token-Ring- und Ethernet-Adapter zusammen mit anderen Protokollen wie TCP/IP verwenden. Es ist möglicherweise erforderlich, eindeutige SAP-Adressen (SAP = Service Access Point) für jedes verwendete Protokoll anzugeben.

## Installationsvoraussetzungen

Die Funktionen, die Sie Communications Server für Linux (aus dem Abschnitt „Funktionsanforderungen für das Netz” auf Seite 19) zuordnen, bestimmen gleichzeitig die Installationsvoraussetzungen. Dieser Abschnitt bietet einen Überblick über die für die Installation von Communications Server für Linux erforderlichen Computerressourcen. Weitere Informationen hierzu finden Sie in der zu den einzelnen Produkten gelieferten Dokumentation.

**Hardware**

Communications Server für Linux erfordert einen Computer, der von einer der nachfolgend genannten Linux-Distributionen unterstützt wird.

Überprüfen Sie mit dem Befehl **uname -m** die CPU-Klasse Ihres Zielcomputers. In der folgenden Tabelle ist für jeden Servertyp die entsprechende Hardware und die Antwort von **uname -m** für diese Hardware angegeben.

| Servertyp | Hardware | Antwort von uname |
|---|---|---|
| 32-Bit Intel | 32-Bit-Intel-System mit Pentium II oder aktuellerem Prozessor | `i686` |
| 64-Bit x86_64 | System mit AMD64 oder Intel EM64T | `x86_64` |
| pSeries | pSeries POWER5 oder OpenPower-System | `ppc64` |

**Betriebssystem Linux**

Bevor Sie Communications Server für Linux auf Ihrer Linux-Workstation installieren und verwenden können, muss auf der Workstation eine geeignete Version des Betriebssystems Linux installiert sein.

Communications Server für Linux unterstützt die folgenden Linux-Distributionen. Die neuesten Informationen zu den spezifischen Versionsnummern und Kernel-Builds, die für jede Distribution unterstützt werden, finden Sie in der Datei **README** auf der CS-Linux-CD.

- Red Hat Enterprise Linux 3 (RHEL3): nur i686
- Red Hat Enterprise Linux 4 (RHEL4)
- SUSE Linux Enterprise Server 8 (SLES8): nur i686
- SUSE Linux Enterprise Server 9 (SLES9)
- SUSE Linux Enterprise Server 10 (SLES10)

**Verbindungshardware**

Verbindungshardware ist nur auf einem Server, nicht aber auf einem Client erforderlich.

Die Installation eines PC in einem oder mehreren Netzen erfordert, dass die Verbindungen nicht in Widerspruch zu dem ausgewählten Übertragungsprotokoll des Netzes stehen. Zur Verbindungshardware gehören ein DFV-Adapter, der im Computer installiert ist, und ein passendes Kabel für den Anschluss an das Netz (Einheitentreibersoftware ist ebenso erforderlich).

**Anmerkung:**

1. DFV-Adapter müssen mit den passenden Kabeln installiert werden. Für einen Ethernet-Adapter benötigen Sie beispielsweise ein Ethernet-Kabel. Andernfalls würde die Verbindung nicht funktionieren.

2. Wenn Sie Enterprise Extender als einzige Verbindungsart verwenden, sind die in diesem Abschnitt aufgelisteten Adapter nicht erforderlich. Stattdessen benötigen Sie einen der für TCP/IP erforderlichen Adapter.

Communications Server für Linux unterstützt DFV-Adapter für die folgenden Verbindungsprotokolle:

- Token-Ring
- Ethernet (Standard oder IEEE 802.3)
- SDLC
- X.25 QLLC

Informationen zu Adaptern, die mit Communications Server für Linux getestet wurden, finden Sie auf der Website http://www.ibm.com/software/network/commserver. Wenn Sie Fragen bezüglich des passenden Adapters oder der erforderlichen Hardware haben, wenden Sie sich an Ihren IBM Vertriebsbeauftragten.

**Zusätzliche Software: Linux**

Communications Server für Linux erfordert die folgende zusätzliche Software. In der Datei **README** auf der CS-Linux-CD finden Sie ausführliche Informationen zu den Voraussetzungen für bestimmte Versionen (je nach verwendeter Linux-Distribution) sowie Anweisungen zur Installation der entsprechenden Softwarepakete.

- LiS Streams. Die Datei **README** enthält Einzelheiten zur erforderlichen Version von LiS Streams sowie die Installationsanweisungen.
- OpenMotif (nur auf einem Server, aber nicht auf einem Client erforderlich). Diese Software wird für die Verwendung des Motif-Verwaltungsprogramms benötigt. Dieses Verwaltungsprogramm wird zum Konfigurieren und Verwalten von Communications Server für Linux empfohlen.
- Java (ist erforderlich, wenn Sie Java CPI-C verwenden möchten). Sie benötigen die Java Runtime Environment (JRE). Wenn Sie neue Java-Klassen für die Verwendung mit einer Java-CPI-C-Anwendung kompilieren müssen, brauchen Sie außerdem das Java SDK.

**WebSphere Application Server (für HTTPS-Zugriff)**

Wenn Sie mit einem Client/Server-System arbeiten möchten, in dem Remote API Clients über HTTPS eine Verbindung zu CS-Linux-Servern herstellen, benötigen Sie WebSphere Application Server, um diesen Clients den HTTPS-Zugriff auf die Server zu ermöglichen.

Communications Server für Linux arbeitet mit WebSphere Application Server Version 5. Sie können diese Version auf einem Computer installieren, auf dem eines der von WebSphere unterstützten Betriebssysteme ausgeführt wird. (Bei Bedarf kann WebSphere Application Server auf demselben Linux-Computer wie Communications Server für Linux installiert werden.) Weitere Informationen zur Installation von WebSphere Application Server finden Sie in der zugehörigen Dokumentation. Um WebSphere zusammen mit Communications Server für Linux verwenden zu können, müssen Sie ein zusätzliches CS-Linux-Plug-in auf diesem Computer installieren. Dieser Schritt ist im Abschnitt „WebSphere Application Server konfigurieren" auf Seite 33 beschrieben.

**Speicher und Hauptspeicher**

Eine Workstation mit Communications Server für Linux, die das gesamte Spektrum der Konfigurationen und Dienste unterstützen soll, muss zusätzlich zu dem für die Linux-Distribution erforderlichen Mindestspeicher über 32 MB Hauptspeicher und über einen Plattenspeicherplatz von 120 MB verfügen. Während der Installation sind zusätzlich 250 MB temporärer Speicher erforderlich.

Falls Sie die Dokumentation zu Communications Server für Linux als Softcopy (PDF) installieren wollen, benötigen Sie zusätzlichen Festplattenspeicherplatz. Für die Installation aller Softcopy-Handbücher benötigen Sie 75 MB Plattenspeicherplatz.

**Anmerkung:** In den hier genannten Anforderungen sind der Hauptspeicher- und Plattenspeicherbedarf für andere Lizenzprogramme, Benutzeranwendungen und Daten nicht enthalten. Sprechen Sie alle Systemvoraussetzungen sowie den Hauptspeicher- und Plattenspeicherbedarf gründlich mit Ihrem zuständigen IBM Ansprechpartner oder IBM Vertriebspartner durch.

## Erweiterte Konfigurationen

Wenn Sie Anwendungen ausführen möchten, für die mehr als die Basiskonfiguration erforderlich ist, müssen Sie zusätzliche Computerressourcen einplanen.

Im Allgemeinen ist der Speicherbedarf zur Ausführung von Communications Server für Linux von vielen verschiedenen Faktoren abhängig, die je nach Funktion und Umgebung der Linux-Workstation variieren. Wenn Sie jedoch die Grundregel berücksichtigen, dass LUs, aktive Verbindungen und laufende Sitzungen die hauptsächlichen Verbraucher von Computerressourcen sind, können Sie den Bedarf an zusätzlichem Hauptspeicher- und Speicherplatz zur Unterstützung der meisten Anwendungen schätzen.

## Hauptspeicher- und Speicherbedarf für den Betrieb

In diesem Abschnitt wird der Hauptspeicher- und Speicherbedarf für eine Workstation mit Communications Server für Linux erläutert.

**Kernel-Speicher**

Linux verwendet Kernel-Speicher, um die Kommunikation zwischen DFV-Subsystemen und DLCs zu ermöglichen. Der Kernel-Speicher ist eine gemeinsam benutzte Ressource, die auf Systemebene verwaltet werden muss. Communications Server für Linux verwendet Kernel-Speicher zum Senden und Empfangen von Daten über das Netz. Hierbei handelt es sich lediglich um eines der Subsysteme, die den Kernel-Speicher verwenden. Die Auslastung des Kernel-Speichers durch Communications Server für Linux kann die Leistung anderer Subsysteme wie TCP/IP oder NFS beeinflussen. Den Bedarf an Kernel-Speicher sollten Sie mit Ihrem Netzadministrator absprechen.

**Haupt- und Plattenspeicher und Speicher für Seitenwechsel**

Communications Server für Linux verwendet wie folgt den primären Speicher (der auch als Haupt- oder Arbeitsspeicher bezeichnet wird), permanenten Plattenspeicher und Plattenspeicher für Seitenwechsel (der auch als Seitenwechselbereich bezeichnet wird):

- Steuerblöcke für SNA-Ressourcen wie LUs, Verbindungen und Sitzungen erfordern primären Speicher.

- Kernel-Speicher belegt nur primären Speicher.
- Die ausführbaren Daten, Konfigurationsdateien und Softcopy-Veröffentlichungen zu Communications Server für Linux belegen permanenten Plattenspeicher.
- Anwendungsprogramme, Sitzungen und ähnliche Prozesse erfordern Seitenwechselbereiche, die permanenten Plattenspeicher belegen.

Der Speicher- und Plattenspeicherbedarf hängt stark von verschiedenen Faktoren ab, die sich je nach Umgebung unterscheiden. TPs und SNA-Sitzungen sind die hauptsächlichen Nutzer von Haupt- und Plattenspeicher.

Ein TP ist ein Programm, das die SNA-Anwendungsprogrammierschnittstelle verwendet, um auf das Netz zuzugreifen. Eine Sitzung ist ein temporärer logischer Kanal zwischen zwei LUs auf Partnerknoten. TPs verwenden diesen Kanal, um miteinander zu kommunizieren.

Die Belegung des Haupt- und Festplattenspeichers hängt stark von der Gesamtanzahl der Sitzungen, der Anzahl zugeordneter Sitzungen (Dialoge), der Intensität des über die Dialoge transportierten Datenverkehrs und der Anzahl der aktiven Benutzer-TPs ab. Der Speicherbedarf richtet sich hauptsächlich nach dem Datenverkehrsaufkommen und der daraus resultierenden Kernel-Speicherbelegung. Der Plattenspeicherbedarf ist von dem für TPs, Sitzungen und den damit zusammenhängenden Prozessen abhängig.

Bei allen LU-Typen wird zwischen einer freien Sitzung und einer zugeordneten Sitzung unterschieden. Eine freie Sitzung ist eine aktive Sitzung, die nicht von TPs verwendet wird. Eine zugeordnete Sitzung unterstützt einen fortlaufenden Dialog. Zum Bestimmen des Gesamtspeicherbedarfs müssen Sie das Datenverkehrsaufkommen und die ungefähre Gesamtanzahl der durchschnittlich zugeordneten Sitzungen schätzen. Sie können das System auch für Spitzenbelastungen konfigurieren. Diese Schätzungen variieren den Umgebungen entsprechend.

Wenn die Sitzungen die Kapazität des Systemspeichers überschreiten, entstehen Kosten für den Seitenwechsel.

**Prozesse**

Communications Server für Linux erfordert mindestens 20 Linux-Prozesse.

## Kompatibilität plattformübergreifender Konfigurationen gewährleisten

SNA-Produkte die auf verschiedenen Plattformen ausgeführt werden, z. B. IBM Personal Communications, Communications Server für Windows oder VTAM NCP auf einem Host, können unter bestimmten Voraussetzungen zusammen mit Communications Server für Linux verwendet werden.

Im Allgemeinen funktioniert das aktuelle Release eines Produkts für den SNA-Netzbetrieb mit Communications Server für Linux, solange es PU-2.1-Knoten und mindestens eine der von Communications Server für Linux unterstützten Verbindungsarten unterstützt. Einige ältere Releases (wie VTAM V2) arbeiten jedoch möglicherweise nicht zuverlässig. Das Leistungsspektrum jedes Produkts für den Netzbetrieb ist im jeweiligen Benutzerhandbuch dokumentiert.

### Kompatibilität plattformübergreifender Konfigurationen gewährleisten

Die folgenden weiteren Faktoren sollten berücksichtigt werden:

- Wenn Sie die unabhängige LU 6.2 verwenden und Ihr Netz kein APPN-Netz ist, müssen Sie sicherstellen, dass die Partner-LUs für das lokale System definiert sind.
- Da die Standardwerte für DLC-Fenstergrößen und -Zeitgeber je nach Einheit variieren, müssen Sie sicherstellen, dass ferne Einheiten den richtigen Wert verwenden. Eine DLC-Fenstergröße, die beispielsweise für einen Knoten mit Communications Server für Windows NT gut geeignet ist, muss sich nicht für einen 3172-Knoten eignen.
- Wenn Sie in einer heterogenen Umgebung (TCP/IP- und SNA-Protokolle in einem LAN) mit verschiedenen LAN-Segmenten arbeiten, stellen Sie sicher, dass Ihre LAN-Verbindungseinheiten gleichzeitig TCP/IP-Rahmen „weiterleiten" und SNA-Rahmen „überbrücken" können.

## Namenskonventionen

Mit Netz-IDs können Sie Ihr physisches Netz logisch in Segmente unterteilen. Falls Sie vorhaben, eine Verbindung zu anderen Netzen herzustellen, sollten Sie Ihre Netz-IDs registrieren lassen, um Konflikte bei Netznamen zu vermeiden.

Sie können Netz- und LU-Namen wie folgt definieren:

**Netznamen**
Sie können verschiedene Netznamen (Netz-IDs) für die Segmentierung von APPN-Netzen definieren. Die Segmentierung begrenzt die Größe der Topologiedatenbanken im Netz und die Häufigkeit der über jedes Netz gesendeten LOCATE-Anforderungen.

Um die Eindeutigkeit einer Netz-ID sicherzustellen, kann der Netzadministrator die ID des Netzes über den weltweiten Registrierungsservice der IBM registrieren lassen. Die IBM Registrierung stellt sicher, dass jede Netz-ID eindeutig ist. Die Registrierungsstandards entsprechen den OSI-Standards (Open Systems Interconnection), einschließlich der OSI-Landescodes, gemäß ISO (International Organization for Standards). Weitere Informationen zur Registrierung finden Sie im *User's Guide for SNA Network Registry*.

**LU-Namen**
Für LU-Namen können Sie Platzhalterzeichen verwenden, um den Aufwand für die Systemdefinition und Suchvorgänge im Netz zu reduzieren.

# Kapitel 3. Communications Server für Linux auf Linux-Servern installieren

Dieses Kapitel enthält allgemeine Informationen zu den Schritten, die für die Installation von Communications Server für Linux auf einem Linux-Server erforderlich sind. Eine ausführliche schrittweise Anleitung für den Installationsprozess finden Sie in der Datei **README** auf der CS-Linux-CD. Diese Datei enthält aktuelle und detaillierte Hinweise zur Ihrer spezifischen Linux-Distribution. In der Datei **README** finden Sie Folgendes:

- Genaue Paketnamen und/oder Versionsnummern für die benötigten zusätzlichen Softwarepakete
- Ausführliche Informationen zur Installation und zu den Konfigurationsbefehlen.

## Angebotene CS-Linux-Lizenzprogrammpakete

Das Lizenzprogramm Communications Server für Linux wird auf drei CDs mit folgendem Inhalt geliefert.

**CD 1: Schnelleinstieg**
Diese CD enthält die vollständige PDF-Dokumentation zu Communications Server für Linux (im Verzeichnis **/DOCS**).

**CD 2: Server**
Diese CD enthält die erforderlichen Dateien für die Installation eines Servers.

- **README**-Dateien mit Informationen zu den Änderungen, die nach Herausgabe der CS-Linux-Dokumentation am Produkt vorgenommen wurden
- Installations-Scripts
- Installationsimages für den Server und die PDF-Handbücher

**CD 3: Clients**
Diese CD enthält die -Dateien, Installations-Scripts und Installationsimages für die Installation der einzelnen Clients.

- Linux-Client für 32-Bit Intel (i686)
- Linux-Client für 64-Bit AMD64/Intel EM64T (x86_64)
- Linux-Client für pSeries (ppc64)
- Linux-Client für System z9 oder System z (s390/s390x)
- AIX-Client
- 32-Bit-Windows-Client
- x64-Windows-Client

In den **README**-Dateien finden Sie ausführliche Angaben zu den auf den CDs enthaltenen Dateien.

**Anmerkung:** Informationen zum Speicherbedarf finden Sie im Abschnitt „Installationsvoraussetzungen" auf Seite 22.

# Installation von Communications Server für Linux vorbereiten

Führen Sie vor der Installation von Communications Server für Linux die folgenden Schritte aus:

- Stellen Sie sicher, dass die Stromverbrauchssteuerung des Linux-PC nicht aktiviert ist.
- Vergewissern Sie sich, dass die gesamte vorausgesetzte Software, die im Abschnitt „Installationsvoraussetzungen" auf Seite 22 aufgelistet ist, installiert wurde.

Die folgenden Abschnitte enthalten Informationen zu diesen Tasks.

## Features für Stromverbrauchssteuerung inaktivieren

Vor der Installation von Communications Server für Linux müssen Sie überprüfen, ob es auf Ihrem Linux-PC Features für erweiterte Stromverbrauchssteuerung gibt. Sollte dies der Fall sein, müssen Sie sicherstellen, dass diese Features inaktiviert sind. Viele moderne PCs bieten diese Features an, um Strom zu sparen, wenn die Tastatur oder Maus nicht benutzt wird. (Dazu wird die Stromzufuhr zu Einheiten wie Plattenlaufwerken unterbrochen und die CPU-Taktrate herabgesetzt.) Die erweiterte Stromverbrauchssteuerung wurde für PCs entwickelt, die als Workstation verwendet werden. Sie ist nicht geeignet, wenn der PC als Server eingesetzt wird, weil ein Server auch ohne Tastatur- oder Mausaktivität normal arbeiten kann.

Zum Inaktivieren dieser Features müssen Sie in der Startphase des PC auf die BIOS-Konfiguration zugreifen (normalerweise durch Drücken der Taste **F1** beim Initialisieren der Hardware) und sowohl die erweiterte Stromverbrauchssteuerung als auch die Stromverbrauchssteuerung der Hardware inaktivieren.

Mit dem folgenden Befehl können Sie das Feature für erweiterte Stromverbrauchssteuerung von Ihrem PC entfernen.

**rpm -e apmd**

## Vorausgesetzte Software installieren

Vor der Installation von Communications Server für Linux müssen Sie die vorausgesetzte Software installieren, die im Abschnitt „Installationsvoraussetzungen" auf Seite 22 aufgelistet ist:

- LiS Streams
- OpenMotif
- Java
- SSL

Umfassende Informationen zu den erforderlichen Softwarepaketen sowie eine schrittweise Anleitung für die Installation finden Sie in der Datei **README** auf der CS-Linux-CD.

## Einzelheiten zur Produktinstallation anzeigen

Sie können Informationen zu Communications Server für Linux und zu den bereits installierten zugehörigen Softwarepaketen anzeigen. Verwenden Sie den folgenden Befehl, um alle installierten Pakete aufzulisten:

**rpm -q -a**

Wenn Sie weitere Details zu einem bestimmten Paket anzeigen möchten, verwenden Sie den folgenden Befehl:

**rpm -q -i** *Paketname*

*Paketname* steht hier für den Basisnamen des installierten Pakets, z. B. **ibm-commserver**.

## Sprachumgebungsvariable ändern

Wenn Sie Communications Server für Linux verwenden, vergewissern Sie sich, dass die Variable `LANG` auf die von Ihnen gewünschte Sprache gesetzt ist.

Mit dem folgenden Befehl können Sie die Variable `LANG` ändern:

**export LANG=***Sprache*

Ersetzen Sie *Sprache* durch den Bezeichner für die gewünschte Sprache. Folgende Bezeichner können angegeben werden:

| Kennung | Sprache |
|---|---|
| **de_DE** | Deutsch |
| **en_US** | Englisch (Vereinigte Staaten) |
| **es_ES** | Spanisch |
| **fr_FR** | Französisch |
| **ja_JP** | Japanisch (PC) |
| **ko_KR** | Koreanisch |
| **pt_BR** | Portugiesisch |
| **zh_CN** | Chinesisch (vereinfacht, EUC) |
| **zh_TW** | Chinesisch (traditionell) |

# Vorversionen von Communications Server für Linux migrieren

Falls Sie bereits eine frühere Version von Communications Server für Linux installiert haben und jetzt auf Version 6.2.2 migrieren möchten, müssen Sie die folgenden Schritte ausführen:

**Speichern aller angepassten Konfigurationsdateien**

Wenn die nachfolgend aufgelisteten Dateien vorhanden sind, speichern Sie sie in einem temporären Verzeichnis. Nicht bei jeder Installation sind alle genannten Dateien vorhanden.

**/etc/opt/sna/sna_node.cfg**
**/etc/opt/sna/sna_domn.cfg**
**/etc/opt/sna/sna.net**
**/etc/opt/sna/sna_tps**
**/etc/opt/sna/ibmcs.kdb**
**/etc/opt/sna/ibmcs.sth**
**/etc/opt/sna/ibmcs.rdb**
**/etc/opt/sna/ibmcs.crl**
**/etc/opt/ibm/sna/sna_node.cfg**
**/etc/opt/ibm/sna/sna_domn.cfg**
**/etc/opt/sna/sna.net**
**/etc/opt/ibm/sna/sna_tps**
**/etc/opt/ibm/sna/ibmcs.kdb**
**/etc/opt/ibm/sna/ibmcs.sth**
**/etc/opt/ibm/sna/ibmcs.rdb**

**/etc/opt/ibm/sna/ibmcs.crl**

Falls Sie die Startdatei **/etc/rc.d/init.d/snastart** wie im Abschnitt „Communications Server für Linux aktivieren" auf Seite 74 beschrieben angepasst und den Befehl **sna start** entfernt haben, damit Communications Server für Linux beim Systemstart nicht automatisch gestartet wird, müssen Sie die Änderungen notieren, die Sie an dieser Datei vorgenommen haben.

**Deinstallieren des alten Release**

Verwenden Sie die folgenden Befehle, um Communications Server für Linux zu stoppen und zu deinstallieren. Möglicherweise sind nicht alle hier aufgelisteten RPM-Pakete auf Ihrem System vorhanden. Dies ist davon abhängig, wie Sie welche Vorversion installiert haben.

```
sna stop
rpm -e CS-LINUX-ptf
rpm -e CS-LINUX-Docs
rpm -e CS-LINUX-ecl
rpm -e CS-LINUX
rpm -e ibm-conmserver-ptf
rpm -e ibm-commserver-docs
rpm -e ibm-commserver-ecl
rpm -e ibm-commserver
rpm -e gsk5bas
rpm -e gsk6bas
```

**Deinstallieren von LiS**

Deinstallieren Sie mit den folgenden Befehlen die aktuelle Version des Open-Source-Pakets LiS.

```
PATH=$PATH:/sbin
unset LD_PRELOAD
rmmod streams
cd /usr/src/LiS
make uninstall
make very-clean
cd /usr/src
rm -rf LiS*
```

**Ändern von PATH und anderen Umgebungsvariablen**

Falls Sie die folgenden Umgebungsvariablen für die frühere Version von Communications Server für Linux modifiziert haben, sollten Sie die Änderungen rückgängig machen, weil die Pfade für das Lizenzprogramm Communications Server für Linux Version 6.2.2 andere sein können.

```
PATH
LD_LIBRARY_PATH
LD_RUN_PATH
LD_PRELOAD
CLASSPATH
```

Mit dem Befehl **env** können Sie alle Umgebungsvariablen auf Referenzen zu **sna** überprüfen:

```
env | grep sna
```

**Weitere Pakete**

Sie sollten Ihre Java-Installation überprüfen und ggf. auf den neuesten Stand bringen.

**Abschließende Bereinigung**
Mit den folgenden Befehlen werden alle verbliebenen Einträge der alten Produktversion entfernt. Möglicherweise sind nicht alle hier aufgelisteten Verzeichnisse auf Ihrem System vorhanden. Dies ist davon abhängig, wie welche Vorversion Sie installiert haben.

**rm -rf /etc/opt/sna /var/opt/sna /opt/sna**

**rm -rf /etc/opt/ibm/sna /var/opt/ibm/sna /opt/ibm/sna**

**Installieren des Lizenzprogramms Communications Server für Linux Version 6.2.2**
Führen Sie für die Installation des Produkts die Anweisungen in diesem Handbuch und in der Datei **README** aus.

**Zurückschreiben der gespeicherten Konfiguration**
Falls Sie im ersten Schritt dieses Prozesses Konfigurationsdateien gespeichert haben, müssen Sie diese jetzt zurückschreiben. Stoppen Sie zunächst die Software Communications Server für Linux mit dem folgenden Befehl:

**/opt/ibm/sna/bin/sna stop**

Falls Sie im ersten Schritt dieses Prozesses **ibmcs.***-Dateien gespeichert haben, müssen Sie jetzt **alle ibmcs.***-Dateien aus dem Verzeichnis **/etc/opt/ibm/sna** entfernen. Wenn Sie beispielsweise **ibmcs.kdb** und **ibmcs.sth** gespeichert haben, müssen Sie **ibmcs.crl** und **ibmcs.rdb** entfernen, obwohl Sie keine Ersatzdateien für diese Dateien gespeichert haben. Es ist wichtig, dass Sie nicht mit einer Mischung aus gespeicherten und neuen Dateien arbeiten.

Schreiben Sie die gespeicherten Dateien in das Verzeichnis **/etc/opt/ibm/sna** zurück.

Falls Sie Änderungen an der Startdatei **/etc/rc.d/init.d/snastart** gespeichert haben, müssen Sie dieselben Änderungen an der neuen Kopie der Datei vornehmen, um sicherzustellen, dass Communications Server für Linux nicht automatisch beim Systemstart gestartet wird. Gehen Sie dazu wie im Abschnitt „Communications Server für Linux aktivieren" auf Seite 74 beschrieben vor.

Geben Sie jetzt den folgenden Befehl ein, um die Software Communications Server für Linux neu zu starten:

**/opt/ibm/sna/bin/sna start**

## Lizenzprogramm Communications Server für Linux installieren

Nachdem Sie die vorausgesetzte Software wie im Abschnitt „Vorausgesetzte Software installieren" auf Seite 28 beschrieben installiert haben, können Sie mit der Installation von Communications Server für Linux beginnen. Gehen Sie dazu wie folgt vor:

1. Melden Sie sich mit Root-Berechtigung an.
2. Installieren Sie Communications Server für Linux wie im Abschnitt „Communications Server für Linux installieren" auf Seite 32 beschrieben.
3. Falls Sie die GSKIT-Software installiert haben, weil Sie TN Server oder TN Redirector mit dem Feature SSL verwenden möchten, müssen Sie die SSL-Software nach der Installation von Communications Server für Linux konfigurieren.

Weitere Informationen hierzu finden Sie im Abschnitt „SSL für die Verwendung mit TN Server oder TN Redirector konfigurieren" auf Seite 36.

4. Passen Sie bei Bedarf die Konfigurationsdaten von Communications Server für Linux an. (Hinweise hierzu finden Sie in Kapitel 8, „Communications Server für Linux konfigurieren und verwenden", auf Seite 71 oder im *Communications Server für Linux Verwaltungshandbuch*.)
5. Starten Sie Communications Server für Linux. Nach der Installation geschieht dies automatisch, wenn die Maschine neu gebootet wird.

   **cd /**

   **sna start**

**Anmerkung:**

1. Bei der automatischen Installation von Communications Server für Linux werden die SNA-Einheitentreiber auf dem lokalen Knoten rekonfiguriert. Wenn Sie die Installation auf einem Computer mit begrenztem Speicher (z. B. 64 MB) ausführen, müssen Sie nach der Installation von Communications Server für Linux unter Umständen einen Warmstart durchführen, bevor der SNA-Knoten gestartet werden kann.
2. Nach der Installation von Communications Server für Linux können Sie Adapter installieren. Communications Server für Linux muss nach dem Hinzufügen eines Adapters nicht erneut installiert werden.

## Communications Server für Linux installieren

1. Legen Sie die Installations-CD in das entsprechende Laufwerk der Linux-Workstation ein.
2. Melden Sie sich mit Root-Berechtigung an.
3. Führen Sie das Programm **installibmcs** von der CD aus. In der Datei **README** auf der CS-Linux-CD finden Sie ausführliche Informationen zu den hierfür erforderlichen Befehlen.

   Das Programm fordert Sie normalerweise zu den folgenden Eingaben auf.

   - Bestätigung der Lizenzbedingungen für Communications Server für Linux
   - Name des Hauptservers in der CS-Linux-Domäne. Wenn Sie Communications Server für Linux als eigenständigen Knoten ausführen möchten, geben Sie diesen Parameter nicht an. In diesem Fall unterstützt der Knoten keine Client/Server-Funktionen.

   Sie können diese Eingabeaufforderungen außer Kraft setzen, indem Sie den Befehl **installibmcs** wie nachfolgend beschrieben mit zusätzlichen Parametern angeben.
4. Falls Sie die PDF-Dokumentation zu Communications Server für Linux installieren möchten, führen Sie das Programm **installibmcsdocs** von der CD aus.
5. Passen Sie die Konfigurationsdaten von Communications Server für Linux an. (Hinweise hierzu finden Sie in Kapitel 8, „Communications Server für Linux konfigurieren und verwenden", auf Seite 71 oder im *Communications Server für Linux Verwaltungshandbuch*.)

Wenn Sie eine nicht überwachte Installation ausführen müssen, können Sie den Befehl **installibmcs** mit zusätzlichen Parametern angeben, um die Lizenzbedingungen für Communications Server für Linux zu akzeptieren und den

Namen des Hauptservers anzugeben. In diesem Fall wird das Shell-Script ausgeführt, ohne den Benutzer zur Eingabe weiterer Informationen aufzufordern. Verwenden Sie den folgenden Befehl:

**./installibmcs license_accepted [** *Hauptservername* **]**

*Hauptservername* steht hier für den Namen des Hauptservers. Wenn Sie Communications Server für Linux als eigenständigen Knoten ausführen möchten, geben Sie diesen Parameter nicht an. In diesem Fall unterstützt der Knoten keine Client/Server-Funktionen.

**Anmerkung:** Bei der automatischen Installation von Communications Server für Linux werden die SNA-Einheitentreiber auf dem lokalen Knoten rekonfiguriert.

## Onlinedokumentation zu Communications Server für Linux

Führen Sie die Schritte im Abschnitt „Communications Server für Linux installieren" auf Seite 32 aus, um die Installations-CD mit Communications Server für Linux zu laden. Melden Sie sich dann mit Root-Berechtigung an und führen Sie das Shell-Script **installibmcsdocs** aus.

**./installibmcsdocs**

## Host Access Class Libraries (HACL)

Die HACL-Dateien werden bei der Installation von Communications Server für Linux automatisch installiert. Der Bibliothekscode befindet sich im Paket **ibm-commserver-ecl** unter **rpm**. Diese Dateien und die README-Datei finden Sie unter **/opt/ibm/sna/ecl** oder können Sie mit folgendem Befehl abrufen:

**rpm —ql ibm-commserver-ecl**

# WebSphere Application Server konfigurieren

Wenn Sie mit einem Client/Server-System arbeiten, in dem Remote API Clients über HTTPS eine Verbindung zu CS-Linux-Servern herstellen, benötigen Sie einen Computer, auf dem WebSphere Application Server ausgeführt wird, um diesen Clients den HTTPS-Zugriff auf die Server zu ermöglichen. Lesen Sie hierzu die Informationen im Abschnitt „Installationsvoraussetzungen" auf Seite 22.

In den folgenden Abschnitten ist beschrieben, mit welchen Schritten Sie WebSphere für die Verwendung mit Communications Server für Linux konfigurieren müssen:

- Konfigurieren eines sicheren Zertifikats auf dem WebSphere-Server, das den Clients vorgelegt wird
- Konfigurieren von WebSphere Application Server für die Verwendung mit Communications Server für Linux
- Installieren der Serverkonfigurationsdatei auf dem WebSphere-Server

Außerdem müssen Sie auf jedem Remote API Client, der auf WebSphere Application Server zugreifen soll, das Client-Sicherheitszertifikat und die Client-Netzdatendatei konfigurieren. Weitere Informationen hierzu finden Sie im Kapitel zur Installation des jeweiligen Client-Typs.

## Sicherheitszertifikat für WebSphere Application Server konfigurieren

Anweisungen zum Konfigurieren eines sicheren Zertifikats auf dem Server finden Sie in der Dokumentation zu WebSphere Application Server. Dieses Serverzertifikat wird einem Remote API Client während der Authentifizierung vorgelegt, wenn der Client versucht, über HTTPS eine Verbindung herzustellen.

Sie sollten WebSphere so konfigurieren, dass die Client-Authentifizierung durchgesetzt wird. Informieren Sie sich hierüber in der Dokumentation zu WebSphere Application Server. Wenn die Client-Authentifizierung erzwungen wird, fordert WebSphere während des Authentifizierungsprozesses Sicherheitszertifikate von Remote API Clients an und akzeptiert ankommende Verbindungen von Remote API Clients nur dann, wenn die Authentizität des Client-Zertifikats verifiziert werden kann.

## WebSphere Application Server konfigurieren

Führen Sie die folgenden Schritte aus, um WebSphere Application Server für die gemeinsame Verwendung mit Communications Server für Linux zu konfigurieren. Weitere Informationen hierzu finden Sie in der Dokumentation zu WebSphere Application Server.

1. Kopieren Sie die beiden Dateien **snahttpsrv.ear** und **snahttpsrv.cfg** aus dem Verzeichnis **ibm-commserver-https** der Installations-CD mit Remote API Client in ein Verzeichnis auf dem Computer mit der WebSphere-Administrationskonsole oder in ein Netzverzeichnis, auf das dieser Computer zugreifen kann, oder übertragen Sie die genannten Dateien mit FTP in dieses Verzeichnis.

   Wenn die Administrationskonsole unter Windows ausgeführt wird, müssen Sie die Dateien nicht kopieren, weil Sie direkt auf die CD mit den Dateien zugreifen können. Sie müssen nur die Installations-CD mit Remote API Client in das CD-Laufwerk des Windows-Computers einlegen.
2. Starten Sie die WebSphere-Administrationskonsole.
3. Erstellen Sie gemäß den Anweisungen in der WebSphere-Dokumentation einen virtuellen Host, auf den nur über eine sichere SSL-Verbindung zugegriffen werden kann. Dieser virtuelle Host wird für das Java-Plug-in verwendet, das SNA-HTTPS-Verbindungen verwaltet.
4. Wählen Sie in der Menüleiste 'Anwendungen' -> 'Neue Anwendung installieren' aus.
5. Geben Sie die Position der Datei **snahttpsrv.ear** an. Klicken Sie auf 'Weiter'.
6. Wenn Sie in den beiden ersten Anzeigen aufgefordert werden, einen virtuellen Hostnamen anzugeben, geben Sie den Namen des virtuellen Hosts ein, den Sie für HTTPS konfiguriert haben. Für alle übrigen Parameter können Sie die Standardeinstellungen übernehmen, sofern Sie keine spezifische WebSphere-Konfiguration erstellen möchten. Klicken Sie in den folgenden Dialoganzeigen jeweils auf 'Weiter', bis nur noch der Knopf 'Fertig stellen' angezeigt wird. Klicken Sie dann auf 'Fertig stellen'. Auf dem Bildschirm wird die Nachricht **Die Anwendung wurde installiert** angezeigt.
7. Klicken Sie auf 'In Master-Konfiguration speichern' und anschließend auf 'Speichern'.
8. Wählen Sie in der Menüleiste 'Anwendungen' -> 'Enterprise-Anwendungen' aus.
9. Suchen Sie in der Liste der Anwendungen den Eintrag **SnaHttpTransport** und klicken Sie auf das daneben befindliche Markierungsfeld. Klicken Sie dann auf

'Starten', um die Anwendung zu starten. (Danach wird die Anwendung automatisch beim Start von WebSphere Application Server gestartet.)

10. Wählen Sie in der Menüleiste 'Umgebung' -> 'Webserver-Plug-in aktualisieren' aus und klicken Sie auf 'OK'. Die WebSphere-Konfiguration wird aktualisiert.

### Serverkonfigurationsdatei installieren

Für die Zusammenarbeit mit Communications Server für Linux benötigt WebSphere Application Server eine Liste der CS-Linux-Server, auf die mit HTTPS zugegriffen werden soll. Führen Sie zum Erstellen und Installieren der Liste die folgenden Schritte aus.

1. Wählen Sie in der Menüleiste der WebSphere-Administrationskonsole 'Umgebung' -> 'WebSphere-Variablen verwalten' aus.
2. Suchen Sie in der Liste nach der Variablen **USER_INSTALL_ROOT** und notieren Sie den Wert der Variablen. (Dies ist der Pfad eines Verzeichnisses auf dem WebSphere-Server.) Die Liste der Umgebungsvariablen kann zwei oder mehr Seiten umfassen, so dass Sie unter Umständen die Taste zum Vorblättern verwenden müssen, um die gesamte Liste durchzublättern.
3. Kopieren Sie die Datei **snahttpsrv.cfg** von der Position, an der Sie sie beim Durcharbeiten des Abschnitts „WebSphere Application Server konfigurieren" auf Seite 34 gespeichert haben, (oder von der Installations-CD) in das von der Variablen **USER_INSTALL_ROOT** angegebene Verzeichnis. Bearbeiten Sie diese Datei dann mit einem Texteditor. Nehmen Sie die CS-Linux-Server auf, auf die Remote API Clients mit HTTPS zugreifen können. Jeder Server muss in einer gesonderten Zeile der Datei und im folgenden Format angegeben werden:

   **server=***servername.domänenname.com*

## Prozeduren für den Installationsabschluss

In den folgenden Abschnitten ist die Ausführung von Verwaltungs-Tasks beschrieben, die nach der Installation von Communications Server für Linux erforderlich sein können.

### Client/Server-Betrieb

Communications Server für Linux wird nach der Installation als eigenständiger Server (mit allen Komponenten auf einem Linux-System) ausgeführt. Falls Sie Communications Server für Linux als Server in einer Client/Server-Domäne ausführen möchten, lesen Sie die diesbezüglichen Anweisungen im Kapitel 'Client/Server-System mit Communications verwalten' des *Communications Server für Linux Verwaltungshandbuchs*.

### PDF-Handbücher anzeigen

Die auf dem Installationsdatenträger für dieses Produkt enthaltenen Handbücher liegen im Portable Document Format (PDF) vor. Das Softcopy-Format ermöglicht Ihnen durch Hypertextverbindungen, die gewünschten Informationen leichter zu finden und zu drucken. Dieses Format vereinfacht auch die gemeinsame Nutzung der Bibliothek an Ihrem Standort, weil PDF-Anzeigeprogramme für viele verschiedene Plattformen verfügbar sind.

Falls Sie bei der Installation des Produkts die PDF-Handbücher zur Installation auswählen, werden diese im Verzeichnis **/opt/ibm/sna/docs** installiert. Die Handbücher sind außerdem im Verzeichnis **/DOCS** des Installationsdatenträgers mit Communications Server für Linux enthalten.

Sie können die PDF-Handbücher mit einem beliebigen PDF-Anzeigeprogramm wie Adobe Acrobat unter Windows oder **xpdf** unter Intel Linux lesen.

## Aktuelle Releaseinformationen prüfen

Der neueste Stand der Informationsdatei **README** zum Produkt befindet sich im Verzeichnis **/opt/ibm/sna/** und enthält Informationen zu allen Produktänderungen, die nach Veröffentlichung der Bibliothek zu Communications Server für Linux vorgenommen wurden. Sie finden diese Datei auch im Stammverzeichnis des Installationsdatenträgers mit Communications Server für Linux. Immer, wenn Sie Produktupdates erhalten, sollten Sie nach zugehörigen Informationen in der Datei **README** suchen.

## SSL für die Verwendung mit TN Server oder TN Redirector konfigurieren

Falls Sie die GSKIT-Software installiert haben, weil Sie TN Server oder TN Redirector mit dem Feature SSL verwenden möchten, müssen Sie die SSL-Software nach der Installation von Communications Server für Linux konfigurieren.

Die SSL-Software erfordert zwei Komponenten:

- Für die Verschlüsselung und Entschlüsselung von Daten wird ein Schlüsselpaar benötigt.
- Für die Serverauthentifizierung ist ein Zertifikat erforderlich.

Zertifikat und Schlüsselpaar zusammen bilden einen Datensatz in einer Schlüsselringdatenbank, die auf dem CS-Linux-Server mit TN Server oder TN Redirector gespeichert wird. Communications Server für Linux verwendet die Datenbank für die Implementierung von SSL.

Geben Sie zum Verwalten der Schlüsselringdatenbank an der Linux-Eingabeaufforderung den folgenden Befehl ein:

**snakeyman**

Der Befehl **snakeyman** startet ein Java-Programm. Weitere Anweisungen finden Sie in den von diesem Programm bereitgestellten Hilfetexten.

Jeder Datensatz in der Datenbank ist durch einen eindeutigen Namen, den Kennsatz, gekennzeichnet. Falls Sie für verschiedene TN-Server- oder TN-Redirector-Sitzungen zwei oder mehr Datensätze verwenden müssen, sollten Sie sich die Kennsätze notieren, die Sie beim Einrichten der Datenbank zuordnen. Anhand dieser Kennsätze wird festgestellt, welcher Datensatz für welche Sitzung zu verwenden ist. Sie können auch einen der Datensätze als Standard definieren, so dass Sitzungen diesen Kennsatz verwenden, solange nicht explizit der Kennsatz eines anderen Datensatzes angegeben wird.

Nachdem Sie die Serverzertifikate mit **snakeyman** aktualisiert haben, müssen Sie das Programm **snakeyman** beenden und den CS-Linux-Knoten stoppen. Starten Sie dann den CS-Linux-Knoten neu, um die aktualisierten Zertifikate zu verwenden. Verwenden Sie die folgenden Befehle, um den Knoten zu stoppen und neu zu starten:

**snaadmin term_node**
**snaadmin init_node**

## Konfigurationsdateien von Communications Server für Linux sichern

Communications Server für Linux erstellt automatisch Sicherungskopien der Knoten-, Domänen- und TP-Konfigurationsdatei, wenn Sie (mit einem der CS-Linux-Verwaltungs-Tools) Änderungen vornehmen, die sich auf diese Dateien auswirken. Wenn Sie beispielsweise eine Änderung vornehmen, die Einfluss auf die Knotenkonfigurationsdatei (**sna_node.cfg**) hat, erstellt Communications Server für Linux eine Sicherungsdatei mit dem Namen **sna_node.bk***n*, wobei die Zahl *n* entweder 1 oder 2 ist.

- Ändern Sie die Datei zum ersten Mal, wird die vorhandene Konfiguration in der Datei **sna_node.bk1** gesichert.
- Ändern Sie die Datei zum zweiten Mal, wird die vorhandene Konfiguration in der Datei **sna_node.bk2** gesichert. Die Datei **sna_node.bk1** bleibt unverändert erhalten.
- Wenn Sie die Datei zum dritten Mal bzw. weitere Male ändern, wird die Datei **sna_node.bk1** gelöscht. Die Datei **sna_node.bk2** wird in **sna_node.bk1** umbenannt, und die vorhandene Konfiguration wird in der Datei **sna_node.bk2** gesichert.

Durch diesen Prozess können Sie jeweils maximal zwei Sicherungsdateien für die Knotenkonfigurationsdatei haben. Dieser Prozess generiert auch die Dateierweiterungen für andere Sicherungsdateien.

In folgenden Situationen sollten Sie zusätzlich zur automatischen Sicherung Sicherungskopien von Konfigurationsdateien erstellen, um sich vor Datenverlusten zu schützen:

- vor Installation einer neuen Version des Betriebssystems Linux
- vor Installation einer neuen Version von Communications Server für Linux
- nach Erstellung einer neuen Konfiguration

Führen Sie zum Sichern von Konfigurationsdateien die folgenden Befehle aus:

**cd /etc/opt/ibm/sna tar cvf** *Einheitenname* **sna_node.cfg sna.net sna_tps sna_domn.cfg ibmcs.***

## Sicherungskopie der Konfigurationsdateien von Communications Server für Linux zurückschreiben

Gehen Sie wie folgt vor, um die Konfigurationsdateien von Communications Server für Linux zurückzuschreiben, die Sie wie im Abschnitt „Konfigurationsdateien von Communications Server für Linux sichern" beschrieben gesichert haben:

1. Vergewissern Sie sich, dass Communications Server für Linux nicht aktiv ist. Dies können Sie durch Eingabe des folgenden Befehls überprüfen:

   **snaadmin status_node**

   Wenn Communications Server für Linux aktiv ist, zeigt der Befehl Informationen zum Status des lokalen Knotens an. Andernfalls wird die Nachricht angezeigt, dass Communications Server für Linux nicht aktiv ist.

   Sollte Communications Server für Linux aktiv sein, geben Sie zum Inaktivieren den folgenden Befehl ein:

   **sna stop**

2. Geben Sie die folgenden Befehle ein:

   **cd /etc/opt/ibm/sna tar xvf** *Einheitenname*

   Hier steht *Einheitenname* für den Pfad- und Dateinamen der Einheit, die Sie beim Sichern der Dateien verwendet haben.

   Dieser Befehl überschreibt alle Konfigurationsdateien mit demselben Namen im Verzeichnis **/etc/opt/ibm/sna**.

## Konfigurationsdateien neu initialisieren

Werden Konfigurationsdateien von Communications Server für Linux unabsichtlich geändert, so dass die darin enthaltenen Daten nicht mehr verwendet werden können, müssen Sie die Dateien möglicherweise neu initialisieren. Auf diese Weise können Sie Communications Server für Linux wieder so konfigurieren, als wäre es neu installiert. Diesen Schritt sollten Sie jedoch nur ausführen, wenn Sie sicher sind, dass die Konfigurationsdaten nicht wiederhergestellt werden können.

**Anmerkung:** Wenn Sie gültige Sicherungskonfigurationsdateien haben, können Sie diese in das Verzeichnis **/etc/opt/ibm/sna/** kopieren und für die Initialisierung des Knotens mit dem Befehl **sna start** verwenden.

Sie können die folgenden Konfigurationsdateien neu initialisieren:

- Knotenkonfigurationsdatei **sna_node.cfg**
- Domänenkonfigurationsdatei **sna_domn.cfg**
- TP-Konfigurationsdatei **sna_tps**
- SSL-Schlüsselringdatenbankdatei und Kennwort-Stash-Datei.

Führen Sie die folgenden Schritte aus, um Konfigurationsdateien neu zu initialisieren:

1. Verlassen Sie das Verwaltungsprogramm, sofern dieses aktiv ist, und inaktivieren Sie Communications Server für Linux durch Eingabe des folgenden Befehls:

   **sna stop**
2. Sichern Sie die vorhandenen Konfigurationsdateien, indem Sie alle Dateien, die Sie neu initialisieren, in ein anderes Verzeichnis kopieren.
3. Löschen Sie die neu zu initialisierenden Dateien.
4. Wenn Sie die Domänenkonfigurationsdatei gelöscht haben, geben Sie zum erneuten Erstellen dieser Datei den folgenden Befehl ein (der die zu Communications Server für Linux gelieferte leere Domänenkonfigurationsdatei kopiert):

   **cp -p /opt/ibm/sna/samples/empty.cfg /etc/opt/ibm/sna/sna_domn.cfg**

   Dieser Befehl erstellt eine neue Domänenkonfigurationsdatei, die für den Start von Communications Server für Linux erforderlich ist.
5. Wenn Sie die SSL-Schlüsselringdatenbankdatei gelöscht haben, geben Sie zum erneuten Erstellen dieser Datei den folgenden Befehl ein (der die zu Communications Server für Linux gelieferte Beispieldatei kopiert):

   **cp -p /opt/ibm/sna/samples/ibmcs.* /etc/opt/ibm/sna**
6. Geben Sie den folgenden Befehl ein, um Communications Server für Linux neu zu starten:

   **sna start**

7. Starten Sie wie folgt das Motif-Verwaltungsprogramm:

   **xsnaadmin &**

   Wenn die Datei **sna_node.cfg** nicht vorhanden ist, fordert das Verwaltungsprogramm Sie auf, den Knoten zu konfigurieren. Sie können nun den Knoten und die übrigen Ressourcen konfigurieren. Lesen Sie dazu die Informationen in Kapitel 8, „Communications Server für Linux konfigurieren und verwenden", auf Seite 71 oder im *Communications Server für Linux Verwaltungshandbuch*.

   Falls Sie eine gültige Datei **sna_node.cfg** verwendet haben, wird der Knoten mit dieser Datei initialisiert.

## Communications Server für Linux deinstallieren

Sie können das Produkt Communications Server für Linux jederzeit deinstallieren. Gehen Sie dazu wie folgt vor:

1. Melden Sie sich mit Root-Berechtigung an.
2. Vergewissern Sie sich, dass Communications Server für Linux nicht aktiv ist. Dies können Sie durch Eingabe des folgenden Befehls überprüfen:

   **snaadmin status_node**

   Wenn Communications Server für Linux aktiv ist, zeigt der Befehl Informationen zum Status des lokalen Knotens an. Andernfalls wird die Nachricht angezeigt, dass Communications Server für Linux nicht aktiv ist.

   Sollte Communications Server für Linux aktiv sein, geben Sie zum Inaktivieren den folgenden Befehl ein:

   **sna stop**
3. Entfernen Sie das CS-Linux-Paket und die zugeordneten Softwarepakete mit den folgenden Anweisungen:

   **rpm —e ibm-commserver-docs**

   **rpm —e ibm-commserver-ecl**

   **rpm —e ibm-commserver**

   **/sbin/shutdown —r now**

## Communications Server für Linux deinstallieren

# Kapitel 4. IBM Remote API Clients unter Linux installieren

Dieses Kapitel beschäftigt sich mit der Installation von IBM Remote API Client unter Linux. Mit diesem Client kann eine Linux-Workstation ohne eine vollständige SNA-Stack-Installation SNA-Anwendungen ausführen. Ein Remote API Client unter Linux kann über ein TCP/IP-Netz eine Verbindung zu CS-Linux-Servern herstellen (oder zu CS/AIX-Servern, jedoch nicht zu beiden gleichzeitig). (CS-Linux-Server können nicht in derselben Domäne wie CS/AIX-Server ausgeführt werden.)

Dieses Kapitel bezieht sich auf IBM Remote API Clients, die auf 32-Bit-Intel-Computern (i686), 64-Bit-Computern mit AMD64/Intel EM64T (x86_64) und pSeries-Computern (ppc64) ausgeführt werden. Falls Sie IBM Remote API Client auf einem System z (s390/s390x) installieren möchten, lesen Sie Kapitel 5, „IBM Remote API Clients unter Linux für System z installieren", auf Seite 47.

Das Installationsprogramm mit den zugehörigen Dateien, einschließlich der README-Datei zu IBM Remote API Client, befindet sich auf der Installations-CD im Verzeichnis für den verwendeten Client-Typ:

| Client-Typ | Verzeichnis auf der CD |
|---|---|
| 32-Bit Intel (i686) | **/ibm-commserver-clients/linux** |
| 64-Bit AMD64/Intel EM64T (x86_64) | **/ibm-commserver-clients/linux-x86_64** |
| pSeries (ppc64) | **/ibm-commserver-clients/linux—ppc64** |

Lesen Sie vor der Installation der Software die README-Datei zu IBM Remote API Client.

## Hardware- und Softwarevoraussetzungen

### Hardwarevoraussetzungen

IBM Remote API Client erfordert einen Computer, der von einer der folgenden Linux-Distributionen unterstützt wird.

Überprüfen Sie mit dem Befehl **uname -m** die CPU-Klasse Ihres Zielcomputers. In der folgenden Tabelle ist für jeden Client-Typ die entsprechende Hardware und die Antwort von **uname -m** für diese Hardware angegeben.

| Client-Typ | Hardware | Antwort von uname |
|---|---|---|
| 32-Bit Intel | 32-Bit-Intel-System mit Pentium II oder aktuellerem Prozessor oder ein Opteron-basiertes System | `i686` |
| 64-Bit AMD64/Intel EM64T | x86_64 (System mit AMD64 oder Intel EM64T) | `x86_64` |
| pSeries | pSeries POWER5 oder OpenPower-System | `ppc64` |

## Version des Betriebssystems Linux

Die aktuelle Version von IBM Remote API Client wurde mit folgenden Versionen des Betriebssystems Linux getestet. Möglicherweise kann das Produkt auch unter anderen Linux-Distributionen zufriedenstellend ausgeführt werden.

- Red Hat Enterprise Linux 3 (RHEL3): nur i686
- Red Hat Enterprise Linux 4 (RHEL4)
- SUSE Linux Enterprise Server 8 (SLES8): nur i686
- SUSE Linux Enterprise Server 9 (SLES9)
- SUSE Linux Enterprise Server 10 (SLES10)

In der Datei **README** auf der Installations-CD finden Sie ausführliche Informationen zu den optionalen Paketen, die ggf. erforderlich sind.

## Java

Falls Sie die Java-API CPI-C verwenden, benötigen Sie Java-Software. In der Datei **README** auf der Installations-CD finden Sie ausführliche Informationen hierzu.

## GSKIT

Wenn der Client mit HTTPS auf CS-Linux-Server zugreifen soll, benötigen Sie GSKIT-Software, um den HTTPS-Zugriff auf die Server über einen WebSphere-Server zu aktivieren. Die GSKIT-Software ist auf der Installations-CD enthalten. Möglicherweise benötigen Sie für die Installation dieser Software jedoch einige optionale Pakete des Betriebssystems Linux. Lesen Sie die Informationen zu benötigten optionalen Paketen in der Datei **README** auf der Installations-CD.

Falls bei Installation des Clients alle vorausgesetzten Pakete installiert sind, bezieht der weiter hinten in diesem Kapitel beschriebene Installationsprozess für den Client die GSKIT-Software mit ein. Andernfalls können Sie sie später installieren.

## Einzelheiten zur Produktinstallation anzeigen

Sie können Informationen zum Remote API Client und zu den bereits installierten zugehörigen Softwarepaketen anzeigen. Verwenden Sie den folgenden Befehl, um alle installierten Pakete aufzulisten:

**rpm -q -a**

Wenn Sie weitere Details zu einem bestimmten Paket anzeigen möchten, verwenden Sie den folgenden Befehl:

**rpm -q -i** *Paketname*

*Paketname* steht hier für den Basisnamen des installierten Pakets, z. B. **ibm-commserver-client**.

## Sprachumgebungsvariable setzen

Mit dem folgenden Befehl können Sie die Variable `LANG` auf die gewünschte Sprache setzen:

**export LANG=***Sprache*

Ersetzen Sie *Sprache* durch den Bezeichner für die gewünschte Sprache. Folgende Bezeichner können angegeben werden:

| Kennung | Sprache |
|---|---|
| **de_DE** | Deutsch |
| **en_US** | Englisch (Vereinigte Staaten) |
| **es_ES** | Spanisch |
| **fr_FR** | Französisch |
| **ja_JP** | Japanisch (PC) |
| **ko_KR** | Koreanisch |
| **pt_BR** | Portugiesisch |
| **zh_CN** | Chinesisch (vereinfacht, EUC) |
| **zh_TW** | Chinesisch (traditionell) |

## Remote API Client unter Linux installieren

Nachdem Sie die vorausgesetzte Software installiert haben, können Sie mit der Installation von IBM Remote API Client beginnen.

Falls bereits eine Vorversion von IBM Remote API Client installiert ist, führen Sie die Schritte im Abschnitt „Remote API Client unter Linux deinstallieren" auf Seite 46 aus, um das Produkt vor der Installation dieser neuen Version zu entfernen. Alle Konfigurationsdaten bleiben erhalten und werden für die neue Installation verwendet.

1. Melden Sie sich mit Root-Berechtigung an.
2. Hängen Sie die CD per Mount an und rufen Sie das angehängte Verzeichnis auf.

   **mount /dev/cdrom**
   **cd /media/cdrom**

   Ersetzen Sie für RHEL3 (nur 32-Bit-Intel-Client) **/media/cdrom** durch **/mnt/cdrom**. Wenn Sie ein DVD-Laufwerk haben, kann der Name **/media/cdrom** abweichen. Mit dem Befehl **df** können Sie feststellen, wo Linux die CD angehängt hat.
3. Rufen Sie das entsprechende Unterverzeichnis der CD auf und führen Sie das Shell-Script aus, um den Client zu installieren. Das folgende Beispiel bezieht sich auf das Unterverzeichnis **/linux** für einen 32-Bit-Intel-Client (i686). Ersetzen Sie das Verzeichnis ggf. durch **/linux-x86_64** oder **/linux-ppc64**.

   **cd ibm-commserver-clients/linux**
   **./installibmcscli**

   Das Shell-Script testet, ob bestimmte Vorbedingungen erfüllt sind, und setzt Warnungen ab, falls sie nicht erfüllt sind. Sie werden aufgefordert, die Lizenzvereinbarung zu lesen und zu akzeptieren. Erst dann installiert das Script die RPMs. Das Script installiert auch die GSKIT-Software, sofern die entsprechenden vorausgesetzten Pakete bereits installiert sind.
4. Fügen Sie die Binärverzeichnisse von IBM Remote API Client zu Ihrem PATH hinzu. Bei Bedarf können Sie Ihr Profil so ändern, dass dieser Schritt automatisch ausgeführt wird.

   **export PATH="$PATH:/opt/ibm/sna/bin"**

   **export LD_LIBRARY_PATH=/usr/lib:/opt/ibm/sna/lib**

   **export LD_RUN_PATH=/usr/lib:/opt/ibm/sna/lib**

   Für Java-CPI-C-Anwendungen sollten Sie außerdem die folgende Umgebungsvariable setzen:

   **export CLASSPATH=$CLASSPATH:/opt/ibm/sna/java/cpic.jar**

Für einige Anwendungen kann es nötig sein, die Umgebungsvariable LD_PRELOAD zu setzen. Sie sollten diesen Schritt jedoch nicht als globale Änderung in Ihr Profil aufnehmen.

**export LD_PRELOAD=/usr/lib/libpLiS.so**

5. Starten Sie IBM Remote API Client. Nach der Installation geschieht dies automatisch, wenn die Maschine neu gebootet wird. Vergewissern Sie sich, dass Sie zu diesem Zeitpunkt nicht mehr auf die Verzeichnisse der CD zugreifen.

   **cd /**
   **sna start**

**Anmerkung:** IBM Remote API Client kann erst HTTPS-Verbindungen zu Servern herstellen, wenn Sie mit dem GSKIT-Schlüsselverwaltungsprogramm das Sicherheitszertifikat für den Client konfiguriert haben. Weitere Informationen hierzu finden Sie im Abschnitt „HTTPS-Sicherheitszertifikate mit dem GSKIT konfigurieren".

Außerdem müssen Sie die Client-Netzdatendatei aktualisieren und die CS-Linux-Server angeben, zu denen der Client eine Verbindung herstellen darf, sowie den WebSphere-Server, der die HTTPS-Unterstützung bereitstellt. Weitere Details hierzu können Sie im *Communications Server für Linux Verwaltungshandbuch* im Abschnitt 'Remote API Clients verwalten' nachlesen.

## HTTPS-Sicherheitszertifikate mit dem GSKIT konfigurieren

Wenn der Client mit HTTPS auf CS-Linux-Server zugreifen soll, muss das GSKIT-Schlüsselverwaltungsprogramm installiert sein. Normalerweise wird dieses Programm zusammen mit dem Client installiert, sofern die erforderlichen vorausgesetzten Pakete des Betriebssystems Linux installiert sind. Diese sind in der Datei **README** auf der Installations-CD angegeben. Falls das GSKIT nicht zusammen mit dem Client installiert wurde, Sie jedoch inzwischen die vorausgesetzten Pakete installiert haben, können Sie die GSKIT-Software wie folgt installieren.

1. Melden Sie sich mit Root-Berechtigung an.
2. Hängen Sie die CD per Mount an und rufen Sie das angehängte Verzeichnis auf.

   **mount /dev/cdrom**
   **cd /media/cdrom**

   Ersetzen Sie für RHEL3 (nur 32-Bit-Intel-Client) **/media/cdrom** durch **/mnt/cdrom**. Wenn Sie ein DVD-Laufwerk haben, kann der Name **/media/cdrom** abweichen. Mit dem Befehl **df** können Sie feststellen, wo Linux die CD angehängt hat.
3. Rufen Sie das entsprechende Unterverzeichnis der CD auf und führen Sie das Shell-Script aus, um die GSKIT-Software zu installieren. Das folgende Beispiel bezieht sich auf das Unterverzeichnis **/linux** für einen 32-Bit-Intel-Client (i686). Ersetzen Sie das Verzeichnis ggf. durch **/linux-x86_64** oder **/linux-ppc64**.

   **cd ibm-commserver-clients/linux ./installgskit**

IBM Remote API Client kann erst HTTPS-Verbindungen zu Servern herstellen, wenn Sie mit dem GSKIT-Schlüsselverwaltungsprogramm das Sicherheitszertifikat für den Client konfiguriert haben.

Gehen Sie dazu wie folgt vor.

1. Führen Sie das GSKIT-Schlüsselverwaltungsprogramm mit dem folgenden Befehl aus:

   **/opt/ibm/sna/bin/snakeyman**

   Öffnen Sie auf der Benutzerschnittstelle des Schlüsselverwaltungsprogramms die Schlüsseldatenbankdatei **/etc/opt/ibm/sna/ibmcs.kdb**, die im CMS-Format vorliegt.
2. Das Anfangskennwort für die Schlüsseldatenbank ist `ibmcs`. Vor dem Konfigurieren der Sicherheitszertifikate **müssen** Sie dieses Kennwort ändern, damit Ihre Konfiguration geschützt bleibt. Im Kennwortänderungsdialog müssen Sie die Option 'Kennwort in einer Datei speichern?' markieren, um sicherzustellen, dass das neue Kennwort gespeichert wird und der Client die Schlüsseldatenbank öffnen kann.
3. Fordern Sie eine Kopie des CA-Zertifikats an, mit dem das Sicherheitszertifikat des Webservers signiert wurde, und installieren Sie die Kopie in der Schlüsseldatenbank. Wählen Sie dazu auf der Benutzerschnittstelle des Schlüsselverwaltungsprogramms 'Unterzeichnerzertifikate' aus und klicken Sie auf 'Hinzufügen'.
4. Falls der WebSphere-Server für das Anfordern von Client-Sicherheitszertifikaten konfiguriert ist, benötigt der Client ein Zertifikat, das von einer Zertifizierungsstelle stammt, deren eigenes Zertifikat in der Webserverdatenbank für Sicherheitszertifikate enthalten ist. Fordern Sie wie folgt neue Zertifikate an:
   a. Wählen Sie auf der Benutzerschnittstelle des Schlüsselverwaltungsprogramms 'Erstellen' -> 'Neue Zertifikatanforderung' aus und machen Sie die erforderlichen Angaben.
   b. Speichern Sie das Zertifikat, extrahieren Sie es in eine Datei und senden Sie diese an die Zertifizierungsstelle.
   c. Wenn das Zertifikat ausgestellt wurde, speichern Sie es in der Datenbank des Webservers. Wählen Sie dazu auf der Benutzerschnittstelle des Schlüsselverwaltungsprogramms 'Persönliche Zertifikate' aus und klicken Sie auf 'Empfangen'.

   Für interne Tests können Sie bis zum Empfang eines Zertifikats von der Zertifizierungsstelle ein vorläufiges selbst signiertes Client-Zertifikat erstellen. Ein solches Zertifikat bietet jedoch nicht das erforderliche Maß an Sicherheit und darf nicht auf einem Produktionssystem verwendet werden. Ein selbst signiertes Zertifikat können Sie wie folgt erstellen:
   a. Wählen Sie auf der Benutzerschnittstelle des Schlüsselverwaltungsprogramms 'Erstellen' -> 'Neues selbst unterzeichnetes Zertifikat' aus und machen Sie die erforderlichen Angaben.
   b. Speichern Sie das Zertifikat und extrahieren Sie es in eine Datei.
   c. Speichern Sie die Zertifikatdatei in der Datenbank des Webservers. Wählen Sie dazu auf der Benutzerschnittstelle des Schlüsselverwaltungsprogramms 'Persönliche Zertifikate' aus und klicken Sie auf 'Empfangen'.
5. Beenden Sie nach dem Konfigurieren der Zertifikate das GSKIT-Schlüsselverwaltungsprogram.

# Remote API Client unter Linux deinstallieren

Sie können Remote API Client unter Linux mit den folgenden Befehlen deinstallieren.

```
/opt/ibm/sna/bin/sna stop
rpm -e ibm-commserver-ptf
rpm -e ibm-commserver-docs
rpm -e ibm-commserver-ecl
rpm -e ibm-commserver-cli
rpm -e ibm-commserver
rpm -e gsk7bas
/sbin/shutdown -r now
```

Nicht alle in diesen Befehlen aufgeführten Pakete werden auf jedem System installiert sein.

Bei der Deinstallation von IBM Remote API Client unter Linux bleiben alle angepassten Konfigurationsdaten erhalten und können für nachfolgende Installationen verwendet werden.

# Kapitel 5. IBM Remote API Clients unter Linux für System z installieren

Dieses Kapitel beschäftigt sich mit der Installation von IBM Remote API Client unter Linux. Mit diesem Client kann ein System-z-Großrechner ohne eine vollständige SNA-Stack-Installation SNA-Anwendungen ausführen. Ein Remote API Client unter Linux für System z kann über ein TCP/IP-Netz eine Verbindung zu CS-Linux-Servern herstellen (oder zu CS/AIX-Servern).

Lesen Sie vor der Installation der Software die README-Datei zu IBM Remote API Client. Sie finden diese Datei auf der Installations-CD im Verzeichnis **/ibm-comm-server-clients/linux-systemz**.

## Hardware- und Softwarevoraussetzungen

### Hardwarevoraussetzungen

IBM Remote API Client erfordert ein 31-Bit- oder 64-Bit-z-System, das von einer der im Abschnitt „Version des Betriebssystems Linux" aufgelisteten Linux-Distributionen unterstützt wird.

Überprüfen Sie mit dem Befehl **uname -m** die CPU-Klasse. Der Befehl muss `s390` für eine 31-Bit-Umgebung oder `s390x` für eine 64-Bit-Umgebung zurückgeben.

### Version des Betriebssystems Linux

Die aktuelle Version von IBM Remote API Client wurde mit folgenden Versionen des Betriebssystems Linux getestet. Möglicherweise kann das Produkt auch unter anderen Linux-Distributionen zufriedenstellend ausgeführt werden.

- Red Hat Enterprise Linux 3 für S/390 (RHEL3–s390)
- Red Hat Enterprise Linux 3 für zSeries (RHEL3–s390x)
- Red Hat Enterprise Linux 4 für S/390 (RHEL4–s390)
- Red Hat Enterprise Linux 4 für zSeries (RHEL4–s390x)
- SUSE Linux Enterprise Server 8 für IBM Mainframe (SLES8–s390*)
- SUSE Linux Enterprise Server 9 für IBM Mainframe (SLES9–s390*)
- SUSE Linux Enterprise Server 10 für IBM Mainframe (SLES10–s390x)

In der Datei **README** auf der Installations-CD finden Sie ausführliche Informationen zu den optionalen Paketen, die ggf. erforderlich sind.

### Java

Falls Sie die Java-API CPI-C verwenden, benötigen Sie Java-Software. In der Datei **README** auf der Installations-CD finden Sie ausführliche Informationen hierzu.

### GSKIT

Wenn der Client mit HTTPS auf CS-Linux-Server zugreifen soll, benötigen Sie GSKIT-Software, um den HTTPS-Zugriff auf die Server über einen WebSphere-Server zu aktivieren. Die GSKIT-Software ist auf der Installations-CD enthalten. Möglicherweise benötigen Sie für die Installation dieser Software jedoch einige optio-

nale Pakete des Betriebssystems Linux. Lesen Sie die Informationen zu benötigten optionalen Paketen in der Datei **README** im Verzeichnis **/ibm-commserver-clients/linux-systemz** der Installations-CD.

Falls bei Installation des Clients alle vorausgesetzten Pakete installiert sind, bezieht der weiter hinten in diesem Kapitel beschriebene Installationsprozess für den Client die GSKIT-Software mit ein. Andernfalls können Sie sie später installieren.

## Einzelheiten zur Produktinstallation anzeigen

Sie können Informationen zum Remote API Client und zu den bereits installierten zugehörigen Softwarepaketen anzeigen. Verwenden Sie den folgenden Befehl, um alle installierten Pakete aufzulisten:

**rpm -q -a**

Wenn Sie weitere Details zu einem bestimmten Paket anzeigen möchten, verwenden Sie den folgenden Befehl:

**rpm -q -i** *Paketname*

*Paketname* steht hier für den Basisnamen des installierten Pakets, z. B. **ibm-commserver-client**.

## Sprachumgebungsvariable setzen

Mit dem folgenden Befehl können Sie die Variable `LANG` auf die gewünschte Sprache setzen:

**export LANG=***Sprache*

Ersetzen Sie *Sprache* durch den Bezeichner für die gewünschte Sprache. Folgende Bezeichner können angegeben werden:

| Kennung | Sprache |
|---|---|
| **de_DE** | Deutsch |
| **en_US** | Englisch (Vereinigte Staaten) |
| **es_ES** | Spanisch |
| **ja_JP** | Japanisch (PC) |
| **fr_FR** | Französisch |
| **ko_KR** | Koreanisch |
| **pt_BR** | Portugiesisch |
| **zh_CN** | Chinesisch (vereinfacht, EUC) |
| **zh_TW** | Chinesisch (traditionell) |

# Remote API Client unter Linux für System z installieren

Nachdem Sie die vorausgesetzte Software installiert haben, können Sie mit der Installation von IBM Remote API Client beginnen.

Falls bereits eine Vorversion von IBM Remote API Client installiert ist, führen Sie die Schritte im Abschnitt „Remote API Client unter Linux für System z deinstallieren” auf Seite 51 aus, um das Produkt vor der Installation dieser neuen Version zu entfernen. Alle Konfigurationsdaten bleiben erhalten und werden für die neue Installation verwendet.

1. Kopieren Sie die Datei **ibm-commserver-client–6.3.0.1–s390.tgz** aus dem Verzeichnis **/ibm-commserver-clients/linux-systemz** der CD-ROM auf das System z mit Linux oder verwenden Sie FTP für die Übertragung der Datei. Kopieren oder übertragen Sie die Datei im Binärmodus.
2. Melden Sie sich auf dem System z mit Linux als root an.
3. Entpacken Sie die TAR-Datei wie folgt in einem leeren temporären Verzeichnis:

   **mkdir /tmp/ibmcs**

   **cd /tmp/ibmcs**

   **tar —xzf ibm-commserver-client–6.3.0.1–s390.tgz**
4. Führen Sie wie folgt das Shell-Script **installibmcscli** aus:

   **./installibmcscli**

   Dieses Shell-Script testet, ob bestimmte Vorbedingungen erfüllt sind, und setzt Warnungen ab, falls sie nicht erfüllt sind. Das Script fordert Sie außerdem auf, die Lizenzbedingungen für Communications Server für Linux zu bestätigen. Sie können diese Eingabeaufforderung außer Kraft setzen, indem Sie den Befehl **installibmcscli** wie nachfolgend beschrieben mit zusätzlichen Parametern angeben. Nach Eingabe der vom Shell-Script angeforderten Informationen installiert das Script die **rpm**-Pakete. Das Script installiert auch die GSKIT-Software, sofern die entsprechenden vorausgesetzten Pakete bereits installiert sind.
5. Fügen Sie die Binärverzeichnisse von IBM Remote API Client zu Ihrem PATH hinzu. Bei Bedarf können Sie Ihr Profil so ändern, dass dieser Schritt automatisch ausgeführt wird.

   **export PATH=”$PATH:/opt/ibm/sna/bin”**

   **export LD_LIBRARY_PATH=/usr/lib:/opt/ibm/sna/lib**

   **export LD_RUN_PATH=/usr/lib:/opt/ibm/sna/lib**

   Wenn Sie 64-Bit-Anwendungen ausführen möchten, verwenden Sie folgende Angaben:

   **export LD_LIBRARY_PATH=/usr/lib64:/opt/ibm/sna/lib64**

   **export LD_RUN_PATH=/usr/lib64:/opt/ibm/sna/lib64**

   Für Java-CPI-C-Anwendungen sollten Sie außerdem die folgende Umgebungsvariable setzen:

   **export CLASSPATH=$CLASSPATH:/opt/ibm/sna/java/cpic.jar**

   Für einige Anwendungen kann es nötig sein, die Umgebungsvariable `LD_PRELOAD` zu setzen. Sie sollten diesen Schritt jedoch nicht als globale Änderung in Ihr Profil aufnehmen.

   **export LD_PRELOAD=/usr/lib/libpLiS.so**
6. Starten Sie IBM Remote API Client. Nach der Installation geschieht dies automatisch, wenn die Maschine neu gebootet wird. Vergewissern Sie sich, dass Sie zu diesem Zeitpunkt nicht mehr auf die Verzeichnisse der CD zugreifen.

   **cd /**
   **sna start**
7. Nach Abschluss der Installation können Sie die während der Installation erstellte Datei **tgz** sowie das temporäre Verzeichnis löschen.

**Anmerkung:** IBM Remote API Client kann erst HTTPS-Verbindungen zu Servern herstellen, wenn Sie mit dem GSKIT-Schlüsselverwaltungsprogramm das Sicherheitszertifikat für den Client konfiguriert haben. Weitere Informationen hierzu finden Sie im Abschnitt „HTTPS-Sicherheitszertifikate mit dem GSKIT konfigurieren” auf Seite 50.

Außerdem müssen Sie die Client-Netzdatendatei aktualisieren und die CS-Linux-Server angeben, zu denen der Client eine Verbindung herstellen darf, sowie den WebSphere-Server, der die HTTPS-Unterstützung bereitstellt. Weitere Details hierzu können Sie im *Communications Server für Linux Verwaltungshandbuch* im Abschnitt 'Remote API Clients verwalten' nachlesen.

## HTTPS-Sicherheitszertifikate mit dem GSKIT konfigurieren

Wenn der Client mit HTTPS auf CS-Linux-Server zugreifen soll, muss das GSKIT-Schlüsselverwaltungsprogramm installiert sein. Normalerweise wird dieses Programm zusammen mit dem Client installiert, sofern die erforderlichen vorausgesetzten Pakete des Betriebssystems Linux installiert sind. Diese sind in der Datei **README** auf der Installations-CD angegeben. Falls das GSKIT nicht zusammen mit dem Client installiert wurde, Sie jedoch inzwischen die vorausgesetzten Pakete installiert haben, können Sie die GSKIT-Software wie folgt installieren.

1. Kopieren Sie die Datei **ibm-commserver-client–6.3.0.1–s390.tgz** aus dem Verzeichnis **/ibm-commserver-clients/linux-systemz** der CD-ROM auf das System z mit Linux oder verwenden Sie FTP für die Übertragung der Datei. Kopieren oder übertragen Sie die Datei im Binärmodus.
2. Melden Sie sich auf dem System z mit Linux als root an.
3. Entpacken Sie die TAR-Datei wie folgt in einem leeren temporären Verzeichnis:

   **mkdir /tmp/ibmcs**

   **cd /tmp/ibmcs**

   **tar —xzf ibm-commserver-client–6.3.0.1–s390.tgz**
4. Führen Sie wie folgt das Shell-Script **installgskit** aus:

   **./installgskit**
5. Nach Abschluss der Installation können Sie die während der Installation erstellte Datei **tgz** sowie das temporäre Verzeichnis löschen.

IBM Remote API Client kann erst HTTPS-Verbindungen zu Servern herstellen, wenn Sie mit dem GSKIT-Schlüsselverwaltungsprogramm das Sicherheitszertifikat für den Client konfiguriert haben. Gehen Sie dazu wie folgt vor.

1. Führen Sie das GSKIT-Schlüsselverwaltungsprogramm mit dem folgenden Befehl aus:

   **/opt/ibm/sna/bin/snakeyman**

   Öffnen Sie auf der Benutzerschnittstelle des Schlüsselverwaltungsprogramms die Schlüsseldatenbankdatei **/etc/opt/ibm/sna/ibmcs.kdb**, die im CMS-Format vorliegt.
2. Das Anfangskennwort für die Schlüsseldatenbank ist `ibmcs`. Vor dem Konfigurieren der Sicherheitszertifikate **müssen** Sie dieses Kennwort ändern, damit Ihre Konfiguration geschützt bleibt. Im Kennwortänderungsdialog müssen Sie die Option 'Kennwort in einer Datei speichern?' markieren, um sicherzustellen, dass das neue Kennwort gespeichert wird und der Client die Schlüsseldatenbank öffnen kann.
3. Fordern Sie eine Kopie des CA-Zertifikats an, mit dem das Sicherheitszertifikat des Webservers signiert wurde, und installieren Sie die Kopie in der Schlüsseldatenbank. Wählen Sie dazu auf der Benutzerschnittstelle des Schlüsselverwaltungsprogramms 'Unterzeichnerzertifikate' aus und klicken Sie auf 'Hinzufügen'.

4. Falls der WebSphere-Server für das Anfordern von Client-Sicherheitszertifikaten konfiguriert ist, benötigt der Client ein Zertifikat, das von einer Zertifizierungsstelle stammt, deren eigenes Zertifikat in der Webserverdatenbank für Sicherheitszertifikate enthalten ist. Fordern Sie wie folgt neue Zertifikate an:
   a. Wählen Sie auf der Benutzerschnittstelle des Schlüsselverwaltungsprogramms 'Erstellen' -> 'Neue Zertifikatanforderung' aus und machen Sie die erforderlichen Angaben.
   b. Speichern Sie das Zertifikat, extrahieren Sie es in eine Datei und senden Sie diese an die Zertifizierungsstelle.
   c. Wenn das Zertifikat ausgestellt wurde, speichern Sie es in der Datenbank des Webservers. Wählen Sie dazu auf der Benutzerschnittstelle des Schlüsselverwaltungsprogramms 'Persönliche Zertifikate' aus und klicken Sie auf 'Empfangen'.

   Für interne Tests können Sie bis zum Empfang eines Zertifikats von der Zertifizierungsstelle ein vorläufiges selbst signiertes Client-Zertifikat erstellen. Ein solches Zertifikat bietet jedoch nicht das erforderliche Maß an Sicherheit und darf nicht auf einem Produktionssystem verwendet werden. Ein selbst signiertes Zertifikat können Sie wie folgt erstellen:
   a. Wählen Sie auf der Benutzerschnittstelle des Schlüsselverwaltungsprogramms 'Erstellen' -> 'Neues selbst unterzeichnetes Zertifikat' aus und machen Sie die erforderlichen Angaben.
   b. Speichern Sie das Zertifikat und extrahieren Sie es in eine Datei.
   c. Speichern Sie die Zertifikatdatei in der Datenbank des Webservers. Wählen Sie dazu auf der Benutzerschnittstelle des Schlüsselverwaltungsprogramms 'Persönliche Zertifikate' aus und klicken Sie auf 'Empfangen'.
5. Beenden Sie nach dem Konfigurieren der Zertifikate das GSKIT-Schlüsselverwaltungsprogram.

## Remote API Client unter Linux für System z deinstallieren

Sie können Remote API Client unter Linux für System z mit den folgenden Befehlen deinstallieren.

```
/opt/ibm/sna/bin/sna stop
rpm -e ibm-commserver-ptf
rpm -e ibm-commserver-docs
rpm -e ibm-commserver-ecl
rpm -e ibm-commserver-cli
rpm -e ibm-commserver
rpm -e gsk7bas
/sbin/shutdown -r now
```

Nicht alle in diesen Befehlen aufgeführten Pakete werden auf jedem System installiert sein.

Bei der Deinstallation von IBM Remote API Client unter Linux für System z bleiben alle angepassten Konfigurationsdaten erhalten und können für nachfolgende Installationen verwendet werden.

# Kapitel 6. IBM Remote API Clients auf AIX-Systemen installieren

Dieses Kapitel beschäftigt sich mit der Installation von IBM Remote API Client unter AIX. Mit diesem Client kann eine AIX-Workstation ohne eine vollständige SNA-Stack-Installation SNA-Anwendungen ausführen. Ein Remote API Client unter AIX kann über ein TCP/IP-Netz eine Verbindung zu CS-Linux-Servern (oder CS/AIX-Servern) herstellen.

Lesen Sie vor der Installation der Software die README-Datei zu IBM Remote API Client. Sie finden diese Datei auf der Installations-CD im Verzeichnis **/ibm-commserver-clients/aix**.

## Hardware- und Softwarevoraussetzungen

### Hardwarevoraussetzungen

IBM Remote API Client erfordert ein pSeries-System, das von einer der im Abschnitt „Betriebssystemversion" aufgelisteten Versionen des Betriebssystems AIX unterstützt wird.

### Betriebssystemversion

Die aktuelle Version von IBM Remote API Client wurde mit folgenden Betriebssystemversionen getestet.

- AIX Version 5.2 ML5
- AIX Version 5.3 ML1

### Java

Falls Sie die Java-API CPI-C verwenden, benötigen Sie Java-Software. Das unter http://www.ibm.com/developerworks/java/jdk verfügbare Java 1.4.2 SDK erfüllt alle Voraussetzungen. Möglicherweise ist auch eine 64-Bit-Java-Version verfügbar. Die API Java-CPI-C erfordert jedoch eine 32-Bit-JVM.

Installieren Sie das Java-SDK-Paket mit dem Befehl **installp**.

### GSKIT

Wenn der Client mit HTTPS auf CS-Linux-Server zugreifen soll, benötigen Sie GSKIT-Software, um den HTTPS-Zugriff auf die Server über einen WebSphere-Server zu aktivieren. In der Datei **README** im Verzeichnis **/ibm-commserver-clients/aix** der Installations-CD finden Sie ausführliche Informationen hierzu. Die GSKIT-Software wird im Rahmen des Hauptinstallationsprozesses für den Client installiert, der weiter hinten in diesem Kapitel beschrieben ist.

### Sprachumgebungsvariable ändern

Wenn Sie den Remote API Client verwenden, vergewissern Sie sich, dass die Variable `LANG` nicht auf `C` gesetzt ist.

Mit den folgenden Schritten können Sie anzeigen, welche `LANG`-Variable verwendet wird, und sie ggf. ändern:

1. Wählen Sie im SMIT-Hauptmenü **Systemumgebungen** aus.

2. Wählen Sie im nächsten SMIT-Menü **Sprachumgebung verwalten** aus.
3. Wählen Sie im nächsten SMIT-Menü **Umgebung für Primärsprache ändern/anzeigen** aus.
4. Wählen Sie im nächsten SMIT-Menü **Länderspezifische Vereinbarung, Sprache oder Tastatur ändern/anzeigen** aus.
5. Wählen Sie die gewünschte Sprache aus. Wenn Sie beispielsweise Nachrichten in Englisch (US) anzeigen möchten, wählen Sie `en_US` aus.

## Remote API Client unter AIX installieren

Nachdem Sie die vorausgesetzte Software installiert haben, können Sie mit der Installation von IBM Remote API Client beginnen.

Falls bereits eine Vorversion von IBM Remote API Client installiert ist, führen Sie die Schritte im Abschnitt „Remote API Client unter AIX deinstallieren" auf Seite 56 aus, um das Produkt vor der Installation dieser neuen Version zu entfernen. Alle Konfigurationsdaten bleiben erhalten und werden für die neue Installation verwendet.

### Dateien für die Installation von Remote API Client auf die AIX-Workstation kopieren

Führen Sie für die Installation von Remote API Client die folgenden Schritte aus.

1. Kopieren Sie die Datei **sna.client.6.3.0.1.bff** aus dem Verzeichnis **/ibm-commserver-clients/aix** der CD-ROM auf die AIX-Workstation oder verwenden Sie FTP zum Übertragen der Datei. Kopieren oder übertragen Sie die Datei im Binärmodus.

   Falls der Client HTTPS-Verbindungen zu CS-Linux-Servern herstellen soll, müssen Sie außerdem die Dateien **gskta.*.I** und **gsksa.*.I** aus dem genannten Verzeichnis der CD kopieren bzw. mit FTP übertragen. Diese Dateien enthalten die für den HTTPS-Zugriff des Clients erforderliche GSKIT-Software.
2. Melden Sie sich auf der AIX-Workstation als root an.
3. Installieren Sie den AIX-Client mit **smit** oder **installp**. Entsprechende Anweisungen finden Sie in der Datei **README** im Verzeichnis **/ibm-commserver-clients/aix** der Installations-CD.
4. Wenn der Client mit HTTPS auf CS-Linux-Server zugreifen soll, installieren Sie die GSKIT-Dateien gemäß den Anweisungen in der Datei **README**.
5. Nach Abschluss der Installation können Sie die Datei **sna.client.6.3.0.1.bff** und die GSKIT-Dateien aus dem Arbeitsverzeichnis löschen.
6. Starten Sie IBM Remote API Client. Nach der Installation geschieht dies automatisch, wenn die Maschine neu gebootet wird.

   ```
   cd /
   sna start
   ```

**Anmerkung:** IBM Remote API Client kann erst HTTPS-Verbindungen zu Servern herstellen, wenn Sie mit dem GSKIT-Schlüsselverwaltungsprogramm das Sicherheitszertifikat für den Client konfiguriert haben. Weitere Informationen hierzu finden Sie im Abschnitt „HTTPS-Sicherheitszertifikate mit dem GSKIT konfigurieren" auf Seite 55.

Außerdem müssen Sie die Client-Netzdatendatei aktualisieren und die CS-Linux-Server angeben, zu denen der Client eine Verbindung herstellen darf, sowie den WebSphere-Server, der die HTTPS-Unter-

stützung bereitstellt. Weitere Details hierzu können Sie im *Communications Server für Linux Verwaltungshandbuch* im Abschnitt 'Remote API Clients verwalten' nachlesen.

## Remote API Client von der CD installieren

Führen Sie für die Installation von Remote API Client die folgenden Schritte aus.

1. Melden Sie sich auf der AIX-Workstation als root an.
2. Hängen Sie die CD auf der AIX-Workstation mit dem folgenden Befehl an.

   **mount -o ro /dev/cd0 /mnt**
3. Installieren Sie den AIX-Client mit **smit** oder **installp**. Entsprechende Anweisungen finden Sie in der Datei **README** im Verzeichnis **/ibm-commserver-clients/aix** der Installations-CD.
4. Wenn der Client mit HTTPS auf CS-Linux-Server zugreifen soll, installieren Sie die GSKIT-Dateien gemäß den Anweisungen in der Datei **README**.
5. Hängen Sie die CD nach Abschluss des Installationsprozesses mit dem folgenden Befehl ab.

   **unmount /mnt**
6. Starten Sie IBM Remote API Client. Nach der Installation geschieht dies automatisch, wenn die Maschine neu gebootet wird. Vergewissern Sie sich, dass Sie zu diesem Zeitpunkt nicht mehr auf die Verzeichnisse der CD zugreifen.

   **cd /**
   **sna start**

**Anmerkung:** IBM Remote API Client kann erst HTTPS-Verbindungen zu Servern herstellen, wenn Sie mit dem GSKIT-Schlüsselverwaltungsprogramm das Sicherheitszertifikat für den Client konfiguriert haben. Weitere Informationen hierzu finden Sie im Abschnitt „HTTPS-Sicherheitszertifikate mit dem GSKIT konfigurieren".

Außerdem müssen Sie die Client-Netzdatendatei aktualisieren und die CS-Linux-Server angeben, zu denen der Client eine Verbindung herstellen darf, sowie den WebSphere-Server, der die HTTPS-Unterstützung bereitstellt. Weitere Details hierzu können Sie im *Communications Server für Linux Verwaltungshandbuch* im Abschnitt 'Remote API Clients verwalten' nachlesen.

## HTTPS-Sicherheitszertifikate mit dem GSKIT konfigurieren

IBM Remote API Client kann erst HTTPS-Verbindungen zu Servern herstellen, wenn Sie mit dem GSKIT-Schlüsselverwaltungsprogramm das Sicherheitszertifikat für den Client konfiguriert haben. Gehen Sie dazu wie folgt vor.

1. Führen Sie das GSKIT-Schlüsselverwaltungsprogramm mit dem folgenden Befehl aus:

   **/usr/bin/snakeyman**

   Öffnen Sie auf der Benutzerschnittstelle des Schlüsselverwaltungsprogramms die Schlüsseldatenbankdatei **/etc/sna/ibmcs.kdb**, die im CMS-Format vorliegt.
2. Das Anfangskennwort für die Schlüsseldatenbank ist `ibmcs`. Vor dem Konfigurieren der Sicherheitszertifikate **müssen** Sie dieses Kennwort ändern, damit Ihre Konfiguration geschützt bleibt. Im Kennwortänderungsdialog müssen Sie die

Option 'Kennwort in einer Datei speichern?' markieren, um sicherzustellen, dass das neue Kennwort gespeichert wird und der Client die Schlüsseldatenbank öffnen kann.

3. Fordern Sie eine Kopie des CA-Zertifikats an, mit dem das Sicherheitszertifikat des Webservers signiert wurde, und installieren Sie die Kopie in der Schlüsseldatenbank. Wählen Sie dazu auf der Benutzerschnittstelle des Schlüsselverwaltungsprogramms 'Unterzeichnerzertifikate' aus und klicken Sie auf 'Hinzufügen'.
4. Falls der WebSphere-Server für das Anfordern von Client-Sicherheitszertifikaten konfiguriert ist, benötigt der Client ein Zertifikat, das von einer Zertifizierungsstelle stammt, deren eigenes Zertifikat in der Webserverdatenbank für Sicherheitszertifikate enthalten ist. Fordern Sie wie folgt neue Zertifikate an:
   a. Wählen Sie auf der Benutzerschnittstelle des Schlüsselverwaltungsprogramms 'Erstellen' -> 'Neue Zertifikatanforderung' aus und machen Sie die erforderlichen Angaben.
   b. Speichern Sie das Zertifikat, extrahieren Sie es in eine Datei und senden Sie diese an die Zertifizierungsstelle.
   c. Wenn das Zertifikat ausgestellt wurde, speichern Sie es in der Datenbank des Webservers. Wählen Sie dazu auf der Benutzerschnittstelle des Schlüsselverwaltungsprogramms 'Persönliche Zertifikate' aus und klicken Sie auf 'Empfangen'.

   Für interne Tests können Sie bis zum Empfang eines Zertifikats von der Zertifizierungsstelle ein vorläufiges selbst signiertes Client-Zertifikat erstellen. Ein solches Zertifikat bietet jedoch nicht das erforderliche Maß an Sicherheit und darf nicht auf einem Produktionssystem verwendet werden. Ein selbst signiertes Zertifikat können Sie wie folgt erstellen:
   a. Wählen Sie auf der Benutzerschnittstelle des Schlüsselverwaltungsprogramms 'Erstellen' -> 'Neues selbst unterzeichnetes Zertifikat' aus und machen Sie die erforderlichen Angaben.
   b. Speichern Sie das Zertifikat und extrahieren Sie es in eine Datei.
   c. Speichern Sie die Zertifikatdatei in der Datenbank des Webservers. Wählen Sie dazu auf der Benutzerschnittstelle des Schlüsselverwaltungsprogramms 'Persönliche Zertifikate' aus und klicken Sie auf 'Empfangen'.
5. Beenden Sie nach dem Konfigurieren der Zertifikate das GSKIT-Schlüsselverwaltungsprogram.

## Remote API Client unter AIX deinstallieren

Sie können Remote API Client mit den folgenden Befehlen deinstallieren.

1. Falls die Client-Software aktiv ist, stoppen Sie sie mit dem folgenden Befehl.

   **sna stop**
2. Melden Sie sich mit Root-Berechtigung an.
3. Entfernen Sie das Remote-Client-Paket und die zugeordneten Softwarepakete mit einem der folgenden Befehle.

   Mit **installp** können Sie das Paket wie folgt entfernen:

   **installp —u sna.client**

   Mit **smit** können Sie das Paket wie folgt entfernen:

   **smit remove**

# Kapitel 7. Installation von Remote API Client unter Windows vorbereiten und ausführen

Dieses Kapitel beschäftigt sich mit der Installation von IBM Remote API Client unter Windows. Mit diesem Client kann ein PC ohne eine vollständige SNA-Stack-Installation SNA-Anwendungen ausführen. Ein Remote API Client unter Windows kann über ein TCP/IP-Netz eine Verbindung zu CS-Linux-Servern (oder CS/AIX-Servern) herstellen.

Es gibt zwei Varianten von IBM Remote API Client für Windows, die je nach der verwendeten Hardware und Windows-Version zum Einsatz kommen. Sofern nicht explizit etwas anderes angegeben ist, gelten die Informationen in diesem Kapitel für beide Varianten.

- Der 32-Bit-Client wird auf einem Intel-basierten 32-Bit-Computer mit Microsoft Windows 2000, 2003 oder XP ausgeführt.
- Der x64-Client wird aur einem AMD64- oder Intel-EM64T-Computer mit Microsoft Windows Server 2003 x64 Edition oder Microsoft Windows XP Professional x64 Edition ausgeführt.

Die vom IBM Remote API Client unter Windows bereitgestellten Schnittstellen sind weitestgehend mit den von IBM Communications Server für Windows und Microsoft Host Integration Server angebotenen Schnittstellen kompatibel.

Das Software Development Kit (SDK) von IBM Remote API Client ist ein optionales Paket, das die Nutzung des Remote API Client für die Entwicklung von Anwendungsprogrammen mit den APIs APPC, CPI-C, LUA und CSV ermöglicht. Weitere Informationen zu diesen APIs finden Sie in den entsprechenden Referenzhandbüchern für Programmierer. Sie müssen dieses Paket nicht installieren, wenn Sie mit dem Remote API Client nur vorhandene Anwendungen ausführen (und keine neuen entwickeln) möchten.

## Hardware- und Softwarevoraussetzungen

Für die Ausführung des **Setup**-Programms und des Remote API Client unter Windows muss der Computer die folgenden Voraussetzungen erfüllen:

- Der Computer muss eines der folgenden Betriebssysteme ausführen:
  - Für den 32-Bit-Windows-Client:
    - Windows 2000
    - Windows XP
    - Windows 2003
  - Für den x64-Windows-Client:
    - Microsoft Windows XP Professional x64 Edition
    - Microsoft Windows Server 2003 x64 Edition
- Der Computer muss mit einem der folgenden Mechanismen auf CS-Linux-Server zugreifen können:
  - Serverzugriff über ein TCP/IP-Netz
  - Zugriff auf einen WebSphere-Server, der den HTTPS-Zugriff auf CS-Linux-Server ermöglicht (In diesem Fall muss während der Client-Installation die GSKIT-Software installiert werden.)

# Zugriff auf das Setup-Programm

Remote API Client und die SDK-Software, die GSKIT-Software und das **Setup**-Programm sind im Windows-Format auf der CD enthalten. Sie können die Software demzufolge direkt von der CD auf dem Windows-Computer installieren. Sie müssen die Remote-API-Client-Software auf jedem Windows-Client-PC installieren. Das SDK ist nur erforderlich, wenn Sie den Client für die Entwicklung neuer Anwendungen mit den Windows Remote APIs nutzen möchten. Wird der Client nur für die Ausführung vorhandener Anwendungen genutzt, ist das SDK nicht erforderlich. Die GSKIT-Software ist nur erforderlich, wenn der Client mit HTTPS auf CS-Linux-Server zugreifen können soll.

Das Installationsimage für Remote API Client unter Windows ist eine selbst entpackende ausführbare ZIP-Datei auf der Installations-CD.

- Für den 32-Bit-Client ist es die Datei **i_w32cli.exe** im Verzeichnis **/ibm-commserver-clients/windows** der CD.
- Für den x64-Client ist es die Datei **i_w64cli.exe** im Verzeichnis **/ibm-commserver-clients/win-x64** der CD.

Sie können diese Datei auch auf andere Windows-PCs im Netz kopieren und dann ohne direkten Zugang zur CS-Linux-CD installieren. Wenn Sie diese ausführbare Datei ausführen, wird das Installationsimage entpackt und automatisch das **Setup**-Programm ausgeführt. Falls Sie das Installationsimage einfach in einem temporären Verzeichnis entpacken möchten, weil Sie das **Setup**-Programm beispielsweise in der Befehlszeile ausführen wollen, können Sie die selbst entpackende Datei mit dem ZIP-Programm entpacken.

Bei der erstmaligen Ausführung des **Setup**-Programms auf einem bestimmten Computer wird das Programm von der ausgewählten Quelle ausgeführt. Das Programm bearbeitet den gesamten Installationsprozess, definiert eine Basiskonfiguration und erstellt und installiert sogar ein Programmsymbol für sich selbst. Nach Abschluss der Installation können Sie das **Setup**-Programm verwenden, um die Software erneut zu installieren. (Dazu können Sie das Programm im Dateimanager auswählen oder das Programmsymbol verwenden.)

Nachdem Sie das Installationsimage für Remote API Client in einem temporären Verzeichnis entpackt haben, können Sie die Software auf eine der beiden folgenden Arten installieren:

- Führen Sie unter Windows das **Setup**-Programm aus. Dieser Prozess ist im Abschnitt „Remote API Client mit dem Setup-Programm unter Windows installieren" auf Seite 59 erläutert. Wenn Sie das SDK installieren möchten, müssen Sie diese Installationsmethode anwenden.
- Geben Sie den Befehl **setup** in der Befehlszeile ein. Gehen Sie dazu wie im Abschnitt „Remote-API-Client-Software in der Befehlszeile installieren" auf Seite 62 beschrieben vor. Bei dieser Methode haben Sie keine Möglichkeit, das SDK zu installieren.

**Anmerkung:** IBM Remote API Client kann erst HTTPS-Verbindungen zu Servern herstellen, wenn Sie die GSKIT-Software installiert und mit dem GSKIT-Schlüsselverwaltungsprogramm das Sicherheitszertifikat für den Client konfiguriert haben. Weitere Informationen hierzu finden Sie in den Abschnitten „GSKIT-Software installieren und Sicherheitszertifikate konfigurieren" auf Seite 65 und „HTTPS-Sicherheitszertifikate mit dem GSKIT konfigurieren" auf Seite 66.

Außerdem müssen Sie die Client-Netzdatendatei aktualisieren und die CS-Linux-Server angeben, zu denen der Client eine Verbindung herstellen darf, sowie den WebSphere-Server, der die HTTPS-Unterstützung bereitstellt. Weitere Details hierzu können Sie im *Communications Server für Linux Verwaltungshandbuch* im Abschnitt 'Remote API Clients verwalten' nachlesen.

## Remote API Client mit dem Setup-Programm unter Windows installieren

Sie können das Setup-Programm automatisch ausführen, indem Sie die selbst entpackende Datei **i_w32cli.exe** (32-Bit-Client) oder **i_w64cli.exe** (x64-Client) ausführen, oder manuell in der Befehlszeile. Das Programm ruft als Erstes eine Anzeige auf, in der Sie die Sprache für die Installation auswählen können.

1. Wählen Sie die Sprache aus, die Sie für die Installation und Konfiguration des Remote API Client verwenden möchten, und klicken Sie auf **OK**.

   Das Programm ruft eine Begrüßungsanzeige auf, die Sie mit dem **Setup**-Programm vertraut macht.
2. Wählen Sie **Weiter** aus, um mit der Installation fortzufahren.

   Das Programm zeigt die Softwarelizenzvereinbarung an, die Sie aufmerksam lesen sollten.
3. Wenn Sie den Lizenzbedingungen zustimmen können, wählen Sie **Akzeptieren** aus, um fortzufahren.

   Das Programm fordert Sie auf, ein Zielverzeichnis anzugeben, in dem die Dateien installiert werden sollen.
4. Geben Sie das Zielverzeichnis ein.

   Das Programm fragt Sie nach der gewünschten Art der Installation:

   **Standard**
   Wählen Sie diese Option aus, wenn Sie das SDK nicht installieren müssen. Das SDK ist nur erforderlich, wenn Sie den Client für die Entwicklung neuer Anwendungen mit den Windows Remote APIs nutzen möchten. Wird der Client nur für die Ausführung vorhandener Anwendungen genutzt, ist das SDK nicht erforderlich.

   **Developer**
   Wählen Sie diese Option aus, wenn Sie das SDK installieren müssen. Dies ist der Fall, wenn Sie den Client für die Entwicklung neuer Anwendungen mit den Windows Remote APIs nutzen möchten.

   **Anmerkung:** Wenn Sie das SDK installieren möchten, müssen Sie **Developer** auswählen.
5. Wählen Sie die Installationsart aus.

   Das Programm fordert Sie auf, den Namen des Programmordners anzugeben, in dem die Symbole für Remote API Client unter Windows angezeigt werden sollen.
6. Geben Sie den Ordnernamen ein.
7. Falls das Systemverzeichnis **.DLL**-Dateien enthält, deren Namen mit denen der von diesem **Setup**-Programm verwendeten Dateien übereinstimmen, jedoch keine Remote-API-Client-Dateien sind (z. B. Dateien einer anderen SNA-Software), fordert das Programm Sie zur Ausführung eines der folgenden Schritte auf:

- Kopieren Sie die **.DLL**-Dateien von Remote API Client über die vorhandenen **.DLL**-Dateien.
- Kopieren Sie die vorhandenen **.DLL**-Dateien in ein Verzeichnis **OTHERSNA**, das ein Unterverzeichnis des Installationsverzeichnisses sein muss. Installieren Sie dann die **.DLL**-Dateien von Remote API Client. Diese Option gibt Ihnen die Möglichkeit, die ursprüngliche Konfiguration vor der Installation von Remote API Client wiederherzustellen, falls Sie die Dateien später deinstallieren. (Lesen Sie dazu den Abschnitt „Remote-API-Client-Software deinstallieren" auf Seite 68.)
- Brechen Sie die Installation der Client-Software ab.

Wenn die **.DLL**-Dateien von Remote API Client bereits vorhanden sind, zeigt das **Setup**-Programm eine entsprechende Nachricht an. Neue **.DLL**-Dateien überschreiben die vorhandenen **.DLL**-Dateien nur, sofern die vorhandenen Dateien eine niedrigere Versionsnummer als die **.DLL**-Dateien des **Setup**-Programms haben.

8. Anschließend kopiert das **Setup**-Programm Dateien von der angegebenen Quelle und installiert sie in den vorgesehenen Verzeichnissen. Während dieses Prozesses zeigt eine Informationsleiste an, welcher Teil der Installation schon abgeschlossen ist. Die **.DLL**-Dateien werden in das Systemverzeichnis oder ein funktional entsprechendes Verzeichnis kopiert. Alle anderen Dateien werden in das Zielverzeichnis kopiert, das Sie in Schritt 2 angegeben haben. Bei jeder Dateiübertragung wird ein Eintrag in die Datei **setup.log** geschrieben, die in dem angegebenen Verzeichnis erstellt wird. Falls eine der zu überschreibenden Dateien schreibgeschützt ist oder eine Datei aus einem anderen Grund nicht kopiert werden kann, werden die neuen Dateien entfernt. Sie empfangen eine Nachricht mit der Aufforderung, sich die Datei **setup.log** anzusehen.
9. Sollte die Quelle, von der Sie das **Setup**-Programm ausführen, nicht alle erforderlichen Dateien enthalten, fordert das Programm Sie zur Eingabe eines Verzeichnisnamens auf. Geben Sie den Namen eines Verzeichnisses ein, in dem sich die erforderlichen Dateien befinden.

   Falls Ihre Angaben nicht ausreichen, um Kopien der Remote-API-Client-Dateien zu finden, ruft das Programm die Eingabeaufforderung erneut auf.
10. Wenn die erforderlichen Dateien kopiert wurden, zeigt das **Setup**-Programm das Konfigurationsfenster an.

    Die Standardkonfigurationswerte werden aus der Domänenkonfigurationsdatei übernommen. Weitere Informationen hierzu finden Sie im *Communications Server für Linux Verwaltungshandbuch*. Falls Sie diese Standardwerte nicht verwenden möchten, können Sie sie wie nachfolgend beschrieben konfigurieren:

    *Domäne*
    : Geben Sie den Namen der Client/Server-Domäne für Communications Server für Linux an.

    Die folgenden Einstellungen sind optional:

    *Servername*
    : Die Anzeige enthält eine Liste mit bis zu neun Servern, zu denen dieser Client eine Verbindung herstellen kann. Die Reihenfolge, in der die Server aufgelistet sind, ist die Reihenfolge, in der der Client diese Server auswählt. Kann der Client keine Verbindung zum ersten Server in der Liste herstellen, versucht er, eine Verbindung zum nächsten Server herzustellen.

      - Mit dem Knopf **Hinzufügen** können Sie einen neuen Server zur Liste hinzufügen.

- Wenn Sie einen Server aus der Liste entfernen möchten, wählen Sie den Server aus und klicken Sie auf den Knopf **Entfernen**.
- Zum Verschieben eines Servers innerhalb der Liste müssen Sie den Server auswählen. Verschieben Sie den Server dann mit den Verschiebungsknöpfen neben der Liste nach oben oder unten.

Wenn der Client sich in demselben privaten Netz wie die Server befindet und mit TCP/IP auf die Server zugreift, können die einzelnen Server einfach mit dem Servernamen bezeichnet werden.

Falls der Client für den Serverzugriff HTTPS verwendet, müssen Sie für jeden Server den Namen des WebSphere-Servers, der die HTTPS-Unterstützung bereitstellt, und den Namen des CS-Linux-Servers im folgenden Format angeben:

*Webservername* **:** *Servername1*

Hierfür wird vorausgesetzt, dass WebSphere für die Verwendung von HTTPS-Verbindungen am Standard-Port 443 konfiguriert ist. Falls Ihr Netzadministrator WebSphere für die Verwendung eines anderen Ports konfiguriert hat, nehmen Sie die Port-Nummer im folgenden Format auf:

*Webservername* **:** *Port-Nummer* **:** *Servername1*

Ausführliche Informationen zum Konfigurieren von WebSphere für die Unterstützung von HTTPS-Verbindungen finden Sie im Abschnitt „WebSphere Application Server konfigurieren" auf Seite 33.

*UDP-Broadcasts*
Geben Sie an, ob dieser Client UDP-Broadcasts verwendet, um eine Verbindung zu einem Server herzustellen. Bei Auswahl dieser Option sendet der Client UDP-Broadcasts über das Netz, um eine Serververbindung zu finden, und versucht nicht, direkt eine Verbindung zu einem bestimmten Server herzustellen.

Die Standardeinstellung ist die Verwendung von UDP-Broadcasts. Wenn Sie diese Einstellung ändern möchten, klicken Sie auf das Markierungsfeld.

*Erweitert*
Sie können an Stelle der vom **Setup**-Programm vorgegebenen Standardwerte zusätzliche Werte angeben. Klicken Sie dazu unten im Fenster auf den Knopf **Erweitert**. Das **Setup**-Programm zeigt das Fenster mit den erweiterten Optionen an, das erweiterte Einstellungen für die Konfiguration des Windows-Clients enthält. Die meisten Benutzer können für diese Parameter die Standardeinstellungen verwenden, so dass Sie die Einstellungen in diesem Dialog wahrscheinlich nicht ändern müssen.

Weitere Informationen zu diesen Parametern finden Sie im Abschnitt „Erweiterte Optionen für die Konfiguration von Remote API Client" auf Seite 62.

Klicken Sie auf **Hilfe**, wenn Sie weitere Informationen zu einem der Konfigurationsparameter oder zu einer der Einstellungen anzeigen möchten.

11. Klicken Sie nach Ausführung aller Schritte im Konfigurationsfenster auf **OK**. Falls die Felder dieser Anzeige nicht richtig oder vollständig ausgefüllt wurden, zeigt das **Setup**-Programm eine entsprechende Nachricht an.

12. Nach erfolgreichem Abschluss der Installation wird das Fertigstellungsfenster angezeigt. Sie können auswählen, ob nach dem Verlassen des Installationsprogramms eine der beiden folgenden Aktionen oder beide Aktionen ausgeführt werden soll(en):

    **README-Datei anzeigen**
    Anzeigen der Datei **README**

    **Client starten**
    Ausführung von CS Linux Client beginnen

    Wählen Sie **Fertig stellen** aus, um das Installationsprogramm zu verlassen.

## Erweiterte Optionen für die Konfiguration von Remote API Client

Im Fenster mit den erweiterten Optionen können Sie einige erweiterte Parameter für Remote API Client konfigurieren. Die meisten Benutzer müssen diese Parameter nicht ändern, Sie können die Standardeinstellungen bei Bedarf jedoch anpassen.

*Zeitlimit für LAN-Zugriff*
Geben Sie die Zeit in Sekunden an, die die Client-Verbindung zu einem Server inaktiv bleiben kann, bevor sie geschlossen wird. Wenn diese Option nicht markiert ist, gilt kein Zeitlimit für LAN-Zugriff (so dass die Inaktivitätszeit unbegrenzt ist). Ist dieses Feld markiert, können Sie im benachbarten Feld einen Zeitlimitwert in Sekunden eingeben. Der Mindestwert liegt bei `60` (für 60 Sekunden). Wenn Sie in diesem Feld keinen Wert oder einen Wert kleiner als `60` eingeben, verwendet der Remote API Client den Mindestwert `60`.

*Maximale Broadcast-Versuche*
Geben Sie an, wie oft der Client versuchen soll, im Broadcast-Betrieb eine Verbindung zu einem Server herzustellen. Wenn das Fenster ″Erweiterte Optionen″ aufgerufen wird, erscheint der Standardwert `5`. Der Wert in diesem Feld wird nur verwendet, wenn im Hauptkonfigurationsfenster die Option ″UDP-Broadcasts″ markiert wurde.

*Zeitlimit für Verbindungswiederherstellung*
Geben Sie die Zeit in Sekunden an, nach deren Ablauf der Client versuchen soll, erneut eine Verbindung zu einem Server herzustellen, die zuvor unterbrochen wurde. Wenn das Fenster ″Erweiterte Optionen″ aufgerufen wird, erscheint der Standardwert `200`.

Klicken Sie auf **Hilfe**, um weitere Informationen zu diesen Parametern aufzurufen.

Klicken Sie nach Ausführung aller Schritte im Fenster ″Erweiterte Optionen″ auf **OK**. Wurden alle Felder der Anzeige korrekt ausgefüllt, kehrt das **Setup**-Programm zum Konfigurationsfenster zurück. Wenn Sie einen neuen Remote API Client installieren möchten, kehren Sie zum Schritt 11 auf Seite 61 zurück. Klicken Sie andernfalls im Konfigurationsdialog auf den Knopf **OK**, um die Konfiguration abzuschließen.

## Remote-API-Client-Software in der Befehlszeile installieren

**Anmerkung:** Wenn Sie das SDK installieren möchten, müssen Sie das **Setup**-Programm verwenden. Dieses Verfahren ist im Abschnitt „Remote API Client mit dem Setup-Programm unter Windows installieren″ auf Seite 59 erläutert. Sie können das SDK nicht von der Befehlszeile aus installieren.

## Remote-API-Client-Software in der Befehlszeile installieren

Nachdem Sie das Installationsimage für den Remote API Client in einem temporären Verzeichnis entpackt haben, müssen Sie die Remote-API-Client-Software nicht mit dem **Setup**-Programm unter Windows installieren. Sie können die Software auch von der Befehlszeile aus installieren. Geben Sie in der Befehlszeile den Befehl **setup** mit den gewünschten Optionen ein. Sie können diese Optionen in Groß- oder Kleinbuchstaben eingeben und ihnen einen Schrägstrich (/) oder einen Bindestrich (-) voranstellen. Wenn ein Parameter, z. B. *Ordner*, eine Zeichenfolge mit einem Leerzeichen ist, müssen Sie diese Zeichenfolge in Anführungszeichen setzen.

Nach Eingabe des Befehls **setup** fordert das **Setup**-Programm Sie zur Eingabe der Informationen auf, die Sie nicht in der Befehlszeile angegeben haben. In den verschiedenen Phasen der Installation zeigt das Programm Bestätigungsnachrichten an. Falls Sie nicht möchten, dass das **Setup**-Programm Sie zu Eingaben auffordert, können Sie die Option **-accept -s** verwenden, um das Programm im Hintergrundmodus ausführen, in dem die Bedingungen der Softwarelizenzvereinbarung akzeptiert werden.

Nachfolgend sind die Optionen für den Befehl **setup** aufgelistet:

**-?** Zeigt eine Liste der Befehlszeilenoptionen an. Diese Option ist identisch mit der Option **-h**.

**-h** Zeigt eine Liste der Befehlszeilenoptionen an. Diese Option ist identisch mit der Option **-?**.

**-accept -s**
Führt die Installation im Hintergrundmodus aus. Die Bedingungen der Softwarelizenzvereinbarung werden akzeptiert. Sie finden diese Vereinbarung im Unterverzeichnis **license** des Windows-Installationsimages.

Die Option **-s** muss als letzte Option in der Befehlszeile angegeben werden. Vergewissern Sie sich, dass Sie davor den Domänennamen (mit der Option **-i**) sowie alle weiteren gewünschten Parameter angegeben haben. Wenn die Installation im Hintergrundmodus ausgeführt wird, werden weder Aufforderungen zur Eingabe von Parametern noch Bestätigungsnachrichten angezeigt. Alle Befehlszeilenargumente nach **-s** werden ignoriert.

**-f2** Geben Sie den vollständigen Pfadnamen der Installationsprotokolldatei an, die während der Installation im Hintergrundmodus (angegeben mit der Option **-s**) erstellt wird.

Wenn Sie diese Option nicht angeben, wird die Datei mit dem Namen **setup.log** in dem Verzeichnis erstellt, in dem Sie das Installationsprogramm ausführen. Falls Sie die Hintergrundinstallation vom CD-ROM-Laufwerk ausführen, müssen Sie diese Option angeben, um sicherzustellen, dass die Datei auf Ihrem Computer erstellt wird. (Auf dem CD-ROM-Laufwerk kann die Datei nicht erstellt werden.)

**-k***Ordner*
Geben Sie den Programmordner an.

**-p***Verzeichnis*
Geben Sie das Installationsverzeichnis an.

**-i***Domäne*
Geben Sie den Domänennamen für diesen Client an. Dieser Parameter ist erforderlich, weil es keinen Standardwert gibt.

**-w***Verzeichnis*
Geben Sie das Quellenverzeichnis mit den Softwaredateien von CS Linux Client an, sofern sich die Quelle auf einer Platte oder CD befindet. Verwenden Sie andernfalls die Option **-v**.

**-v***Server*
Geben Sie den Server an, von dem die Client-Softwaredateien heruntergeladen werden sollen. Sie können den Servernamen oder die TCP/IP-Adresse angeben. Falls Sie die Quellendateien von einer Platte oder CD kopieren, verwenden Sie an Stelle der Option **-v** die Option **-w**.

**-l***Server*
Geben Sie einen Server an, der in die Liste der Server aufgenommen werden soll, auf die dieser Client zugreifen kann.

Wenn der Client sich in demselben privaten Netz wie die Server befindet und mit TCP/IP auf die Server zugreift, können die einzelnen Server einfach mit dem Servernamen bezeichnet werden.

Falls der Client für den Serverzugriff HTTPS verwendet, müssen Sie für jeden Server den Namen des WebSphere-Servers, der die HTTPS-Unterstützung bereitstellt, und den Namen des CS-Linux-Servers im folgenden Format angeben:

*Webservername* **:** *Servername1*

Hierfür wird vorausgesetzt, dass WebSphere für die Verwendung von HTTPS-Verbindungen am Standard-Port 443 konfiguriert ist. Falls Ihr Netzadministrator WebSphere für die Verwendung eines anderen Ports konfiguriert hat, nehmen Sie die Port-Nummer im folgenden Format auf:

*Webservername* **:** *Port-Nummer* **:** *Servername1*

Ausführliche Informationen zum Konfigurieren von WebSphere für die Unterstützung von HTTPS-Verbindungen finden Sie im Abschnitt „WebSphere Application Server konfigurieren" auf Seite 33.

**-o** Überschreibt vorhandene **.DLL**-Dateien. Wenn die **.DLL**-Dateien des Remote API Client bereits vorhanden sind, überschreibt das **Setup**-Programm diese Dateien auch dann, wenn sie eine höhere Versionsnummer als die **.DLL**-Dateien des **Setup**-Programms haben.

**-y** Sichert vorhandene **.DLL**-Dateien. Wenn die **.DLL**-Dateien des Remote API Client bereits in den entsprechenden Verzeichnissen vorhanden sind, kopiert das **Setup**-Programm die vorhandenen **.DLL**-Dateien in ein Unterverzeichnis des Installationsverzeichnisses, bevor es die **.DLL**-Dateien des Remote API Client installiert. Die Kopien in dem Unterverzeichnis stellen sicher, dass eine vollständige Deinstallation der Software Remote API Client möglich ist.

**-n** Bricht die Installation ab, falls vorhandene **.DLL**-Dateien des Remote API Client gefunden werden.

**-a***Zeitlimit*
Geben Sie das Zeitlimit für LAN-Zugriff in Sekunden an. Eine inaktive Client-Verbindung zu einem Server wird nach Ablauf dieses Zeitlimits geschlossen. Der Wert `0` gibt an, dass kein Zeitlimit gilt.

**-b***max. Broadcast-Versuche*
Geben Sie die maximale Anzahl von UDP-Broadcast-Versuchen an. Ein

UDP-Broadcast ist der Versuch eines Clients, einen beliebigen Server in der Domäne zu erreichen. Der Wert `0` gibt an, dass keine Broadcast-Versuche gestartet werden.

**-j***Zeitlimit für Verbindungswiederherstellung*
Geben Sie die Zeit in Sekunden an, nach deren Ablauf der Client versuchen soll, erneut eine Verbindung zu einem Server herzustellen, die zuvor unterbrochen wurde.

## GSKIT-Software installieren und Sicherheitszertifikate konfigurieren

**Anmerkung:** Das erste Release von x64 Remote API Client für Windows unterstützt keine HTTPS-Verbindungen zu Servern. Dieses Feature wird mit ausführlichen Installations- und Konfigurationsanweisungen in einer vorläufigen Programmkorrektur (PTF) bereitgestellt. Die folgenden Anweisungen gelten nur für 32-Bit-Clients.

Wenn der IBM Remote API Client für die Verbindung zu Servern HTTPS verwendet, müssen Sie die GSKIT-Software zur Verwaltung der Sicherheitszertifikate installieren. Führen Sie dazu die folgenden Schritte aus.

1. Erstellen Sie auf dem Windows-Computer ein temporäres Verzeichnis für die Installationsdateien.
2. Für den 32-Bit-Client:
   - Kopieren Sie die Datei **gsk7bas.exe** aus dem Verzeichnis **/ibm-commserver-clients/windows** der Installations-CD in das temporäre Verzeichnis.
   - Rufen Sie in einem Befehlsfenster das temporäre Verzeichnis auf.
   - Führen Sie zum Entpacken der Installationsdateien den folgenden Befehl aus:

     **gsk7bas** *temporäres_Verzeichnis* /D

     Hier steht *temporäres_Verzeichnis* für den vollständigen Pfad des temporären Verzeichnisses.
   - Führen Sie zum Starten des Installationsprogramms den folgenden Befehl aus:

     **setup sxclient**
3. Führen Sie die auf dem Bildschirm angezeigten Anweisungen für die Installation der GSKIT-Software aus.
4. Entfernen Sie nach Abschluss der Installation das im ersten Schritt erstellte temporäre Verzeichnis und dessen Inhalt.

Jetzt können Sie die Sicherheitszertifikate wie im folgenden Abschnitt beschrieben konfigurieren.

Falls Sie auf 32-Bit-Clients eine nicht überwachte Installation ausführen müssen (weil Sie die GSKIT-Software beispielsweise auf vielen Client-Computern installieren müssen und zur Automatisierung des Prozesses eine Stapeldatei erstellen möchten), verwenden Sie den folgenden Befehl, um das Installationsprogramm im Hintergrundmodus auszuführen:

**setup gskit -s -f1** *"temporäres_Verzeichnis*\SETUP.ISS"

Hier steht *temporäres_Verzeichnis* für den vollständigen Pfad des im ersten Schritt erstellten temporären Verzeichnisses.

Dieser Befehl installiert die Software ohne Anzeige der Benutzerschnittstelle des Installationsprogramms und fordert keine Benutzereingaben an. Die Standardeinstellungen für die Installation werden aus der Datei **SETUP.ISS** übernommen. Dies ist eine der Dateien, die Sie zu Beginn des Installationsprozesses im temporären Verzeichnis entpackt haben. Falls Sie das Installationsverzeichnis für die GSKIT-Software ändern müssen, können Sie die Datei **SETUP.ISS** in einem Texteditor bearbeiten, nachdem Sie die Dateien im temporären Verzeichnis entpackt haben. Anschließend können Sie die Dateien in diesem Verzeichnis, einschließlich der aktualisierten ISS-Datei, für die Installation auf anderen Client-Computern verwenden und müssen nicht jedes Mal die Dateien neu entpacken und das Installationsverzeichnis anpassen.

## HTTPS-Sicherheitszertifikate mit dem GSKIT konfigurieren

IBM Remote API Client kann erst HTTPS-Verbindungen zu Servern herstellen, wenn Sie mit dem GSKIT-Schlüsselverwaltungsprogramm das Sicherheitszertifikat für den Client konfiguriert haben. Gehen Sie dazu wie folgt vor.

1. Führen Sie das GSKIT-Schlüsselverwaltungsprogramm aus (*Installationsverzeichnis***snakeyman.exe**). *Installationsverzeichnis* steht hier für das Verzeichnis, in dem Sie die Client-Software installiert haben. Wenn Sie während der Client-Installation kein anderes Verzeichnis angegeben haben, ist dies das Verzeichnis **C:\IBMCS\w32cli** (32-Bit-Client).

   Öffnen Sie auf der Benutzerschnittstelle des Schlüsselverwaltungsprogramms die Schlüsseldatenbankdatei *Installationsverzeichnis***ibmcs.kdb**, die im CMS-Format vorliegt.
2. Das Anfangskennwort für die Schlüsseldatenbank ist `ibmcs`. Vor dem Konfigurieren der Sicherheitszertifikate **müssen** Sie dieses Kennwort ändern, damit Ihre Konfiguration geschützt bleibt. Im Kennwortänderungsdialog müssen Sie die Option 'Kennwort in einer Datei speichern?' markieren, um sicherzustellen, dass das neue Kennwort gespeichert wird und der Client die Schlüsseldatenbank öffnen kann.
3. Fordern Sie eine Kopie des CA-Zertifikats an, mit dem das Sicherheitszertifikat des Webservers signiert wurde, und installieren Sie die Kopie in der Schlüsseldatenbank. Wählen Sie dazu auf der Benutzerschnittstelle des Schlüsselverwaltungsprogramms 'Unterzeichnerzertifikate' aus und klicken Sie auf 'Hinzufügen'.
4. Falls der WebSphere-Server für das Anfordern von Client-Sicherheitszertifikaten konfiguriert ist, benötigt der Client ein Zertifikat, das von einer Zertifizierungsstelle stammt, deren eigenes Zertifikat in der Webserverdatenbank für Sicherheitszertifikate enthalten ist. Fordern Sie wie folgt neue Zertifikate an:
   a. Wählen Sie auf der Benutzerschnittstelle des Schlüsselverwaltungsprogramms 'Erstellen' -> 'Neue Zertifikatanforderung' aus und machen Sie die erforderlichen Angaben.
   b. Speichern Sie das Zertifikat, extrahieren Sie es in eine Datei und senden Sie diese an die Zertifizierungsstelle.
   c. Wenn das Zertifikat ausgestellt wurde, speichern Sie es in der Datenbank des Webservers. Wählen Sie dazu auf der Benutzerschnittstelle des Schlüsselverwaltungsprogramms 'Persönliche Zertifikate' aus und klicken Sie auf 'Empfangen'.

   Für interne Tests können Sie bis zum Empfang eines Zertifikats von der Zertifizierungsstelle ein vorläufiges selbst signiertes Client-Zertifikat erstellen. Ein solches Zertifikat bietet jedoch nicht das erforderliche Maß an Sicherheit und darf nicht auf einem Produktionssystem verwendet werden.

Ein selbst signiertes Zertifikat können Sie wie folgt erstellen:

a. Wählen Sie auf der Benutzerschnittstelle des Schlüsselverwaltungsprogramms 'Erstellen' -> 'Neues selbst unterzeichnetes Zertifikat' aus und machen Sie die erforderlichen Angaben.
b. Speichern Sie das Zertifikat und extrahieren Sie es in eine Datei.
c. Speichern Sie die Zertifikatdatei in der Datenbank des Webservers. Wählen Sie dazu auf der Benutzerschnittstelle des Schlüsselverwaltungsprogramms 'Persönliche Zertifikate' aus und klicken Sie auf 'Empfangen'.

5. Beenden Sie nach dem Konfigurieren der Zertifikate das GSKIT-Schlüsselverwaltungsprogram.

## Remote-API-Client-Software nach der Installation anpassen

Nach der Erstinstallation können Sie die anpassbaren Einstellungen der Software jederzeit mit dem **Konfigurationsdienstprogramm** ändern. Sie finden dieses Programm in der CS-Linux-Programmgruppe. Das Programm zeigt das gleiche Konfigurationsfenster wie beim Installationsprozess an. Sie können die Angaben in den Feldern ändern. Gehen Sie dazu wie im Abschnitt „Remote API Client mit dem Setup-Programm unter Windows installieren" auf Seite 59 beschrieben vor.

Falls Sie während der Erstinstallation nicht die SDK-Dateien installiert haben und diese jetzt hinzufügen möchten, müssen Sie erneut das Setup-Programm ausführen. Wählen Sie als Installationsart **Benutzerdefiniert** aus. Wählen Sie dann das SDK-Paket aus.

## Remote-API-Client-Software erneut installieren

Sie können die Remote-API-Client-Software jederzeit neu installieren, z. B., wenn Sie ein Softwareupgrade durchführen möchten.

Führen Sie dazu das Setup-Programm wie üblich aus. Sie können sich dabei auf die Anweisungen im Abschnitt „Remote API Client mit dem Setup-Programm unter Windows installieren" auf Seite 59 oder im Abschnitt „Remote-API-Client-Software in der Befehlszeile installieren" auf Seite 62 stützen. Das **Setup**-Programm zeigt das Verzeichnis an, von dem die Client-Softwaredateien während der Erstinstallation kopiert wurden. Klicken Sie auf **OK**, um neue Kopien der Dateien aus demselben Verzeichnis abzurufen. Wenn Sie auf **OK** klicken, kopiert das **Setup**-Programm die Dateien und ruft erneut die Anzeige mit den Optionen auf.

**Anmerkung:** Wenn Sie die erneute Installation der Remote-API-Client-Software im Hintergrundmodus ausführen (siehe Abschnitt „Remote-API-Client-Software in der Befehlszeile installieren" auf Seite 62), müssen Sie den Computer möglicherweise neu starten, um die Installation abzuschließen. Dies ist notwendig, wenn einige der Programmdateien während der Installation verwendet werden (z. B., wenn Remote API Client ausgeführt wird) und nicht durch die neuen Dateien ersetzt werden können. In diesem Fall werden die neuen Dateien in ein temporäres Verzeichnis kopiert und nach dem Neustart des Computers automatisch in das Zielverzeichnis verschoben.

Sie können überprüfen, ob der Computer neu gestartet werden muss. Sehen Sie sich dazu in einem Texteditor wie **Notepad** den Inhalt der Installationsprotokolldatei an, wenn der Installationsprozess beendet ist. Die Installationsprotokolldatei heißt **setup.log** und wird in dem Verzeichnis erstellt, von dem aus das Setup-Programm ausgeführt wurde, sofern Sie nicht mit der Befehlszeilenoption **-f2** einen anderen Pfad- und Dateinamen angegeben haben.

Am Ende der Datei finden Sie unter der Überschrift `Response Result` die Zeile `Result Code`, auf die einer der Werte `0` (null) oder `-12` folgt. Lautet der Wert `0`, müssen Sie den Computer nicht neu starten. Wenn der Wert `-12` ist, starten Sie den Computer neu, bevor Sie versuchen, den Windows-Client zu verwenden.

## Remote-API-Client-Software deinstallieren

Sie können die Remote-API-Client-Software jederzeit deinstallieren. Wählen Sie dazu in der Systemsteuerung von Windows die Option **Software > Programme ändern oder entfernen** aus. Sobald Sie die Deinstallation bestätigt haben, führt Windows die folgenden Schritte aus:

- Es werden alle installierten Dateien gelöscht.
- Falls während der Erstinstallation **.DLL**-Dateien in einem Unterverzeichnis gespeichert wurden, werden diese in ihr ursprüngliches Verzeichnis zurückgestellt.
- Es wird das Unterverzeichnis gelöscht, in dem die gespeicherten **.DLL**-Dateien abgelegt wurden, sobald das Verzeichnis leer ist.
- Der Programmordner und das erstellte Verzeichnis werden entfernt, wenn sie leer sind.
- Wenn die Deinstallation fehlerfrei verlaufen ist, wird die Datei **setup.log** gelöscht, die Einträge zur Übertragung und zum Löschen aller Dateien enthält.
- Es wird eine Nachricht angezeigt, ob die Deinstallation ordnungsgemäß abgeschlossen wurde oder ob der Benutzer die Datei **setup.log** prüfen soll, weil ein Teil der Deinstallation gescheitert ist.

Wenn Sie auf den Knopf **Beenden** klicken, kehrt das System zu Windows zurück.

Falls Sie die GSKIT-Software nur für den Windows Remote API Client (32-Bit-Client) installiert haben und diese Software von keinen anderen Anwendungen genutzt wird, können Sie sie ebenfalls deinstallieren. Eine diesbezügliche Beschreibung finden Sie im Abschnitt „GSKIT-Software deinstallieren” auf Seite 69.

## GSKIT-Software deinstallieren

Falls Sie die GSKIT-Software nur für den Windows Remote API Client (32-Bit-Client) installiert haben und diese Software von keinen anderen Anwendungen genutzt wird, können Sie sie nach der Deinstallation des Windows Remote API Client ebenfalls deinstallieren. Gehen Sie dazu wie folgt vor.

1. Rufen Sie in einem Befehlsfenster das Verzeichnis auf, in dem Windows installiert ist. Normalerweise ist dies das Verzeichnis **C:\Windows**.
2. Führen Sie den folgenden Befehl aus:

   **gskbui sxclient**

Falls das GSKIT von keiner anderen Anwendung genutzt wird, entfernt Windows die Dateien. Wenn das GSKIT noch von Anwendungen genutzt wird, bleiben die Dateien installiert, bis diese Anwendungen ebenfalls deinstalliert wurden.

## Hilfe

Falls Sie Hilfe benötigen, können Sie jederzeit über die Taste **F1** Hilfetexte aufrufen. Im Konfigurationsfenster und im Fenster ″Erweiterte Optionen″ gibt es außerdem einen Knopf **Hilfe**.

# Kapitel 8. Communications Server für Linux konfigurieren und verwenden

Der einfachste Weg, die CS-Linux-Konfiguration zu definieren und zu ändern, ist die Verwendung des Motif-Verwaltungsprogramms (**xsnaadmin**). Dieses Programm stellt eine grafische Benutzerschnittstelle bereit, über die Sie SNA-Ressourcen auf dem lokalen Knoten anzeigen und verwalten können. Sie können auch andere Verwaltungs-Tools verwenden, z. B. das Befehlszeilenverwaltungsprogramm. Wir empfehlen Ihnen jedoch, mit dem Motif-Programm zu arbeiten.

Das Motif-Verwaltungsprogramm stellt Hilfeanzeigen mit übersichtlichen Informationen zu SNA und Communications Server für Linux, Referenzinformationen zu CS-Linux-Dialoganzeigen und Anleitungen zur Ausführung bestimmter Aufgaben bereit. Das Programm führt Sie mit Menüs durch die Konfiguration der notwendigen Ressourcen. Es gibt Menüs für jede Aufgabe (z. B. die Konfiguration des Knotens) und jede Übertragungsart (z. B. TN3270 oder APPC).

Mit dem Motif-Verwaltungsprogramm können Sie alle erforderlichen Parameter für Standardkonfigurationen von Communications Server für Linux definieren. Für erweiterte Parameter gibt das Motif-Verwaltungsprogramm Standardwerte vor. Sie müssen nur die grundlegenden Konfigurationsdaten angeben und können so die SNA-Kommunikation schnell und einfach konfigurieren.

Mit dem Motif-Verwaltungsprogramm können Sie außerdem das aktive CS-Linux-System verwalten. Das Verwaltungsprogramm bietet Ihnen die Möglichkeit, die Konfiguration zu ändern, während Communications Server für Linux aktiv ist. In diesem Programm können Sie auch auf komfortable Weise Statusinformationen zu den Knotenressourcen aufrufen.

Das Motif-Verwaltungsprogramm zeigt automatisch Statusinformationen zu CS-Linux-Ressourcen an. Die meisten dieser Informationen werden im Knotenfenster angezeigt (siehe Abschnitt „Communications Server für Linux mit dem Motif-Verwaltungsprogramm verwalten" auf Seite 74). Über die Knöpfe **Starten** und **Stoppen** des Knotenfensters können sie außerdem bestimmte Ressourcen wie Knoten und Verbindungsstationen steuern. Andere Ressourcen werden immer automatisch aktiviert und inaktiviert, so dass Sie sie nicht manuell steuern müssen.

**Anmerkung:**

1. Wenn Sie Ressourcen für Communications Server für Linux definieren oder ändern möchten, müssen Sie zur Anmeldegruppe `sna` gehören.
2. Für die Verwendung des Motif-Verwaltungsprogramms brauchen Sie ein X-Terminal.
3. Zusätzliche Informationen zur Benutzerschnittstelle des Motif-Verwaltungsprogramms, z. B. zu den in den Fenstern angezeigten Knöpfen und Symbolen, können Sie den Hilfetextanzeigen des Programms und dem *Communications Server für Linux Verwaltungshandbuch* entnehmen.

4. In Abhängigkeit davon, welche Option Sie in einer bestimmten Dialoganzeige ausgewählt haben, können sich die Fenster und Dialoganzeigen des Motif-Verwaltungsprogramms von den in diesem Handbuch abgebildeten unterscheiden.

Informationen zu weiteren CS-Linux-Verwaltungs-Tools (u. a. zum Befehlszeilenverwaltungsprogramm und zu NOF-Anwendungsprogrammen) finden Sie im *Communications Server für Linux Verwaltungshandbuch*, im Handbuch *Communications Server for Linux Administration Command Reference* oder im *Communications Server for Linux NOF Programmer's Guide*.

## CS-Linux-Konfiguration planen

Es ist sehr wichtig, dass Sie jede Konfigurationsänderung vor ihrer Ausführung sorgfältig planen. Von Ihnen vorgenommene Änderungen können die Arbeit der Benutzer des lokalen Knotens und unter Umständen sogar aller Benutzer im gesamten Netz unterbrechen.

Eine gute Hilfe ist eine grafische Übersicht über alle Änderungen, die Sie an der Topologie des Netzes vornehmen. Wenn Sie Verbindungen zu anderen Knoten hinzufügen oder entfernen, zeichnen Sie eine Skizze des lokalen Knotens und der anderen Knoten. Über das Motif-Verwaltungsprogramm können Sie Informationen zu allen vorhandenen Verbindungen aufrufen und diese in Ihre grafische Übersicht aufnehmen.

Wenn Sie Ihre Übersicht durch neue Ressourcen ergänzen, können Sie leicht feststellen, ob diese Ressourcen eventuell schon vorhanden sind oder Namenskonflikte auftreten. Ihre grafische Übersicht unterstützt Sie bei der Entscheidung, welche Ressourcen entfernt werden müssen, und hilft verhindern, dass Sie unbedingt erforderliche Ressourcen löschen.

Wenn Sie ein CS-Linux-Client/Server-System mit mehreren Knoten konfigurieren, vergewissern Sie sich, dass alle CS-Linux-Knoten mit den zugehörigen Konnektivitätsressourcen in Ihre grafische Übersicht aufgenommen wurden. Anschließend können Sie jeden Knoten wie in diesem Kapitel beschrieben konfigurieren, als wäre er ein eigenständiger Knoten.

Sobald Sie Klarheit darüber gewonnen haben, welche Änderungen nötig sind, sollten Sie die entsprechenden Konfigurationsdaten zusammenstellen. Mit Hilfe der Aufgabenblätter in der Onlinehilfe des Motif-Verwaltungsprogramms und der Planungsblätter im *Communications Server für Linux Verwaltungshandbuch* können Sie feststellen, welche Konfigurationsdaten Sie für bestimmte CS-Linux-Funktionen erfassen müssen.

Im vorliegenden Kapitel finden Sie Anweisungen für das Konfigurieren der am häufigsten verwendeten Funktionen von Communications Server für Linux. Zu jeder Konfigurationsaufgabe sind die Informationen angegeben, die Sie zusammenstellen müssen, bevor Sie die Ressource konfigurieren.

**Anmerkung:** Dieses Handbuch enthält keine ausführliche Beschreibung der Konfigurationsdaten, die Sie in den Dialoganzeigen von Communications Server für Linux eingeben müssen. Weitere Informationen zu den Feldern einzelner Dialoganzeigen finden Sie in den Texten der Onlinehilfe des Motif-Verwaltungsprogramms.

## Planungsblätter

Bevor Sie mit dem Konfigurieren von Ressourcen für Communications Server für Linux beginnen, müssen Sie alle Konfigurationsdaten für die neuen Ressourcen zusammenstellen. Verwenden Sie zum Erfassen der Daten für eine bestimmte Funktion oder Anwendung die im *Communications Server für Linux Verwaltungshandbuch* enthaltenen Planungsblätter.

Möglicherweise müssen Sie Informationen von verschiedenen Quellen anfordern, z. B. von Netzadministratoren, Hostadministratoren, Anwendungsprogrammierern und Endbenutzern.

Wenn Sie versuchen, eine Verbindung zu einem anderen Knoten herzustellen, ist der Administrator dieses Knotens Ihr erster und wichtigster Ansprechpartner. Der Administrator eines Knotens kann Ihnen Namen, Adressen und Kenndaten aller Ressourcen auf diesem Knoten nennen. Oft müssen Sie sicherstellen, dass auf dem lokalen und dem fernen Knoten übereinstimmende Konfigurationsparameter eingegeben werden.

## Aufgabenblätter

Die Onlinehilfe des Motif-Verwaltungsprogramms enthält Aufgabenblätter mit einer Anleitung für bestimmte Konfigurationsaufgaben. In den Aufgabenblättern finden Sie Zeiger auf alle Hilfeanzeigen zu den Dialogen, in denen Sie die Konfigurationsdaten eingeben müssen. Mit diesen Aufgabenblättern können Sie die Hilfetexte durchblättern und genau feststellen, welche Daten zu erfassen sind.

Die Aufgabenblätter enthalten außerdem Verweise auf ausführlichere Hilfetexte zu den einzelnen Fenstern und Dialoganzeigen, die Sie zum Eingeben der Konfigurationsdaten verwenden müssen. In diesen Hilfeanzeigen ist jedes einzelne Feld, das Sie auswählen oder in dem Sie einen Wert eingeben müssen, erläutert.

# Motif-Verwaltungsprogramm verwenden

Bevor Sie das Motif-Verwaltungsprogramm verwenden, sollten Sie zu Ihrer Datei **.login** oder **.profile** Pfadangaben hinzufügen, damit das System ausführbare Programme finden kann (siehe Abschnitt „Pfad zu CS-Linux-Programmen angeben"). Darüber hinaus müssen Sie die Software Communications Server für Linux aktivieren, bevor Sie das Verwaltungsprogramm verwenden können (siehe Abschnitt „Communications Server für Linux aktivieren" auf Seite 74).

Informationen zum Aufrufen des Motif-Verwaltungsprogramms und einen Überblick über die Verwendung des Programms finden Sie im Abschnitt „Communications Server für Linux mit dem Motif-Verwaltungsprogramm verwalten" auf Seite 74.

## Pfad zu CS-Linux-Programmen angeben

Voraussetzung für die Ausführung von CS-Linux-Programmen ist, dass Sie den Pfad zu dem Verzeichnis angeben, das die ausführbaren CS-Linux-Programme enthält. Sie können den Pfad angeben, indem Sie vor der ersten Ausführung der Programme das Verzeichnis zur Umgebungsvariablen `PATH` hinzufügen oder indem Sie bei jedem Aufruf der Programme den Verzeichnisnamen mit angeben.

Das Motif-Verwaltungsprogramm ist im Verzeichnis **/opt/ibm/sna/bin/X11** gespeichert. Die übrigen Programme befinden sich im Verzeichnis **/opt/ibm/sna/bin**. Wenn Sie diese Verzeichnisse zur Definition der Umgebungsvariablen `PATH` in Ihrer

Datei **.login** oder **.profile** hinzufügen, findet Communications Server für Linux die Programme automatisch. Alternativ dazu können Sie wie in den folgenden Beispielen den Verzeichnisnamen angeben, wenn Sie das Programm ausführen:

**/opt/ibm/sna/bin/sna start**

**/opt/ibm/sna/bin/X11/xsnaadmin**

Bei den in diesem Handbuch angegebenen Beispielbefehlszeilen wird davon ausgegangen, dass Sie die Verzeichnisse zur Umgebungsvariablen `PATH` hinzugefügt haben und die Verzeichnisnamen nicht jedes Mal eingeben müssen.

## Communications Server für Linux aktivieren

Sie können den lokalen Knoten erst konfigurieren oder verwalten, nachdem Sie Communications Server für Linux auf dem lokalen System aktiviert haben. Wie bei allen X/Motif-Anwendungen müssen Sie gegebenenfalls die Umgebungsvariable `DISPLAY` definieren, um einen geeigneten X-Server anzugeben.

Geben Sie zum Aktivieren von Communications Server für Linux an der Linux-Eingabeaufforderung den folgenden Befehl ein:

**sna start**

Bei der Installation von Communications Server für Linux aktualisiert das Installationsdienstprogramm automatisch die Startdatei **/etc/rc.d/init.d/snastart** und fügt einen Eintrag für den Befehl **sna start** hinzu. Damit wird sichergestellt, dass Communications Server für Linux beim Systemstart automatisch gestartet wird. Falls Sie nicht möchten, dass Communications Server für Linux automatisch gestartet wird, können Sie diese Zeile löschen oder auf Kommentar setzen und dann die in diesem Abschnitt enthaltenen Anweisungen für das manuelle Aktivieren der Software Communications Server für Linux ausführen.

Communications Server für Linux schreibt Nachrichten auf die Standardfehlerausgabe (in der Regel der Bildschirm Ihres Terminals) und gibt so an, ob die Initialisierung erfolgreich verläuft.

## Communications Server für Linux mit dem Motif-Verwaltungsprogramm verwalten

Stellen Sie vor Verwendung des Motif-Verwaltungsprogramms für Communications Server für Linux sicher, dass Communications Server für Linux wie im Abschnitt „Communications Server für Linux aktivieren" beschrieben initialisiert ist. (Gegebenenfalls müssen Sie die Umgebungsvariable `DISPLAY` definieren, um einen geeigneten X-Server anzugeben.)

Wenn Sie das Motif-Verwaltungsprogramm im Hintergrund starten wollen, setzen Sie den folgenden Befehl ab:

**xsnaadmin &**

Communications Server für Linux zeigt das Domänenfenster an. Dieses Fenster zeigt alle definierten Knoten an und stellt Optionen für das Aktivieren und Inaktivieren von Knoten bereit. Durch doppeltes Klicken auf einen Knoten wird das in Abb. 4 auf Seite 76 gezeigte Knotenfenster für diesen Knoten aufgerufen.

Das Knotenfenster enthält Informationen zum Knoten und zu seinen Ressourcen. Sollten Sie den Knoten noch nicht konfiguriert haben, fordert das Verwaltungsprogramm Sie auf, den Knoten wie im Abschnitt „Knoten konfigurieren" auf Seite 80 beschrieben zu konfigurieren.

**Anmerkung:** Im vorliegenden Handbuch wird der Begriff Fenster für die Motif-Fenster verwendet, in denen Informationen zu CS-Linux-Ressourcen angezeigt werden. Ein Fenster kann ein oder mehrere Teilfenster enthalten. Eine Dialoganzeige ist ein Motif-Fenster, in dem Sie Informationen eingeben können.

Das Knotenfenster zeigt die meisten von Ihnen benötigten Informationen an und ermöglicht den einfachen Zugriff auf alle weiteren Informationen. Es enthält alle wichtigen Ressourcen auf dem lokalen Knoten.

Wenn Sie ein CS-Linux-Client/Server-System mit mehreren Knoten konfigurieren, führen Sie die Anweisungen in diesem Kapitel aus, um die einzelnen Knoten zu konfigurieren. (Kehren Sie jeweils zum Domänenfenster zurück, um den nächsten Knoten auszuwählen.)

Über das Menü **Fenster** des Knotenfensters können Sie andere Fenster aufrufen. Dazu gehören unter anderem:

- Fenster für LU-Pools
- Fenster für CPI-C-Bestimmungsorte

Über das Menü **Dienste** des Knotenfensters können Sie Ressourcen schnell hinzufügen und Hilfetexte zu Konfigurations- und Verwaltungsaufgaben aufrufen. Über das Menü **Diagnoseprogramm** können Sie die Dialoganzeige für Protokollierung und die Trace-Dialoganzeige aufrufen.

## Knotenfenster

Abb. 4 auf Seite 76 zeigt ein Beispiel für ein Knotenfenster. In der Titelleiste ist der Name des Linux-Systems angegeben.

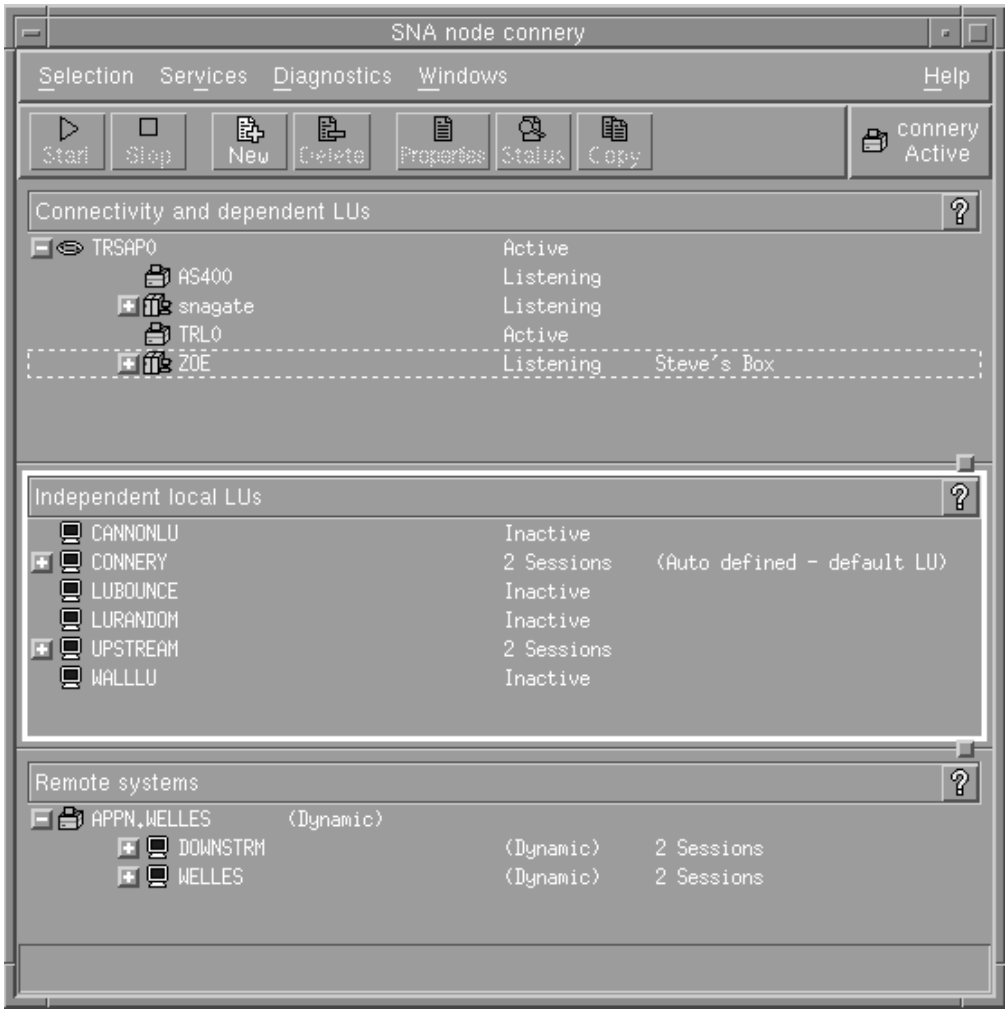


*Abbildung 4. Knotenfenster*

Im Knotenfenster können Sie alle Ressourcen und Komponenten des CS-Linux-Knotens konfigurieren und verwalten:

- Ports
- Verbindungsstationen
- LUs des Typs 0-3 und abhängige LUs des Typs 6.2
- DLUR-interne PUs
- Unabhängige lokale LUs
- Ferne Knoten
- Partner-LUs

Alle hier genannten Ressourcen können Sie im Knotenfenster hinzufügen, löschen, ändern und verwalten. Die Darstellung der Ressourcen im Fenster gibt Aufschluss über die Anordnungsbeziehungen zwischen Ressourcen und ermöglicht Ihnen zu steuern, welche Ressourcen angezeigt werden.

Ports, lokale LUs und ferne Knoten werden immer angezeigt. Im Knotenfenster wird jede Verbindungsstation unter dem zugehörigen Eltern-Port und jede abhängige LU unter der zugehörigen Elternverbindungsstation angezeigt. Darüber hinaus werden Partner-LUs unter lokalen LUs und fernen Knoten angezeigt.

Das Knotenfenster enthält verschiedene Bereiche für die unterschiedlichen Arten von Knotenressourcen:

- Das Knotenfeld oben rechts im Knotenfenster gibt an, ob der Knoten `Aktiv` oder `Inaktiv` ist.
- Im oberen Teilfenster des Knotenfensters (dem Konnektivitätsteilfenster) sind die Konnektivitätsressourcen aufgelistet. Dazu gehören Ports, Verbindungsstationen oder PUs der einzelnen Ports und abhängige LUs einer bestimmten Verbindungsstation oder PU. Dieses Fenster zeigt aktuelle Statusinformationen zu jeder einzelnen Ressource an.
- Das mittlere Teilfenster (das Teilfenster für unabhängige lokale LUs) enthält die auf dem lokalen Knoten definierten unabhängigen LUs. In diesem Fenster werden auch Informationen zu Sitzungen angezeigt, die eine bestimmte LU benutzen, sowie alle Einträge, die die Position einer Partner-LU über die Verbindungsstation definieren, die für den Zugriff auf diese Partner-LU verwendet wird.
- Das untere Teilfenster (das Teilfenster für ferne Systeme) enthält Informationen zu fernen Knoten und Partner-LUs. Darüber hinaus zeigt es Sitzungsinformationen zu jedem fernen Knoten und zu jeder Partner-LU an.

Sie können diese Teilfenster auswählen, indem Sie darauf klicken. Bestimmte Ressourcen innerhalb eines Teilfensters können Sie auswählen, indem Sie auf die Zeile für die Ressource klicken. Wenn Sie die Konfiguration einer Komponente anzeigen oder ändern wollen, müssen Sie doppelt auf die Komponente klicken. (Das Fenster stellt Knöpfe und Menüs bereit, über die Sie die Konfigurationsdaten bestimmter Ressourcen aufrufen können.)

Zu den Informationen, die zu jeder aufgelisteten Komponente angezeigt werden, gehören auch Informationen zu den zugehörigen Ressourcen. Verbindungsstationen sind beispielsweise unter dem Port, zu dem sie gehören, aufgelistet. Wenn Sie neben einer Komponente auf den Knopf **Einblenden** (+) klicken, werden die Ressourcen für diese Komponente angezeigt (sofern sie nicht schon vorher angezeigt wurden). Klicken Sie auf den Knopf **Ausblenden** (−), wird die Anzeige der Ressourcen für diese Komponente verdeckt.

Im Knotenfenster können Sie die folgenden Verwaltungsaufgaben ausführen:

**Ressource aktivieren oder inaktivieren**
: Wählen Sie die Ressource aus und klicken Sie auf den Knopf **Starten** oder **Stoppen**. (Alternativ dazu können Sie im Menü **Auswahl** die Option **Eintrag starten** oder **Eintrag stoppen** auswählen.)

**Ressource für eine Komponente hinzufügen**
: Wählen Sie die Komponente aus und klicken Sie auf den Knopf **Neu** (oder wählen Sie im Menü **Auswahl** die Option **Neu** aus). Wenn Sie beispielsweise eine Verbindungsstation für einen Port hinzufügen wollen, wählen Sie den Port aus und klicken Sie auf den Knopf **Neu**.

**Ressource löschen**
: Wählen Sie die Ressource aus und klicken Sie auf den Knopf **Löschen** (oder wählen Sie im Menü **Auswahl** die Option **Löschen** aus).

**Konfiguration für eine Ressource anzeigen oder ändern**
: Wählen Sie die Ressource aus und klicken Sie auf den Knopf **Merkmale** (oder wählen Sie im Menü **Auswahl** die Option **Merkmale** aus).

**Statusinformationen für eine Ressource abrufen**
: Wählen Sie die Ressource aus und klicken Sie auf den Knopf **Status** (oder wählen Sie im Menü **Auswahl** die Option **Status** aus).

**Konfiguration für eine Ressource kopieren**
Wählen Sie die Ressource aus und klicken Sie auf den Knopf **Kopieren** (oder wählen Sie im Menü **Auswahl** die Option **Kopieren** aus).

Darüber hinaus können Sie im Menü **Dienste** bestimmte Konfigurationsaufgaben für den Knoten auswählen, über das Menü **Diagnoseprogramm** die Protokollierung (für die Domäne) und den Trace (für den Knoten) steuern und durch Auswahl eines Eintrags im Menü **Fenster** Domänenressourcen anzeigen oder ändern.

## Ressourceneinträge

Die Darstellung der Ressourcen in einem Fenster gibt Aufschluss über die Anordnungsbeziehungen zwischen den Ressourcen.

Wenn einem Eintrag ein oder mehrere Kindelement(e) zugeordnet sind, wird neben diesem Eintrag das Symbol **Einblenden** (+) oder **Ausblenden** (–) angezeigt.

- Das Symbol **Einblenden** gibt an, dass die zugehörigen Kindelemente verdeckt sind. Sie können diese Elemente durch Klicken auf das Symbol **Einblenden** oder Drücken der Taste **+** auf dem numerischen Tastenblock anzeigen.
- Das Symbol **Ausblenden** gibt an, dass die Kindelemente angezeigt werden. Sie können diese Elemente durch Klicken auf das Symbol **Ausblenden** oder Drücken der Taste **–** auf dem numerischen Tastenblock verdecken.
- Wird neben einem Eintrag keines der Symbole angezeigt, sind diesem Eintrag keine Kindressourcen zugeordnet.

Nehmen wir z. B. an, einem bestimmten Port ist eine Verbindungsstation zugeordnet. Im Konnektivitätsteilfenster des Knotenfensters wird die Verbindungsstation zusammen mit allen anderen diesem Port zugeordneten Verbindungsstationen unter dem Eltern-Port angezeigt. Der Port wird immer angezeigt. Sie können jedoch auswählen, ob die Liste der zugeordneten Verbindungsstationen ebenfalls angezeigt oder verdeckt wird. In ähnlicher Weise kann die Liste von LUs, die einer Verbindungsstation zugeordnet sind, angezeigt oder verdeckt werden.

Eine Elternressource muss stets vor den Kindressourcen konfiguriert werden. Beim Löschen der Elternressource werden gleichzeitig alle zugehörigen Kindressourcen gelöscht.

## Knöpfe der Funktionsleiste

Ressourcenfenster enthalten eine Funktionsleiste mit Knöpfen, die das Ausführen allgemeiner Funktionen vereinfachen. Abb. 5 zeigt eine Funktionsleiste für Communications Server für Linux.


*Abbildung 5. Funktionsleiste für Communications Server für Linux*

In den Funktionsleisten der einzelnen Ressourcenfenster werden nicht alle Knöpfe angezeigt. Wenn die Operation, die über einen Knopf ausgeführt wird, für die derzeit ausgewählte Komponente ungültig ist (oder für eine Operation eine Komponente ausgewählt werden muss und dies nicht geschehen ist), wird der Knopf abgeblendet, so dass die Funktion nicht ausgewählt werden kann (und das Klicken auf den Knopf wirkungslos bleibt). In Ressourcenfenstern werden die folgenden Knöpfe angezeigt:

**Starten**
Aktiviert das ausgewählte Element

**Stoppen**
Inaktiviert das ausgewählte Element

**Neu** Fügt einen neuen Ressourceneintrag hinzu

**Löschen**
Löscht die ausgewählten Ressourcen

**Merkmale**
Öffnet für das ausgewählte Element den Dialog, über den die Konfiguration des Elements angezeigt oder geändert werden kann

**Status** Zeigt den aktuellen Status des ausgewählten Elements an

**Kopieren**
Kopiert das ausgewählte Element. Durch Klicken auf diesen Knopf wird eine Dialoganzeige geöffnet, deren Felder eine Kopie der Konfiguration der ausgewählten Komponente enthalten. Zum Hinzufügen der neuen Ressource müssen Sie die Angaben vervollständigen (den Namen der neuen Komponente eingeben).

Viele Ressourcen, z. B. Ports und Verbindungsstationen, können nicht geändert werden, solange sie aktiv sind. Sie können jedoch die Parameter aktiver Ressourcen aufrufen, indem Sie die gewünschte Ressource auswählen und durch Klicken auf den Knopf **Merkmale** die zugehörige Dialoganzeige öffnen. Wenn Sie die Dialoganzeige wieder schließen wollen, klicken Sie auf den Knopf **Schließen**.

## Client/Server-Funktionen konfigurieren

Dieser Abschnitt ist für Sie nur von Relevanz, wenn Sie Communications Server für Linux für die Ausführung in einer Client/Server-Umgebung (mit mehreren CS-Linux-Knoten in einem Netz) installiert haben.

Ein einer Client/Server-Umgebung kann ein Server als Konfigurationsserver markiert werden. Communications Server für Linux verwaltet eine Liste dieser Konfigurationsserver. Der erste aufgelistete Server ist der Hauptserver. Alle weiteren Server in der Liste sind Ausweichserver. Die Server werden der Reihenfolge nach aufgelistet, so dass der zweite aufgelistete Server (der erste Ausweichserver) die Aufgaben des Hauptservers übernimmt, wenn dieser nicht verfügbar ist. Der dritte Server in der Liste (der zweite Ausweichserver) übernimmt diese Aufgaben, falls weder der Hauptserver noch der erste Ausweichserver verfügbar ist, usw.

Wenn Knoten in der Domäne aktiv sind, wird der erste verfügbare Konfigurationsserver der Domäne (der erste Server mit der Software Communications Server für Linux, zu dem eine Verbindung hergestellt werden kann) zum Hauptserver. Falls der aktuelle Hauptserver nicht mehr verfügbar ist (weil keine Verbindung hergestellt wird, weil ein Netzfehler vorliegt oder weil die auf dem Server ausgeführte SNA-Software gestoppt wurde), wird der nächste verfügbare Konfigurationsserver in der Liste zum neuen Hauptserver.

Communications Server für Linux kann ohne einen Hauptserver ausgeführt werden. Dies geschieht, wenn es nicht möglich ist, zu einem der Server in der Liste der Konfigurationsserver eine Verbindung herzustellen. In einer solchen Situation können Sie die Knotenressourcen nur auf den Servern anzeigen und konfigurieren, zu denen eine Verbindung möglich ist.

**Anmerkung:** Sie können nicht direkt angeben, welcher Knoten die Rolle des Hauptservers übernehmen soll. Der Hauptserver wird auf der Basis der Reihenfolge ausgewählt, in der die Knoten zur Liste der Konfigurationsserver hinzugefügt werden. Falls Sie einen Server an den Anfang der Liste verschieben möchten, entfernen Sie alle anderen Knoten aus der Liste und fügen Sie sie dann erneut hinzu.

Im Domänenfenster des Motif-Verwaltungsprogramms können Sie einen Konfigurationsserver hinzufügen, indem Sie im Menü **Auswahl** die Option **Als Konfigurationsserver festlegen** auswählen. Der Server wird am Ende der Liste hinzugefügt. Er wird demzufolge erst zum Hauptserver; wenn alle anderen Konfigurationsserver nicht verfügbar sind. Wenn Sie einen Server entfernen möchten, wählen Sie im Menü **Auswahl** die Option **Konfigurationsserver entfernen** aus.

**Anmerkung:** Sie können einen Server nicht löschen, wenn er der einzige aufgelistete Server ist, auf dem die Software Communications Server für Linux ausgeführt wird, weil in diesem Fall kein Server mehr verfügbar wäre, der die Aufgaben des Hauptservers übernehmen könnte. In einer Client/Server-Konfiguration ist mindestens ein aktivierter Hauptserver erforderlich.

Weitere Informationen zum Konfigurieren und Verwalten eines Client/Server-Systems mit Communications Server für Linux finden Sie im *Communications Server für Linux Verwaltungshandbuch*. Dieses Handbuch enthält auch Hinweise zur erweiterten Client/Server-Konfiguration, z. B. zum Verschieben von Clients und Servern in andere CS-Linux-Domänen und zum detaillierten Konfigurieren des Client-Betriebs.

## Knoten konfigurieren

Der erste Schritt der CS-Linux-Konfiguration auf einem System ist das Konfigurieren des lokalen Knotens. Die Knotenkonfiguration stellt die Basisdaten bereit, die der Knoten für die Kommunikation in einem SNA-Netz benötigt. Erst nachdem Sie den Knoten konfiguriert haben, können Sie die Konnektivität oder andere Ressourcen für den Knoten definieren.

Falls der Knoten bereits konfiguriert wurde, können Sie die Knotenkonfiguration mit den in diesem Abschnitt beschriebenen Prozeduren ändern. Bevor Sie Konfigurationsänderungen vornehmen, müssen Sie den Knoten jedoch stoppen.

Entscheiden Sie vor dem Konfigurieren des Knotens, ob der Knoten als APPN-Knoten konfiguriert werden soll. Diese Entscheidung können Sie nur treffen, wenn Sie etwas über das Leistungsspektrum der anderen SNA-Knoten wissen, mit denen der lokale Knoten kommunizieren soll.

Abb. 6 auf Seite 81 zeigt einen CS-Linux-Knoten, der direkt mit einem Host kommuniziert.

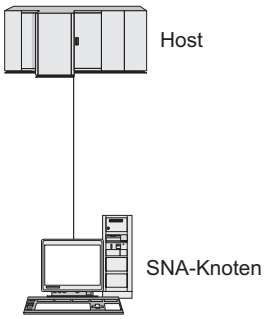


*Abbildung 6. CS-Linux-Knoten, der direkt mit einem Host kommuniziert*

Wenn der Host keine Unterstützung für APPN bereitstellt, konfigurieren Sie den CS-Linux-Knoten als LEN-Knoten. Sollte der Host APPN unterstützen, können Sie den CS-Linux-Knoten als APPN-Netzknoten oder APPN-Endknoten konfigurieren. (Wenn Communications Server für Linux für die Kommunikation mit dem Host ausschließlich SNA verwendet, werden Sie den CS-Linux-Knoten wahrscheinlich als Endknoten oder Zweignetzknoten konfigurieren.)

Abb. 7 zeigt mehrere CS-Linux-Knoten in einem APPN-Netz.

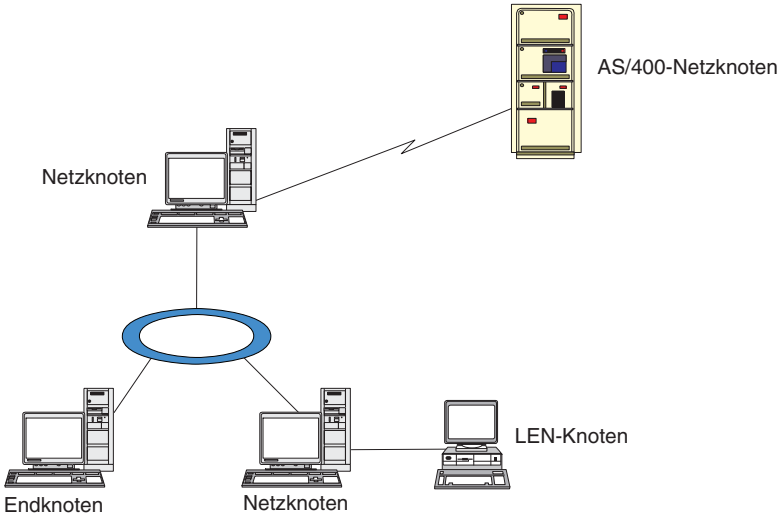


*Abbildung 7. CS-Linux-Knoten in einem APPN-Netz*

Wenn der lokale Knoten Teil eines APPN-Netzes ist und APPN-Routing-Dienste für andere Knoten bereitstellen soll, konfigurieren Sie ihn als APPN-Netzknoten. Werden die Routing-Dienste von anderen Knoten bereitgestellt, konfigurieren Sie den lokalen Knoten als APPN-Endknoten. Wenn der lokale Knoten nur mit einem Knoten (egal welchen Typs) kommuniziert, zu dem eine Direktverbindung besteht, konfigurieren Sie den Knoten als LEN-Knoten.

Stellen Sie vor Beginn der Knotenkonfiguration die folgenden Informationen zusammen:

- Art der APPN-Unterstützung (Netzknoten, Zweignetzknoten, Endknoten oder LEN-Knoten)

- Steuerpunktname (und Aliasname des Steuerpunkts, sofern sich dieser vom Steuerpunktnamen unterscheidet). Fragen Sie den Planungsbeauftragten für Ihr Netz nach diesem Namen.
- Standardknoten-ID (Sie können diese Standardeinstellung überschreiben, wenn Sie eine individuelle Kommunikationsverbindung konfigurieren.)

Führen Sie im Knotenfenster die folgenden Schritte aus, um den Knoten zu konfigurieren:

1. Wählen Sie im Menü **Dienste** des Knotenfensters den Eintrag **Knotenparameter konfigurieren** aus oder klicken Sie oben rechts im Knotenfenster doppelt auf das Knotenfeld. Communications Server für Linux zeigt den Dialog für Knotenparameter an.
2. Geben Sie die Ebene der APPN-Unterstützung, den Steuerpunktnamen und (sofern erforderlich) die Standardknoten-ID an.
3. Klicken Sie auf **OK**, um den Knoten zu definieren. Beim Definieren des Knotens definiert Communications Server für Linux automatisch eine Standard-LU, die denselben Namen wie der Steuerpunkt hat.

   Wenn Sie die Dialoganzeige verlassen wollen, ohne die eingegebenen Werte zu sichern, klicken Sie auf den Knopf **Abbrechen**.

## Konnektivität konfigurieren

Ein CS-Linux-Knoten kann erst mit anderen Knoten kommunizieren, wenn Sie Konnektivität zu mindestens einem Nachbarknoten konfiguriert haben. Eine Verbindung kann für abhängigen Verkehr, unabhängigen Verkehr oder beide Arten von Verkehr konfiguriert werden.

In Ihrem Computer können Adapter für ein oder mehrere Verbindungsprotokoll(e) installiert sein. Viele der Informationen, die Sie beim Konfigurieren der Konnektivität eingeben müssen, hängen vom verwendeten Verbindungsprotokoll ab. Eine Liste der von Communications Server für Linux unterstützten Verbindungsprotokolle finden Sie im Abschnitt „Installationsvoraussetzungen" auf Seite 22.

Zum Konfigurieren einer Verbindung müssen Sie einen Port und (in den meisten Fällen) eine Verbindungsstation definieren. Wenn Sie das Motif-Verwaltungsprogramm verwenden, wird im Rahmen der Port-Konfiguration automatisch eine DLC (Datenübertragungssteuerung) konfiguriert. Sie können den Port aber auch als Teil eines Verbindungsnetzes definieren.

Welche Verbindungen Sie konfigurieren müssen, hängt von Ihrer Zielsetzung und davon ab, ob Ihr Netz ein APPN-Netz ist. Die erforderlichen Informationen richten sich nach dem Verbindungsprotokoll und danach, ob die Verbindung für abhängigen Verkehr, unabhängigen Verkehr oder für beide Arten von Verkehr konfiguriert werden soll.

In diesem Abschnitt wird die Konfiguration für die folgende Auswahl von Verbindungsarten erläutert:

- Verbindungen, die den abhängigen Datenverkehr mit einem Hostsystem über eine SDLC-Verbindung unterstützen
- Verbindungen, die den Transport von abhängigem und unabhängigem Verkehr in ein APPN-Netz über das Ethernet-Verbindungsprotokoll unterstützen. In dieser Beispielkonfiguration ist auch das Definieren eines Verbindungsnetzes für den Ethernet-Port beschrieben.

- Enterprise-Extender-Verbindungen zu einem APPN-Netz (Enterprise-Extender-Verbindungen unterstützen nur unabhängigen Datenverkehr).

Hinweise zu anderen Verbindungsprotokollen finden Sie im *Communications Server für Linux Verwaltungshandbuch* oder in der Onlinehilfe des Motif-Verwaltungsprogramms.

## SDLC-Verbindung für abhängigen Datenverkehr konfigurieren

Für einen SDLC-Port (Steuerung für synchrone Datenübertragung) benötigen Sie die folgenden Informationen:

- Name des SNA-Ports (in der Regel können Sie die Standardeinstellung verwenden). Sie müssen auch die SDLC-Einheitennummer angeben.
- die Information, ob der Port beim Start des Knotens automatisch aktiviert werden soll
- Leitungstyp (abgehende/ankommende Wählleitung oder Standleitung)
- Funktion der Verbindungsstation ('Primär', 'Sekundär', 'Aushandelbar', 'Primär für Mehrpunktverbindungen' oder 'Sekundär, mehrere PUs')
- Aufrufadresse (nur für eine ankommende Wählleitung an einem nicht primären Port). Bei anderen Port-Typen wird die Aufrufadresse auf der Verbindungsstation konfiguriert.

Für eine SDLC-Verbindungsstation benötigen Sie die folgenden zusätzlichen Informationen:

- Aktivierungsmethode ('Durch Administrator', 'Bei Initialisierung des Knotens' oder 'Bei Anforderung')
- Art des unterstützten Verkehrs (in diesem Beispiel nur abhängiger Verkehr)
- Funktion des fernen Knotens (in diesem Beispiel 'Host')

Führen Sie im Knotenfenster die folgenden Schritte aus, um die SDLC-Verbindung zu konfigurieren:

1. Konfigurieren Sie wie folgt den Port:
   a. Wählen Sie das Konnektivitätsteilfenster aus.
   b. Wählen Sie im Untermenü **Konnektivität** des Menüs **Dienste** den Eintrag **Neuer Port** aus (oder klicken Sie in der Symbolleiste auf den Knopf **Neu**).
   c. Wählen Sie im Auswahlmenü der daraufhin erscheinenden Dialoganzeige den Protokolltyp und anschließend die Option zum Definieren eines Ports aus.

      Wenn Sie auf **OK** klicken, zeigt Communications Server für Linux den Dialog für SDLC-Ports an.
   d. Geben Sie in den Feldern der Dialoganzeige die entsprechenden Werte ein.
   e. Klicken Sie auf **OK**, um den Port zu definieren.

      Der Port wird im Konnektivitätsteilfenster des Knotenfensters angezeigt.
2. Definieren Sie wie folgt eine Verbindungsstation für den Port:
   a. Vergewissern Sie sich, dass Sie im Konnektivitätsteilfenster des Knotenfensters den Port ausgewählt haben, zu dem die Verbindungsstation hinzugefügt werden soll.
   b. Wählen Sie im Untermenü **Konnektivität** des Menüs **Dienste** den Eintrag **Neue Verbindungsstation** aus (oder klicken Sie in der Symbolleiste auf den Knopf **Neu**).
   c. Klicken Sie auf **OK**.

Communications Server für Linux zeigt den Dialog für SDLC-Verbindungsstationen an.

d. Geben Sie in den Feldern der Dialoganzeige die entsprechenden Werte ein.

e. Klicken Sie auf **OK**, um die Verbindungsstation zu definieren.

Die Verbindungsstation wird im Konnektivitätsteilfenster des Knotenfensters unterhalb des Ports, dem sie zugeordnet ist, angezeigt.

## Ethernet-Verbindung für abhängigen und unabhängigen Verkehr konfigurieren

Das folgende Beispiel erläutert, wie Sie eine Ethernet-Verbindung konfigurieren können, die den Transport von abhängigem und unabhängigem Verkehr in ein APPN-Netz unterstützt. Darüber hinaus wird das Definieren eines Verbindungsnetzes für den Ethernet-Port beschrieben.

Für einen Ethernet-Port benötigen Sie die folgenden Informationen:

- Name des SNA-Ports (in der Regel können Sie die Standardeinstellung verwenden). Wenn Sie mehrere Ethernet-Netzadapterkarten verwenden, müssen Sie außerdem die Nummer der Ethernet-Karte angeben. Darüber hinaus müssen Sie die Nummer des lokalen SAP (Service Access Point) angeben (für Intel- und OSA2-Adapter in der Regel `04`). Für einen OSA-Express-Adapter muss die lokale SAP-Nummer mit der Nummer übereinstimmen, die in der OSA/SF für die E/A-Einheitenadressen definiert wurde, die der ethX-Schnittstelle dieses Linux-Images entsprechen.
- die Information, ob der Port beim Start des Knotens automatisch aktiviert werden soll
- Name des Verbindungsnetzes (muss für alle Ports innerhalb eines Verbindungsnetzes identisch sein)

Für eine Ethernet-Verbindungsstation benötigen Sie die folgenden zusätzlichen Informationen:

- Aktivierungsmethode ('Durch Administrator', 'Bei Initialisierung des Knotens' oder 'Bei Anforderung')
- Art des unterstützten Verkehrs (in diesem Beispiel sowohl abhängiger als auch unabhängiger Verkehr)
- Steuerpunktname des fernen Knotens (wird nur für einen LEN-Knoten benötigt)
- Art des fernen Knotens (Netzknoten, Endknoten oder 'Feststellen')
- Funktion des fernen Knotens (in diesem Beispiel: untergeordnetes SNA-Gateway oder Durchgriff-DLUR)
- Zum Konfigurieren einer selektiven Verbindungsstation benötigen Sie die MAC-Adresse und die SAP-Nummer (in der Regel `04`) der fernen Workstation. Wenn Sie keine Adressdaten angeben und für das Feld `Aktivierung` die Option *Durch Administrator* auswählen, ist die Verbindungsstation eine nicht selektive empfangsbereite Verbindungsstation.

Führen Sie im Knotenfenster die folgenden Schritte aus, um die Ethernet-Verbindung zu konfigurieren:

1. Konfigurieren Sie wie folgt den Port:
   a. Wählen Sie das Konnektivitätsteilfenster aus.
   b. Wählen Sie im Untermenü **Konnektivität** des Menüs **Dienste** den Eintrag **Neuer Port** aus (oder klicken Sie in der Symbolleiste auf den Knopf **Neu**).

c. Wählen Sie im Auswahlmenü der daraufhin erscheinenden Dialoganzeige den Protokolltyp und anschließend die Option zum Definieren eines Ports aus.

   Wenn Sie auf **OK** klicken, zeigt Communications Server für Linux den Ethernet-SAP-Dialog an.

d. Geben Sie in den Feldern der Dialoganzeige die entsprechenden Werte ein.

e. Klicken Sie auf **OK**, um den Port zu definieren.

   Der Port wird im Konnektivitätsteilfenster des Knotenfensters angezeigt.

2. Definieren Sie wie folgt eine Verbindungsstation für den Port:

   a. Vergewissern Sie sich, dass Sie im Konnektivitätsteilfenster des Knotenfensters den Port ausgewählt haben, zu dem die Verbindungsstation hinzugefügt werden soll.

   b. Wählen Sie im Untermenü **Konnektivität** des Menüs **Dienste** den Eintrag **Neue Verbindungsstation** aus (oder klicken Sie in der Symbolleiste auf den Knopf **Neu**).

   c. Klicken Sie auf **OK**.

      Communications Server für Linux zeigt den Dialog für Ethernet-Verbindungsstationen an.

   d. Geben Sie in den Feldern der Dialoganzeige die entsprechenden Werte ein.

   e. Klicken Sie auf **OK**, um die Verbindungsstation zu definieren.

      Die Verbindungsstation wird im Konnektivitätsteilfenster des Knotenfensters unterhalb des Ports, dem sie zugeordnet ist, angezeigt.

## Enterprise-Extender-Verbindung konfigurieren

Das folgende Beispiel erläutert, wie Sie eine Enterprise-Extender-Verbindung zu einem APPN-Netz konfigurieren können. Beachten Sie, dass Enterprise-Extender-Verbindungen nur unabhängigen LU-Datenverkehr unterstützen.

Für einen Enterprise-Extender-Port benötigen Sie die folgenden Informationen:

- Name des SNA-Ports (in der Regel können Sie die Standardeinstellung verwenden). Wenn Sie mehrere Netzadapterkarten verwenden, die IP ausführen, müssen Sie außerdem den Namen der zu verwendenden IP-Schnittstelle (z. B. `eth0`) angeben.
- die Information, ob der Port beim Start des Knotens automatisch aktiviert werden soll

Für eine Enterprise-Extender-Verbindungsstation benötigen Sie die folgenden zusätzlichen Informationen:

- Aktivierungsmethode ('Durch Administrator', 'Bei Initialisierung des Knotens' oder 'Bei Anforderung')
- Art des fernen Knotens (Netzknoten, Endknoten oder 'Feststellen')
- Zum Konfigurieren einer selektiven Verbindungsstation benötigen Sie den IP-Hostnamen oder die IP-Adresse der fernen Station. Wenn Sie diese Daten nicht angeben und für das Feld `Aktivierung` die Option *Durch Administrator* auswählen, ist die Verbindungsstation eine nicht selektive empfangsbereite Verbindungsstation.

Führen Sie im Knotenfenster die folgenden Schritte aus, um die Enterprise-Extender-Verbindung zu konfigurieren:

1. Konfigurieren Sie wie folgt den Port:

   a. Wählen Sie das Konnektivitätsteilfenster aus.

b. Wählen Sie im Untermenü **Konnektivität** des Menüs **Dienste** den Eintrag **Neuer Port** aus (oder klicken Sie in der Symbolleiste auf den Knopf **Neu**).
c. Wählen Sie im Auswahlmenü der daraufhin erscheinenden Dialoganzeige den Protokolltyp und anschließend die Option zum Definieren eines Ports aus.

   Wenn Sie auf **OK** klicken, zeigt Communications Server für Linux den Dialog für IP-Ports an.
d. Geben Sie in den Feldern der Dialoganzeige die entsprechenden Werte ein.
e. Klicken Sie auf **OK**, um den Port zu definieren.

   Der Port wird im Konnektivitätsteilfenster des Knotenfensters angezeigt.

2. Definieren Sie wie folgt eine Verbindungsstation für den Port:
   a. Vergewissern Sie sich, dass Sie im Konnektivitätsteilfenster des Knotenfensters den Port ausgewählt haben, zu dem die Verbindungsstation hinzugefügt werden soll.
   b. Wählen Sie im Untermenü **Konnektivität** des Menüs **Dienste** den Eintrag **Neue Verbindungsstation** aus (oder klicken Sie in der Symbolleiste auf den Knopf **Neu**).
   c. Klicken Sie auf **OK**.

      Communications Server für Linux zeigt den Dialog für IP-Verbindungsstationen an.
   d. Geben Sie in den Feldern der Dialoganzeige die entsprechenden Werte ein.
   e. Klicken Sie auf **OK**, um die Verbindungsstation zu definieren.

      Die Verbindungsstation wird im Konnektivitätsteilfenster des Knotenfensters unterhalb des Ports, dem sie zugeordnet ist, angezeigt.

## LUs des Typs 0-3 konfigurieren

Zur Unterstützung von Benutzeranwendungen, die LUs des Typs 0-3 verwenden, müssen Sie abhängige LUs konfigurieren. Zuvor müssen Sie jedoch die folgenden Konfigurationsschritte ausführen:

- Konfigurieren Sie den Knoten wie im Abschnitt „Knoten konfigurieren" auf Seite 80 beschrieben.
- Konfigurieren Sie eine Verbindung für abhängigen LU-Datenverkehr. Lesen Sie dazu die Beschreibung im Abschnitt „Konnektivität konfigurieren" auf Seite 82.

  Wenn Sie mit SNA Gateway eine Verbindung zu einem anderen übergeordneten Knoten herstellen oder DLUR verwenden, müssen Sie keine Direktverbindung zum Host konfigurieren. Weitere Informationen hierzu finden Sie in den Abschnitten „SNA Gateway konfigurieren" auf Seite 97 und „DLUR konfigurieren" auf Seite 99.

Zur Unterstützung der Kommunikation mit einem Hostsystem müssen Sie abhängige LUs der Typen 0–3 konfigurieren. Anhand der Informationen in diesem Abschnitt können Sie eine LU für die Unterstützung von LUA, DLUR oder PU-Konzentration definieren. Sie können außerdem einen Bereich von LUs definieren, falls Sie mehrere LUs eines Typs für eine Operation konfigurieren möchten.

Darüber hinaus können Sie einen Pool mit LUs definieren, die dann bei Bedarf verwendet werden. Dazu können Sie eine LU einem Pool zuordnen, wenn Sie die LU definieren. Sie können aber auch bereits definierte LUs einem Pool zuordnen.

## LUs des Typs 0-3 definieren

Stellen Sie vor dem Konfigurieren der 3270-LU die folgenden Informationen zusammen:

- LU-Name (Dies ist ein lokaler Bezeichner, der nicht mit der Hostkonfiguration übereinstimmen muss.)
- LU-Nummer (bzw. bei einem Bereich von LUs die LU-Nummern)
- LU-Typ (Modell des 3270-Datensichtgeräts oder 3270-Drucker)
- Poolname (wenn Sie die LU zu einem Pool hinzufügen)

Führen Sie im Knotenfenster die folgenden Schritte aus, um eine LU des Typs 0–3 für eine bereits definierte Verbindungsstation zu konfigurieren:

1. Wählen Sie im Konnektivitätsteilfenster die Verbindungsstation zum Host aus.
2. Klicken Sie auf den Knopf **Neu**.
3. Wählen Sie in der daraufhin erscheinenden Dialoganzeige den LU-Typ (**Neue 3270-Anzeige-LU** oder **Neue 3270-Drucker-LU**) aus.

   Wenn Sie diesen Eintrag auswählen und auf **OK** klicken, zeigt Communications Server für Linux den Dialog für LUs des Typs 0-3 an.
4. Geben Sie in den Feldern der Dialoganzeige die entsprechenden Werte ein.
5. Klicken Sie auf **OK**, um die LU zu definieren.

   Die LU wird im Konnektivitätsteilfenster des Knotenfensters unterhalb der Verbindungsstation zum Host angezeigt.

## LU-Pool definieren

Für LUs des Typs 0-3 können Sie LU-Pools definieren, um die Benutzerkonfiguration zu vereinfachen und eine größere Flexibilität beim Aufbauen von Hostsitzungen zu erzielen. Sie können beispielsweise mehrere LUs in einem Pool definieren und dann mehrere Benutzer für die Verwendung dieses Pools konfigurieren. Dadurch wird die Konfiguration von Benutzersitzungen einfacher, und alle Sitzungen können jede beliebige LU des Pools benutzen.

**Anmerkung:** Sie können einer bestimmten LU oder einem LU-Pool eine Benutzersitzung zuordnen.

- Wenn Sie die Benutzersitzung einer bestimmten LU zuordnen, die in einem Pool enthalten ist, verwendet die Sitzung diese LU, sofern sie verfügbar ist. Andernfalls verwendet die Sitzung eine beliebige freie LU aus dem Pool, als hätten Sie die Sitzung dem LU-Pool und nicht dieser speziellen LU zugeordnet.
- Falls der Benutzer nur eine angegebene LU verwenden soll, so dass die Benutzersitzung nicht aufgebaut wird, wenn die LU bereits benutzt wird, müssen Sie sicherstellen, dass die LU nicht in einem Pool enthalten ist.

Die LU-Pools für den lokalen CS-Linux-Knoten werden im Fenster für LU-Pools angezeigt. Dieses Fenster listet die auf dem lokalen System konfigurierten LU-Pools auf. Sie können in diesem Fenster LUs auswählen und zu einem LU-Pool hinzufügen.

Zu einem Pool können Sie LUs der folgenden Typen hinzufügen (ein Pool darf keine Mischung verschiedener LU-Typen enthalten):

- 3270-Anzeige-LU
- unbeschränkte LU

### LUs des Typs 0-3 konfigurieren

Bevor Sie LUs zu einem Pool hinzufügen, müssen Sie die LUs auf dem lokalen Knoten definieren.

Führen Sie im Knotenfenster die folgenden Schritte aus, um einen LU-Pool zu konfigurieren:

1. Wählen Sie im Menü **Fenster** den Eintrag **LU-Pools** aus.

   Communications Server für Linux zeigt das Fenster für LU-Pools an.
2. Klicken Sie auf den Knopf **Neu**.

   Communications Server für Linux zeigt den Konfigurationsdialog für LU-Pools an.

   Im rechten Feld sind LUs aufgelistet, die noch keinem Pool zugeordnet sind. Jede dieser LUs kann in den neuen Pool integriert werden.
3. Wählen Sie die LU oder LUs aus, die Sie zum Pool hinzufügen wollen, und klicken Sie auf den Knopf **Neu**, um die ausgewählten LUs in das linke Feld zu verschieben.

   Wenn Sie eine LU aus dem linken Feld entfernen wollen, wählen Sie die LU aus und klicken Sie auf den Knopf **Entfernen**.
4. Klicken Sie auf **OK**, um den LU-Pool zu definieren.

   Alle im linken Feld enthaltenen LUs werden zum LU-Pool hinzugefügt.

   Der Pool wird im Fenster für LU-Pools angezeigt.

## APPC-Kommunikation konfigurieren

Voraussetzung für die Kommunikation von APPC- und CPI-C-Anwendungen ist die Konfiguration von APPC. Eine APPC-Anwendung benutzt die LU-6.2-Ressourcen des Knotens, um in einem bestimmten Modus mit anderen APPC- oder CPI-C-Anwendungen auf einem Host oder einem Peer-Computer zu kommunizieren.

Bevor Sie die APPC-Kommunikation konfigurieren können, müssen Sie die folgenden Konfigurationsschritte ausführen:

1. Konfigurieren Sie den Knoten wie im Abschnitt „Knoten konfigurieren" auf Seite 80 beschrieben.
2. Konfigurieren Sie die Konnektivität wie im Abschnitt „Konnektivität konfigurieren" auf Seite 82 beschrieben.

Die verbleibenden Konfigurationsschritte richten sich danach, ob die Konfiguration abhängigen Verkehr, unabhängigen Verkehr oder beide Arten von Verkehr unterstützt.

**Unabhängiges APPC**

Unabhängiges APPC verwendet unabhängige LUs. An jeder LU-LU-Sitzung nehmen eine lokale LU und eine Partner-LU teil.

Als lokale LU können Sie die bereits definierte, dem Knotensteuerpunkt zugeordnete Standard-LU verwenden. Sie können aber auch neue lokale LUs konfigurieren.

Die Partner-LU muss nicht konfiguriert werden, wenn der CS-Linux-Knoten ein Endknoten oder Netzknoten in einem APPN-Netz ist, da APPN Partner-LUs dynamisch lokalisieren kann. Ist das Netz kein APPN-Netz oder der Knoten ein LEN-Knoten, müssen Sie die Partner-LU allerdings konfigurieren. In diesem Fall müssen Sie den fernen Knoten, auf dem sich die Partner-LU befindet, konfigurieren und dann die Partner-LU auf dem fernen Knoten definieren.

**Abhängiges APPC**
: Wenn der ferne Knoten ein Host ist, der keine Unterstützung für unabhängige LUs 6.2 bietet, müssen Sie eine Konfiguration für abhängigen Verkehr definieren. Für abhängiges APPC müssen Sie eine lokale LU konfigurieren.

Benutzen die Anwendungen CPI-C, müssen Sie nach der Konfiguration von APPC möglicherweise zusätzliche Konfigurationsschritte für CPI-C ausführen (siehe Abschnitt „Konfiguration für CPI Communications" auf Seite 94). Eine CPI-C-Anwendung benutzt die LU-6.2-Ressourcen und die Modusressourcen des Knotens, um mit einer anderen APPC- oder CPI-C-Anwendung auf einem Host oder einem Peer-Computer zu kommunizieren. Für eine CPI-C-Anwendung müssen Sie die gleichen Ressourcen wie für eine APPC-Anwendung definieren. Wenn das Transaktionsprogramm auf dem CS-Linux-Computer das aufrufende Transaktionsprogramm oder Quellen-TP ist (das den Dialog startet), müssen Sie für dieses Transaktionsprogramm möglicherweise Einträge mit Nebeninformationen definieren. Gehen Sie dazu wie im Abschnitt „Konfiguration für CPI Communications" auf Seite 94 beschrieben vor. Jeder dieser Einträge stellt Informationen zu einem Partnertransaktionsprogramm, die für den Zugriff auf dieses Programm verwendeten LU- und Modusressourcen sowie alle benötigten Sicherheitsinformationen bereit.

Im folgenden Abschnitt („Einfaches APPN-Netz konfigurieren") ist die Konfiguration eines einfachen, aus einem Netzknoten, einem Endknoten und einem LEN-Knoten bestehenden APPN-Netzes (mit unabhängigen LUs 6.2) erläutert. (Dieses Beispielszenario zeigt auch, wie Sie Statusinformationen zu CP-CP-Sitzungen zwischen Knoten abrufen können.)

Im Abschnitt „Abhängiges APPC konfigurieren" auf Seite 94 finden Sie darüber hinaus eine Beschreibung der Konfiguration für die unabhängige APPC-Kommunikation.

Für beide Beispielszenarien wird vorausgesetzt, dass APPC-Sitzungen einen Standardmodus und eine Standardserviceklasse (COS, Class Of Service) verwenden.

Hinweise zum Konfigurieren zusätzlicher APPC-Informationen wie Modi, Sicherheit und aufrufbare Transaktionsprogramme (Ziel-TPs) finden Sie im *Communications Server für Linux Verwaltungshandbuch*.

## Einfaches APPN-Netz konfigurieren

Das einfachste APPN-Netz, das Sie konfigurieren können, besteht aus zwei Knoten: einem APPN-Netzknoten und einem APPN-Endknoten. Der Netzknoten führt für den Endknoten das Sitzungs-Routing aus.

### Netzknoten konfigurieren

Bei diesem Szenario wird davon ausgegangen, dass Sie die Steuerpunkt-LU und einen Standardmodus sowie eine LAN-Verbindungsart (Token-Ring, Ethernet) verwenden. In diesem Fall ist die Konfiguration des Endknotens einfach. Führen Sie die folgenden Schritte aus:

1. Konfigurieren Sie den Knoten wie im Abschnitt „Knoten konfigurieren" auf Seite 80 beschrieben. Wählen Sie für das Feld *APPN-Unterstützung* den Wert `Netzknoten` aus. Notieren Sie den Steuerpunktnamen.
2. Konfigurieren Sie die Konnektivität wie im Abschnitt „Konnektivität konfigurieren" auf Seite 82 beschrieben. Konfigurieren Sie die Verbindung für die Unterstützung von unabhängigem Verkehr.

Wenn Sie von einem benachbarten Endknoten eine Verbindung zu diesem Knoten aufbauen wollen, müssen Sie die MAC-Adresse und die SAP-Nummer des Ports auf dem Netzknoten kennen. Die MAC-Adresse eines CS-Linux-Knotens können Sie wie folgt abrufen:

1. Wählen Sie im Knotenfenster den Port aus.
2. Klicken Sie auf den Knopf **Starten**, um den Port zu aktivieren.
3. Klicken Sie auf den Knopf **Status**, um die Statusinformationen zum Port aufzurufen. Im Statusdialog für den Port werden die MAC-Adresse und die SAP-Nummer angezeigt.
4. Notieren Sie die MAC-Adresse und die SAP-Nummer, damit Sie diese Werte auf dem Endknoten im Konfigurationsdialog für die Verbindungsstation eingeben können.

## Endknoten konfigurieren

Bei diesem Szenario wird davon ausgegangen, dass Sie die Steuerpunkt-LU und einen Standardmodus sowie eine LAN-Verbindungsart (Token-Ring, Ethernet) verwenden. In diesem Fall ist die Konfiguration des Endknotens einfach. Führen Sie die folgenden Schritte aus:

1. Konfigurieren Sie den Knoten wie im Abschnitt „Knoten konfigurieren" auf Seite 80 beschrieben. Wählen Sie für das Feld *APPN-Unterstützung* den Wert `Endknoten` aus.
2. Konfigurieren Sie die Konnektivität wie im Abschnitt „Konnektivität konfigurieren" auf Seite 82 beschrieben. Konfigurieren Sie die Verbindung für die Unterstützung von unabhängigem Verkehr und geben Sie für die Verbindungsstation die folgenden Informationen an:
   - Geben Sie für das Feld *Ferner Knoten* als Wert den Namen des Netzknotens ein (siehe Abschnitt „Netzknoten konfigurieren" auf Seite 89).
   - Geben Sie im Teilfenster 'Verbindungsinformationen' des Konfigurationsdialogs für die Verbindungsstation die MAC-Adresse und die SAP-Nummer des Ports auf dem Netzknoten ein.

   In einem APPN-Netz ist es möglich, über nur eine Verbindungsstation zu einem benachbarten Netzknoten mit allen fernen Knoten im Netz zu kommunizieren. Sie müssen deshalb nicht zu jedem fernen Knoten eine gesonderte Verbindungsstation konfigurieren.

## Konnektivität zwischen zwei Knoten prüfen

In diesem Szenario wird vorausgesetzt, dass Sie einen Netzknoten gemäß der Beschreibung im Abschnitt „Netzknoten konfigurieren" auf Seite 89 und einen Endknoten gemäß der Beschreibung im Abschnitt „Endknoten konfigurieren" konfiguriert haben. Auf dem Endknoten können Sie die folgenden Schritte ausführen:

1. Wählen Sie im Knotenfenster die Verbindungsstation zum benachbarten Netzknoten aus.
2. Klicken Sie auf den Knopf **Starten**, um die Verbindungsstation zu aktivieren.

   Wenn die Verbindungsstation aktiviert wird, werden die CP-CP-Sitzungen zwischen den beiden Knoten automatisch aufgebaut. Diese Sitzungen werden im Teilfenster für unabhängige lokale LUs des Knotenfensters angezeigt.
3. Wenn Sie zu einer Sitzung Statusinformationen abrufen wollen, wählen Sie die Sitzung im Knotenfenster aus und klicken Sie auf den Knopf **Status**.

## Unabhängige APPC-LU konfigurieren

In vielen Fällen können Anwendungen die Steuerpunkt-LU des lokalen Knotens benutzen, die beim Konfigurieren des Knotens automatisch definiert wird. Dies ist die Standard-LU. Wenn eine Anwendung keine bestimmte LU angibt, kann sie

diese LU verwenden. Benutzt die Anwendung die Standard-LU, müssen Sie keine lokale LU definieren. Diesbezügliche Informationen finden Sie in der Dokumentation zur APPC-Anwendung. Entsprechende Hinweise kann auch der Anwendungsprogrammierer geben.

Für das Konfigurieren einer unabhängigen LU 6.2 benötigen Sie die folgenden Informationen:

- Name der lokalen LU
- Aliasname der lokalen LU (wenn ein von dieser LU unterstütztes Transaktionsprogramm einen Aliasnamen verwendet)

Führen Sie im Knotenfenster die folgenden Schritte aus, um eine unabhängige lokale LU zu konfigurieren:

1. Wählen Sie das Teilfenster für unabhängige lokale LUs aus.
2. Wählen Sie im Untermenü **APPC** des Menüs **Dienste** den Eintrag **Neue unabhängige lokale LU** aus (oder klicken Sie auf den Knopf **Neu**).

   Communications Server für Linux zeigt den Dialog für lokale LUs an.
3. Geben Sie in den Feldern der Dialoganzeige die entsprechenden Werte ein.
4. Klicken Sie auf **OK**, um die lokale LU zu definieren. Die unabhängige LU wird im Teilfenster für unabhängige lokale LUs des Knotenfensters angezeigt.

## Partner-LUs für einen LEN-Knoten konfigurieren

In folgenden Fällen müssen Sie einen fernen Knoten (und die Partner-LUs auf dem Knoten) definieren:

- Wenn der lokale Knoten ein LEN-Knoten ist, müssen Sie alle fernen Knoten und alle Partner-LUs auf dem fernen Knoten, mit denen der lokale Knoten über APPC kommuniziert, definieren. Ein LEN-Knoten kann Partner-LUs nicht dynamisch lokalisieren. Dies ist nur über die Definition des fernen Knotens möglich.
- Wenn der lokale Knoten nicht Teil eines APPN-Netzes ist (z. B., wenn zwei Endknoten ohne Netzknotenserver direkt miteinander verbunden sind), können LUs nicht dynamisch lokalisiert werden. In diesem Fall müssen Sie alle Partner-LUs konfigurieren.
- Wenn der ferne Knoten ein LEN-Knoten und der lokale Knoten ein Netzknoten ist, der für den LEN-Knoten die Funktion eines Netzknotenservers hat, müssen Sie den LEN-Knoten (mit den Partner-LUs) auf dem Netzknotenserver als fernen Knoten definieren. Durch diese Definition können die Knoten im übrigen APPN-Netz LUs auf dem LEN-Knoten lokalisieren.
- Wenn sich der ferne Knoten in einem anderen APPN-Netz befindet, müssen Sie den fernen Knoten definieren, da dieser nicht dynamisch lokalisiert werden kann.

Definieren Sie keine Partner-LUs, wenn der lokale und der ferne Knoten zum selben APPN-Netz gehören.

Wenn Sie eine Definition für einen fernen Knoten hinzufügen, wird automatisch eine Partner-LU mit demselben Namen hinzugefügt. Dies ist die Steuerpunkt-LU des fernen Knotens. Falls Ihre Anwendung diese Partner-LU benutzt, müssen Sie keine andere Partner-LU hinzufügen. Bei Bedarf können Sie jedoch einen LU-Aliasnamen für die Partner-LU hinzufügen. Klicken Sie zum Hinzufügen eines Aliasnamens doppelt auf die Partner-LU und geben Sie im Konfigurationsdialog für Partner-LUs den Aliasnamen ein.

Wenn Ihre Anwendung mit einem LU-Aliasnamen auf die zugehörige Partner-LU verweist, sollten Sie für die LU die Definition eines Aliasnamens hinzufügen.

Ist der lokale oder der ferne Knoten ein LEN-Knoten, müssen Sie die Partner-LU als Kind des fernen Knotens definieren, da der LEN-Knoten nicht in der Lage ist, LUs dynamisch zu lokalisieren. Benutzt Ihre Anwendung die Steuerpunkt-LU des fernen Knotens als Partner-LU, müssen Sie keine Partner-LU definieren, denn die Steuerpunkt-LU wurde bereits beim Konfigurieren des fernen Knotens automatisch definiert.

Mit dem Motif-Verwaltungsprogramm können Sie einen Aliasnamen für eine Partner-LU hinzufügen (siehe Abschnitt „Aliasnamen für Partner-LU definieren"), eine Definition für eine Partner-LU auf einem bestimmten fernen Knoten hinzufügen (siehe Abschnitt „Partner-LU auf einem fernen Knoten definieren" auf Seite 93) oder mehrere Partner-LUs unter Verwendung von Platzhaltern definieren (siehe Abschnitt „Mehrere Partner-LUs unter Verwendung von Platzhaltern definieren" auf Seite 93).

**Fernen Knoten definieren:** Bevor Sie einen fernen Knoten konfigurieren, benötigen Sie die folgenden Informationen:

- vollständig qualifizierter SNA-Netzname des Knotens

Führen Sie im Knotenfenster die folgenden Schritte aus, um einen fernen Knoten zu konfigurieren:

1. Wählen Sie das Teilfenster für ferne Systeme aus.
2. Wählen Sie im Untermenü **APPC** des Menüs **Dienste** den Eintrag **Neuer ferner Knoten** aus (oder klicken Sie in der Symbolleiste auf den Knopf **Neu** und wählen Sie die Option **Fernen Knoten definieren** aus).

   Communications Server für Linux zeigt den Konfigurationsdialog für ferne Knoten an.
3. Geben Sie in den Feldern der Dialoganzeige die entsprechenden Werte ein.
4. Klicken Sie auf **OK**, um den fernen Knoten zu definieren. Der ferne Knoten wird im Teilfenster für ferne Systeme des Knotenfensters angezeigt.

   Wenn Sie ein fernes System definieren, definiert Communications Server für Linux auf dem lokalen Knoten automatisch die Steuerpunkt-LU des fernen Knotens als Partner-LU.

**Aliasnamen für Partner-LU definieren:** Für das Definieren des Aliasnamens einer Partner-LU benötigen Sie die folgenden Informationen:

- vollständig qualifizierter Name der Partner-LU (SNA-Netzname und LU-Name)
- von einem lokalen Transaktionsprogramm verwendeter Aliasname der Partner-LU

Führen Sie im Knotenfenster die folgenden Schritte aus, um den Aliasnamen einer Partner-LU hinzuzufügen:

1. Wählen Sie das Teilfenster für ferne Systeme aus.
2. Wählen Sie im Menü **Dienste** die Optionen **APPC**, **Neue Partner-LUs** und **Aliasname der Partner-LU** aus (oder klicken Sie in der Symbolleiste auf den Knopf **Neu** und wählen Sie die Option **Aliasnamen für Partner-LU definieren** aus).

   Communications Server für Linux zeigt den Konfigurationsdialog für Aliasnamen von Partner-LUs an.

3. Geben Sie in der Dialoganzeige den Namen und den Aliasnamen der Partner-LU ein.
4. Klicken Sie auf **OK**, um den Aliasnamen der Partner-LU zu definieren. Der Aliasname der Partner-LU wird im Teilfenster für ferne Systeme des Knotenfensters (als Teil der Netzdefinition) angezeigt.

**Partner-LU auf einem fernen Knoten definieren:** Für das Definieren einer Partner-LU auf einem bestimmten fernen Knoten benötigen Sie die folgenden Informationen:

- vollständig qualifizierter Name der Partner-LU
- Aliasname der Partner-LU (wenn ein lokales Transaktionsprogramm einen Aliasnamen verwendet)
- vollständig qualifizierter Name des Knotens mit den Verzeichnisinformationen für die Partner-LU

Führen Sie im Knotenfenster die folgenden Schritte aus, um die Definition einer Partner-LU für einen bestimmten fernen Knoten hinzuzufügen:

1. Wählen Sie den fernen Knoten aus.
2. Wählen Sie im Menü **Dienste** die Optionen **APPC**, **Neue Partner-LUs** und **Partner-LU auf fernem Knoten** aus (oder klicken Sie in der Symbolleiste auf den Knopf **Neu** und wählen Sie die Option **Partner-LU auf fernem Knoten definieren** aus).

   Communications Server für Linux zeigt den Konfigurationsdialog für Partner-LUs an.
3. Geben Sie in den Feldern der Dialoganzeige die entsprechenden Werte ein.
4. Klicken Sie auf **OK**, um die Partner-LU zu definieren. Der Aliasname der Partner-LU wird im Teilfenster für ferne Systeme des Knotenfensters unter dem fernen System angezeigt, zu dem die Partner-LU gehört.

**Mehrere Partner-LUs unter Verwendung von Platzhaltern definieren:** Mit Hilfe von Platzhaltern können Sie die Position von Partner-LUs definieren, die sich alle auf demselben fernen Knoten befinden und deren Namen mit denselben Zeichen beginnen. Bei Verwendung von Platzhaltern müssen Sie nicht jede Partner-LU einzeln konfigurieren.

Wenn Sie Partner-LUs unter Verwendung von Platzhaltern definieren, müssen Sie die folgenden Informationen angeben:

- Generischer Name der Partner-LU. Der generische Name der Partner-LU besteht aus zwei EBCDIC-Zeichenfolgen des Typs A mit einer Länge von jeweils 1–8 Zeichen, die mit den vollständig qualifizierten LU-Namen mehrerer Partner-LUs übereinstimmen.

  Die erste Zeichenfolge kann ein vollständiger SNA-Netzname sein, der mit dem Netznamen der Partner-LUs identisch ist, oder ein generisches Präfix, das mit dem Anfang des Netznamens übereinstimmt. Wenn Sie für den Netznamen ein generisches Präfix eingeben, dürfen Sie im Feld für die zweite Zeichenfolge keinen Wert eingeben.

  Haben Sie für die erste Zeichenfolge einen vollständigen SNA-Netznamen vorgegeben, können Sie auch für die zweite Zeichenfolge einen Wert angeben. (Geben Sie für die zweite Zeichenfolge nur einen Wert ein, wenn Sie für die erste Zeichenfolge einen gültigen SNA-Netznamen angegeben haben.) Die zweite Zeichenfolge wird als generisches Präfix interpretiert, das mit dem Anfang des zweiten Teils des vollständig qualifizierten Namens der Partner-LUs übereinstimmen muss.

- Name des Knotens, auf dem sich die Partner-LUs befinden

Führen Sie im Knotenfenster die folgenden Schritte aus, um mehrere Partner-LUs hinzuzufügen:

1. Wählen Sie den fernen Knoten aus, für den Sie die Partner-LUs definieren.
2. Wählen Sie im Menü **Dienste** die Optionen **APPC**, **Neue Partner-LUs** und **Generische Partner-LU auf fernem Knoten** aus (oder klicken Sie in der Symbolleiste auf den Knopf **Neu** und wählen Sie die Option **Generische Partner-LU auf fernem Knoten definieren** aus).

   Communications Server für Linux zeigt den Konfigurationsdialog für generische Partner-LU an.
3. Geben Sie in den Feldern der Dialoganzeige die entsprechenden Informationen ein.
4. Klicken Sie auf **OK**, um die Partner-LUs zu definieren. Die Partner-LUs werden im Teilfenster für ferne Systeme des Knotenfensters unter dem fernen Knoten angezeigt, zu dem sie gehören.

## Abhängiges APPC konfigurieren

Für das Konfigurieren einer abhängigen LU 6.2 benötigen Sie die folgenden Informationen:

- Name der lokalen LU
- Aliasname der lokalen LU (wenn ein von dieser LU unterstütztes Transaktionsprogramm einen Aliasnamen verwendet)
- Name der Verbindungsstation für die Verbindung zum Host
- LU-Nummer
- die Information, ob die LU dem Standardpool für abhängige LUs 6.2 zugeordnet werden soll

Wenn Sie abhängige LUs des Typs 6.2 für APPC- oder CPI-C-Anwendungen konfigurieren, können Sie sie als LUs des Standardpools definieren. Einer Anwendung, die keine bestimmte lokale LU angibt, wird eine nicht benutzte LU des Standard-LU-Pools zugeordnet.

Führen Sie im Knotenfenster die folgenden Schritte aus, um eine abhängige lokale LU zu konfigurieren:

1. Wählen Sie im Konnektivitätsteilfenster eine Verbindungsstation aus.
2. Wählen Sie im Untermenü **APPC** des Menüs **Dienste** den Eintrag **Neue abhängige lokale LU** aus (oder klicken Sie in der Symbolleiste auf den Knopf **Neu** und wählen Sie die Option **Neue abhängige lokale LU** aus).

   Communications Server für Linux zeigt den Dialog für lokale LUs an.
3. Geben Sie in den Feldern der Dialoganzeige die entsprechenden Werte ein.
4. Klicken Sie auf **OK**, um die lokale LU zu definieren. Die abhängige LU wird im Konnektivitätsteilfenster unterhalb der Verbindungsstation angezeigt, zu der sie gehört.

# Konfiguration für CPI Communications

Wenn Ihr System eine CPI-C-Anwendung unterstützt, die symbolische CPI-C-Bestimmungsorte verwendet, müssen Sie die CPI-C-Nebeninformationen definieren. Die Nebeninformationen ordnen dem symbolischen Bestimmungsort Informationen zum Partner-TP, zur Partner-LU, zum Modus und zur Dialogsicherheit zu.

Den symbolischen Bestimmungsort für CPI-C kann Ihnen der Anwendungsentwickler nennen. (Für Anwendungen eines anderen Herstellers können Sie den Bestimmungsort der Produktdokumentation entnehmen.)

Bevor Sie CPI-C-Nebeninformationen konfigurieren, benötigen Sie die folgenden Informationen:

- den Vom Transaktionsprogramm (TP) verwendeten symbolischen Bestimmungsort
- den Namen des Partner-TP
- den Namen oder Aliasnamen der Partner-LU
- den Modusnamen

Führen Sie im Knotenfenster die folgenden Schritte aus, um CPI-C-Nebeninformationen zu konfigurieren:

1. Wählen Sie im Untermenü **APPC** des Menüs **Dienste** den Eintrag **CPI-C** aus.

   Communications Server für Linux zeigt das Fenster für CPI-C-Bestimmungsorte an.
2. Klicken Sie auf den Knopf **Neu**.

   Communications Server für Linux zeigt den Konfigurationsdialog für CPI-C-Bestimmungsorte an.
3. Geben Sie in den Feldern der Dialoganzeige die entsprechenden Werte ein.
4. Klicken Sie auf **OK**, um die CPI-C-Nebeninformationen zu definieren.

## LUA konfigurieren

Die API LUA ist für Anwendungen geeignet, die über LUs des Typs 0-3 mit einem Host kommunizieren. (Ausführliche Informationen zur API LUA finden Sie im *Communications Server for Linux LUA Programmer's Guide*.)

Führen Sie vor dem Konfigurieren der API LUA die folgenden Konfigurationsschritte aus:

1. Konfigurieren Sie den Knoten wie im Abschnitt „Knoten konfigurieren" auf Seite 80 beschrieben.
2. Konfigurieren Sie Konnektivität für abhängigen Verkehr wie im Abschnitt „Konnektivität konfigurieren" auf Seite 82 beschrieben. (Wenn Sie ein übergeordnetes SNA-Gateway oder DLUR verwenden, konfigurieren Sie anstelle einer Direktverbindung zum Host eine Verbindung zum übergeordneten Knoten.)

Für das Konfigurieren der API LUA benötigen Sie die folgenden Informationen:

- den LU-Namen oder den Namen des LU-Pools
- die LU-Nummer jeder LU (Die LU-Nummer muss mit der auf dem Host konfigurierten LU-Nummer übereinstimmen.)

Definieren Sie wie folgt die LU für LUA:

1. Wählen Sie im Konnektivitätsteilfenster des Knotenfensters die Verbindungsstation zum Host aus.
2. Klicken Sie auf den Knopf **Neu**.
3. Wählen Sie in der daraufhin erscheinenden Dialoganzeige die Option **Neue LU für LUA** aus.
4. Geben Sie in den Feldern der Dialoganzeige die entsprechenden Werte ein. Geben Sie als LU-Typ `Unbeschränkt` an.

5. Klicken Sie auf **OK**. Die LU wird im Konnektivitätsteilfenster des Knotenfensters unterhalb der Verbindungsstation zum Host angezeigt.
6. Wenn Sie LU-Pools verwenden wollen, definieren Sie diese wie im Abschnitt „LU-Pool definieren" auf Seite 87 beschrieben.

## LU-Pool definieren

Sie können LU-Pools definieren, um die Benutzerkonfiguration zu vereinfachen und beim Aufbauen von Hostsitzungen mehr Flexibilität zu haben. Sie können beispielsweise mehrere LUs in einem Pool definieren und dann mehrere LUA-Anwendungen für die Verwendung dieses Pools konfigurieren. Dadurch wird die Konfiguration von Anwendungen einfacher, und alle Anwendungen können jede beliebige LU des Pools benutzen.

**Anmerkung:** Sie können einer bestimmten LU oder einem LU-Pool eine Benutzersitzung zuordnen.

- Wenn Sie die Benutzersitzung einer bestimmten LU zuordnen, die in einem Pool enthalten ist, verwendet die Sitzung diese LU, sofern sie verfügbar ist. Andernfalls verwendet die Sitzung eine beliebige freie LU aus dem Pool, als hätten Sie die Sitzung dem LU-Pool und nicht dieser speziellen LU zugeordnet.
- Falls der Benutzer nur eine angegebene LU verwenden soll, so dass die Benutzersitzung nicht aufgebaut wird, wenn die LU bereits benutzt wird, müssen Sie sicherstellen, dass die LU nicht in einem Pool enthalten ist.

Die LU-Pools für den lokalen CS-Linux-Knoten werden im Fenster für LU-Pools angezeigt. Dieses Fenster listet die auf dem lokalen System konfigurierten LU-Pools auf. Sie können in diesem Fenster LUs auswählen und zu einem LU-Pool hinzufügen.

Zu einem Pool für 3270 können Sie LUs der folgenden Typen hinzufügen (ein Pool darf keine Mischung verschiedener LU-Typen enthalten):

- 3270-Anzeige-LU
- unbeschränkte LU

Bevor Sie LUs zu einem Pool hinzufügen, müssen Sie die LUs auf dem lokalen Knoten definieren.

Führen Sie im Knotenfenster die folgenden Schritte aus, um einen LU-Pool zu konfigurieren:

1. Wählen Sie im Menü **Fenster** den Eintrag **LU-Pools** aus.

   Communications Server für Linux zeigt das Fenster für LU-Pools an.
2. Klicken Sie auf den Knopf **Neu**.

   Communications Server für Linux zeigt den Konfigurationsdialog für LU-Pools an.

   Im rechten Feld sind LUs aufgelistet, die noch keinem Pool zugeordnet sind. Jede dieser LUs vom Typ `Unbeschränkte LU` kann in den neuen Pool für LUA integriert werden.
3. Wählen Sie die LU oder LUs aus, die Sie zum Pool hinzufügen wollen, und klicken Sie auf den Knopf **Neu**, um die ausgewählten LUs in das linke Feld zu verschieben.

Wenn Sie eine LU aus dem linken Feld entfernen wollen, wählen Sie die LU aus und klicken Sie auf den Knopf **Entfernen**.

4. Klicken Sie auf **OK**, um den LU-Pool zu definieren.

   Alle im linken Feld enthaltenen LUs werden zum LU-Pool hinzugefügt.

   Der Pool wird im Fenster für LU-Pools angezeigt.

## SNA Gateway konfigurieren

Communications Server für Linux ermöglicht nicht nur den Direktzugriff auf einen Host, sondern kann auch SNA-Gateway-Funktionen bereitstellen. Mit Hilfe dieses Features können andere Computer über einen CS-Linux-Knoten auf einen Host zugreifen, so dass keine gesonderte Verbindung vom Host zu jedem einzelnen Computer erforderlich ist.

Das Feature SNA Gateway ist in Abb. 8 veranschaulicht.

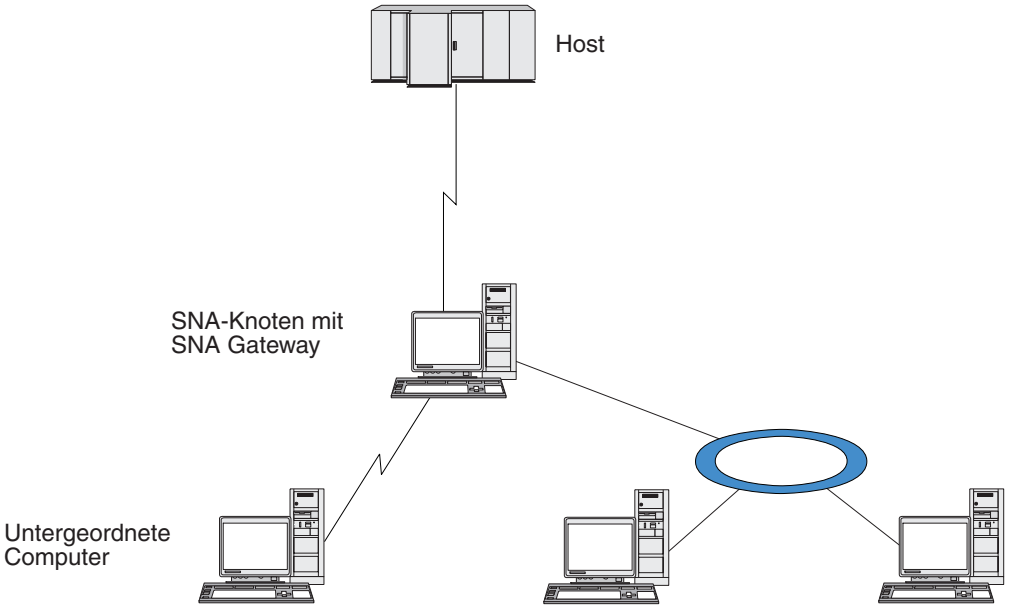


*Abbildung 8. SNA Gateway*

Der untergeordnete Computer muss über eine SNA-PU des Typs 2.0 oder 2.1 verfügen, um abhängige LUs unterstützen zu können. Der untergeordnete Computer könnte beispielsweise ein weiterer CS-Linux-Computer oder ein PC sein, auf dem Communications Server für Windows NT ausgeführt wird.

Wenn der lokale CS-Linux-Knoten das Feature SNA Gateway nutzt, werden alle Daten, die zwischen dem Host und dem untergeordneten Computer übertragen werden, über den lokalen Knoten geleitet. Dadurch benötigt der untergeordnete Computer keine Direktverbindung und kann die Hostverbindung gemeinsam mit dem CS-Linux-Computer oder mit anderen untergeordneten Computern nutzen. Sie könnten z. B. mehrere untergeordnete Computer installieren, die über ein lokales Token-Ring-Netz mit dem CS-Linux-Computer verbunden sind. In diesem Fall könnten alle Computer auf dieselbe Standfernleitung des CS-Linux-Computers zum Host zugreifen.

Die Verwendung von SNA Gateway vereinfacht darüber hinaus die Konfiguration auf dem Host, denn Sie müssen die untergeordneten Computer und die zu diesen führenden DFV-Verbindungen nicht definieren. Die Hostkonfiguration muss nur den CS-Linux-Computer und dessen Hostübertragungsleitung umfassen. Die LUs auf den untergeordneten Computern werden zusammen mit den Ressourcen des CS-Linux-Computers konfiguriert. Der Host hat keine Kenntnis von der Verwendung des Features SNA Gateway.

Bevor Sie SNA Gateway konfigurieren, müssen Sie die folgenden Konfigurationsschritte ausführen:

- Definieren Sie den lokalen Knoten wie im Abschnitt „Knoten konfigurieren" auf Seite 80 beschrieben.
- Konfigurieren Sie einen Port und eine Verbindungsstation für abhängigen Verkehr zwischen dem lokalen Knoten und dem Host. Gehen Sie dazu wie im Abschnitt „Konnektivität konfigurieren" auf Seite 82 beschrieben vor. Konfigurieren Sie außerdem Ports und Verbindungsstationen für abhängigen Verkehr zwischen dem lokalen Knoten und den untergeordneten Knoten. Wenn Sie Unterstützung für untergeordnete LUs benötigen, die noch nicht definiert wurden, können Sie für den Port eine Schablone für die Unterstützung impliziter PUs und untergeordneter LUs definieren (siehe Abschnitt „Implizite untergeordnete LUs unterstützen").
- Definieren Sie die LUs auf dem lokalen Knoten, die für die Kommunikation mit dem Host verwendet werden (übergeordnete LUs). Definieren Sie die übergeordneten LUs des Typs 0–3 als `Unbeschränkt`. (Der Typ der LUs auf untergeordneten Knoten ist beliebig.)
- Wenn Sie LU-Pools verwenden wollen, definieren Sie diese wie im Abschnitt „LU-Pool definieren" auf Seite 96 beschrieben.

## Implizite untergeordnete LUs unterstützen

Zur Unterstützung untergeordneter LUs, die noch nicht für Communications Server für Linux definiert wurden, können Sie für den Port eine Schablone für implizite untergeordnete PUs und LUs definieren. (Die wichtigsten Schritte der Port-Konfiguration sind im Abschnitt „Konnektivität konfigurieren" auf Seite 82 beschrieben.) Diese Schablonen bieten Unterstützung für untergeordnete LUs, so dass Sie nicht jede LU auf dem lokalen Knoten für die Unterstützung aller LUs auf einem untergeordneten Knoten konfigurieren müssen.

Bevor Sie eine untergeordnete LU für SNA Gateway konfigurieren, benötigen Sie die folgenden Informationen:

- Bereich der LUs (Nummern), die untergeordnete LUs unterstützen
- Name der Host-LU

Führen Sie die folgenden Schritte aus, um eine Schablone für implizite untergeordnete LUs zu definieren:

1. Wenn Sie den Port bereits konfiguriert haben, klicken Sie im Konnektivitätsteilfenster des Knotenfensters doppelt auf die Port-Definition. Communications Server für Linux zeigt den Konfigurationsdialog für Ports an.

   Sollten Sie den Port noch nicht konfiguriert haben, holen Sie dies jetzt nach. Gehen Sie dazu wie folgt vor:

   a. Wählen Sie im Knotenfenster das Konnektivitätsteilfenster aus.
   b. Klicken Sie auf den Knopf **Neu**.

c. Wählen Sie in der daraufhin erscheinenden Dialoganzeige die Option zum Definieren eines Ports und den Verbindungsprotokolltyp aus.

   Communications Server für Linux zeigt den Konfigurationsdialog für Ports an.

d. Geben Sie gemäß der Beschreibung im Abschnitt „Konnektivität konfigurieren" auf Seite 82 die wichtigsten Port-Parameter ein.

2. Klicken Sie unten in der Dialoganzeige auf den Knopf **Erweitert**.

   Communications Server für Linux zeigt den Dialog für Port-Parameter an. Im unteren Teilfenster sind die Einstellungen aufgelistet, die Einfluss auf Schablonen für untergeordnete LUs haben.

3. Wählen Sie die Option *Untergeordnete LUs für Zugriff auf implizite PUs konfigurieren* aus.
4. Klicken Sie auf **OK**.

   Communications Server für Linux zeigt den Konfigurationsdialog für Schablonen für untergeordnete LUs an.

5. Geben Sie in den Feldern der Dialoganzeige die entsprechenden Werte ein.
6. Klicken Sie auf **OK**, um die Schablone für implizite untergeordnete LUs zu definieren.

### Untergeordnete LUs definieren

Bevor Sie eine untergeordnete LU für SNA Gateway konfigurieren, benötigen Sie die folgenden Informationen:

- LU-Name jeder untergeordneten LU (Dies ist ein lokaler Bezeichner, der nicht mit der Konfiguration des untergeordneten Systems übereinstimmen muss.)
- LU-Nummer jeder untergeordneten LU
- Verbindungsstation zum untergeordneten Knoten
- Name der übergeordneten LU (für die Host-LU)

Führen Sie die folgenden Schritte aus, um eine untergeordnete LU für SNA Gateway zu konfigurieren:

1. Wählen Sie im Konnektivitätsteilfenster des Knotenfensters die Verbindungsstation zum untergeordneten Knoten aus.
2. Klicken Sie auf den Knopf **Neu**.
3. Wählen Sie die Option **Neue untergeordnete LU** aus und klicken Sie auf **OK**.

   Communications Server für Linux zeigt den Dialog für untergeordnete LUs an.

4. Geben Sie in den Feldern der Dialoganzeige die entsprechenden Werte ein.
5. Klicken Sie auf **OK**, um die untergeordnete LU zu definieren.

   Die LU-Definition wird im Konnektivitätsteilfenster des Knotenfensters unterhalb der Verbindungsstation zum untergeordneten Knoten angezeigt.

## DLUR konfigurieren

Communications Server für Linux ermöglicht nicht nur den Direktzugriff auf einen Host, sondern kann auch DLUR-Funktionen bereitstellen. Bei Verwendung dieses Features können sich Sitzungen für abhängige LUs über mehrere Knoten in einem APPN-Netz erstrecken und benötigen keine Direktverbindung zum Host.

Normalerweise erfordert eine abhängige LU-Sitzung eine direkte DFV-Verbindung zum Host. Wenn in einem APPN-Netz viele Knoten (einschließlich eines Hostknotens) verbunden sind, haben einige von ihnen unter Umständen keine Direktverbindung zum Host, sondern nur eine indirekte Verbindung über einen anderen Knoten. LUs auf diesen indirekt mit dem Host verbundenen Knoten können keine abhängigen LU-Sitzungen mit dem Host aufbauen.

Dependent LU Requester (DLUR) ist ein APPN-Feature, das diese Einschränkung aufhebt.

Das Feature DLUR auf einem APPN-Knoten (z. B. einem CS-Linux-Knoten) arbeitet mit DLUS (Dependent LU Server) auf dem Host zusammen, um Sitzungen von abhängigen LUs auf dem DLUR-Knoten über das APPN-Netz zum DLUS-Host weiterzuleiten. Die Route zum Host kann sich über mehrere Knoten erstrecken und von den APPN-Funktionen für Netzverwaltung, für dynamische Ressourcenlokalisierung und Routenberechnung profitieren. DLUR muss auf dem Knoten verfügbar sein, auf dem sich die LUs befinden. DLUS muss auf dem Hostknoten verfügbar sein. Auf den Zwischenknoten der Sitzungsroute ist das Feature DLUR nicht erforderlich.

Wenn der CS-Linux-DLUR-Knoten ein Netzknoten oder ein Zweignetzknoten ist, kann er auch Durchgriff-DLUR-Funktionen für abhängige LUs auf untergeordneten Computern, die mit dem CS-Linux-Knoten verbunden sind, bereitstellen. Diese LUs können ebenso wie knoteninterne LUs DLUR auf dem CS-Linux-Knoten nutzen, um über das Netz auf den Host zuzugreifen. Die untergeordneten Computer führen DLUR nicht aus und müssen keine Kenntnis davon haben, dass DLUR verwendet wird.

Abb. 9 zeigt einen als APPN-Netzknoten konfigurierten CS-Linux-Server mit einer Implementierung von Durchgriff-DLUR zur Unterstützung von Sitzungen zwischen LUs auf dem Host (dem übergeordneten Knoten) und LUs auf den Knoten im APPN-Netz (den untergeordneten Knoten).

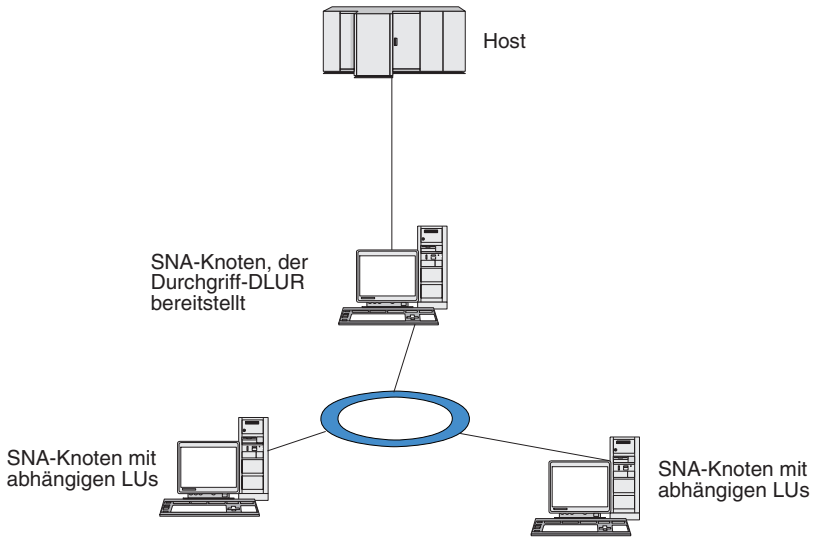


*Abbildung 9. CS-Linux-Knoten, der DLUR bereitstellt*

**Anmerkung:**

1. Auf einem LEN-Knoten können Sie DLUR nicht konfigurieren.
2. Durchgriff-DLUR können Sie nur auf einem Netzknoten oder Zweignetzknoten konfigurieren.
3. Wenn Sie Branch Extender verwenden, können Sie DLUR nicht auf einem Endknoten des Zweignetzes (dessen Netzknotenserver ein Zweignetzknoten ist) konfigurieren. Dieser Knoten kann jedoch abhängige LU-Anwendungen unterstützen, sofern Sie Durchgriff-DLUR auf den Zweignetzknoten konfigurieren (so dass der Endknoten im Zweignetz zwar nicht DLUR ausführt, jedoch Durchgriff-DLUR auf dem Zweignetzknoten verwendet).

Die für die DLUR-Konfiguration erforderlichen Schritte richten sich danach, ob sich die abhängigen LUs auf dem lokalen Knoten oder auf untergeordneten Knoten befinden.

## DLUR-Unterstützung auf dem lokalen Knoten konfigurieren

Für diese Aufgabe benötigen Sie die folgenden Informationen:

- PU-ID der PU auf dem lokalen Knoten
- PU-Name (Dies ist ein lokaler Bezeichner, der nicht mit der Hostkonfiguration übereinstimmen muss.)
- Name des DLUS auf dem Host (und ggf. Name des Ausweich-DLUS)
- LU-Name, LU-Nummer und LU-Typ aller untergeordneten LUs. Die LU-Nummer muss mit der auf dem Host konfigurierten Nummer übereinstimmen.

Zum Konfigurieren der DLUR-Unterstützung auf dem lokalen Knoten müssen Sie die folgenden Konfigurationsschritte ausführen:

1. Definieren Sie den lokalen Knoten wie im Abschnitt „Knoten konfigurieren" auf Seite 80 beschrieben. Wenn Sie Durchgriff-DLUR-Unterstützung für untergeordnete Knoten bereitstellen wollen, definieren Sie den Knoten als APPN-Netzknoten oder Zweignetzknoten.
2. Konfigurieren Sie die Konnektivität zum APPN-Netz. Für die APPN-Konnektivität sind mindestens ein Port und eine Verbindungsstation für unabhängigen Verkehr zwischen dem lokalen Knoten und dem benachbarten APPN-Netzknoten erforderlich. Lesen Sie die diesbezüglichen Informationen im Abschnitt „Konnektivität konfigurieren" auf Seite 82.
3. Definieren Sie eine DLUR-PU auf dem lokalen Knoten (die DLUR-PU unterstützt die Konnektivität zum Host).

   Führen Sie im Knotenfenster die folgenden Schritte aus, um die DLUR-PU zu konfigurieren:

   a. Wählen sie das Menü **Dienste** und dann im Untermenü **Konnektivität** den Eintrag **Neue DLUR-PU** aus (oder klicken Sie in der Symbolleiste auf den Knopf **Neu** und wählen Sie die Option **DLUR-PU** aus).

      Wenn Sie auf **OK** klicken, zeigt Communications Server für Linux den Konfigurationsdialog für DLUR-PUs an.

   b. Geben Sie in den Feldern der Dialoganzeige die entsprechenden Werte ein.

   c. Klicken Sie auf **OK**, um die DLUR-PU zu definieren.

      Die DLUR-PU wird im Konnektivitätsteilfenster unter dem DLUR-Eintrag angezeigt.

4. Wenn Sie DLUR für die Unterstützung von LUs auf dem lokalen Knoten konfigurieren wollen, müssen Sie die LUs auf dem lokalen Knoten hinzufügen. Die LUs müssen wie im Abschnitt „LUA konfigurieren" auf Seite 95 beschrieben für die Unterstützung von LUA konfiguriert werden. In Abhängigkeit von den Anforderungen der von den LUs unterstützten Benutzeranwendungen können weitere Konfigurationsschritte erforderlich sein.

### Durchgriff-DLUR-Unterstützung für untergeordnete Knoten konfigurieren

Für diese Aufgabe benötigen Sie die folgenden Informationen:

- Name der untergeordneten PU für jeden untergeordneten Knoten oder für jede PU auf dem untergeordneten Knoten (Dies ist ein lokaler Bezeichner, der nicht mit der Hostkonfiguration übereinstimmen muss.)
- Name des DLUS auf dem Host

Zum Konfigurieren der Durchgriff-DLUR-Unterstützung für untergeordnete Knoten müssen Sie die folgenden Konfigurationsschritte ausführen:

1. Definieren Sie den lokalen Knoten als APPN-Netzknoten (siehe Abschnitt „Knoten konfigurieren" auf Seite 80).
2. Konfigurieren Sie die Konnektivität zu den untergeordneten Knoten. Konfigurieren Sie Ports und Verbindungsstationen für abhängigen Verkehr zwischen dem lokalen Knoten und allen untergeordneten Knoten. Gehen Sie dazu wie im Abschnitt „Konnektivität konfigurieren" auf Seite 82 beschrieben vor. (Sie müssen keine DLUR-PU für die Unterstützung von Durchgriff-DLUR für untergeordnete Knoten definieren.)
3. Ein untergeordneter Knoten kann mehrere PUs unterstützen. In einem solchen Fall ist jede untergeordnete PU einer anderen Verbindung zugeordnet, so dass Sie zwischen dem CS-Linux-DLUR-Knoten und dem untergeordneten Knoten mehrere Verbindungen konfigurieren und für jede Verbindung den Namen der untergeordneten PU kennen müssen.

## TN Server konfigurieren

3270-Emulationsprogramme, die über TCP/IP (und nicht über ein SNA-Netz) kommunizieren, werden als TN3270-Programme (Telnet-3270-Emulationsprogramme) bezeichnet.

Einige TN3270-Programme bieten Unterstützung für TN3270E (Standarderweiterungen für Telnet 3270). TN3270E ist ein offenes Protokoll, das über Telnet die 3270-Einheitenemulation (von Terminals und Druckern) unterstützt. Das Protokoll ermöglicht einem Telnet-Client, eine bestimmte Einheit (durch Angabe des LU-Namens) auszuwählen, und stellt erweiterte Unterstützung für verschiedene Funktionen bereit, z. B. für die Schlüssel ATTN und SYSREQ und die Bearbeitung von SNA-Antworten.

**Anmerkung:** Im vorliegenden Handbuch wird die Bezeichnung TN3270 für Informationen verwendet, die sich auf die Protokolle TN3270, TN3287 und TN3270E beziehen.

TN Server von Communications Server für Linux ermöglicht TN3270-Benutzern den Zugriff auf 3270-Hosts. Über TN Server können TN3270-Benutzer eine Hostverbindung gemeinsam mit Communications Server für Linux oder anderen TN3270-Benutzern verwenden und benötigen keine Direktverbindung. Mit TN Server können TN3270-Benutzer auch auf Hosts ohne TCP/IP zugreifen.

Abb. 10 zeigt einen CS-Linux-Knoten mit TN-Server-Unterstützung für TN3270-Clients. Der TN-Server-Knoten kommuniziert über das TCP/IP-Netz mit den Clients.

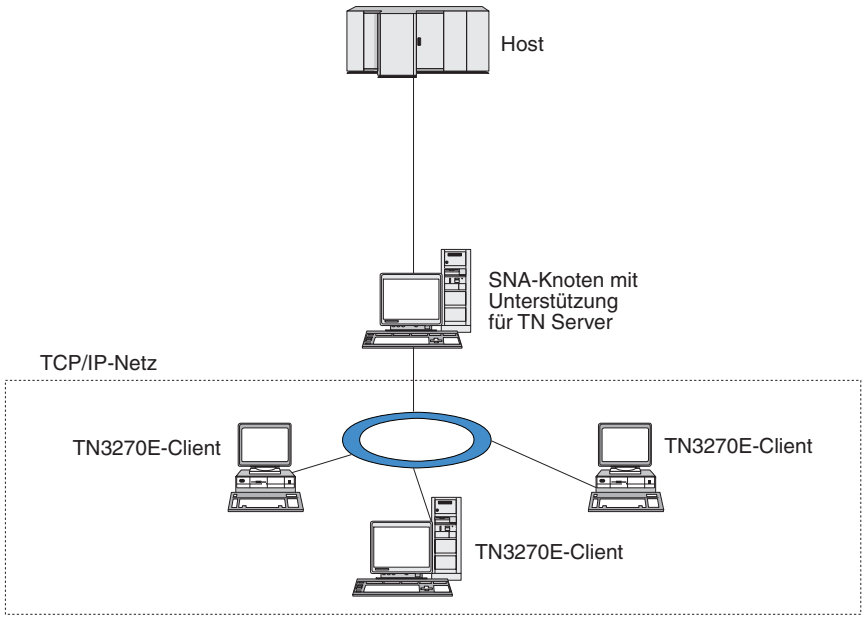


*Abbildung 10. Für TN Server konfigurierter CS-Linux-Knoten*

Das Feature TN Server von Communications Server für Linux ermöglicht die Zuordnung eines TN3270-Benutzers zu einer 3270-LU unter Communications Server für Linux. Alle Daten des TN3270-Benutzers werden an die LU weitergeleitet. Dies bedeutet, dass die Konfiguration für den Host und den TN3270-Benutzer so ist, als wären sie direkt miteinander verbunden. Keiner von beiden muss wissen, dass die Daten über TN Server weitergeleitet werden.

TN Server von Communications Server für Linux unterstützt alle TN3270-Client-Emulationsprogramme, die die in den IETF-RFCs 1123, 1576, 1646, 1647 und 2355 definierten Protokolle richtig implementieren.

Wenn ein TN3270-Programm mit TN Server kommuniziert, identifiziert Communications Server für Linux das Programm über die TCP/IP-Adresse des Computers, auf dem das TN3270-Programm ausgeführt wird. Communications Server für Linux kann zwei TN3270-Programme, die von zwei verschiedenen Benutzern auf demselben Computer ausgeführt werden, nicht unterscheiden. In den Handbüchern zu Communications Server für Linux bezieht sich die Bezeichnung 'Benutzer von TN Server' auf den Computer, auf dem ein TN3270-Programm ausgeführt wird, nicht auf einen individuellen Programmbenutzer.

Wie in Abb. 11 auf Seite 104 gezeigt, stellt sich die Konfiguration aus Sicht des Hosts und des TN-Server-Benutzers unterschiedlich dar.

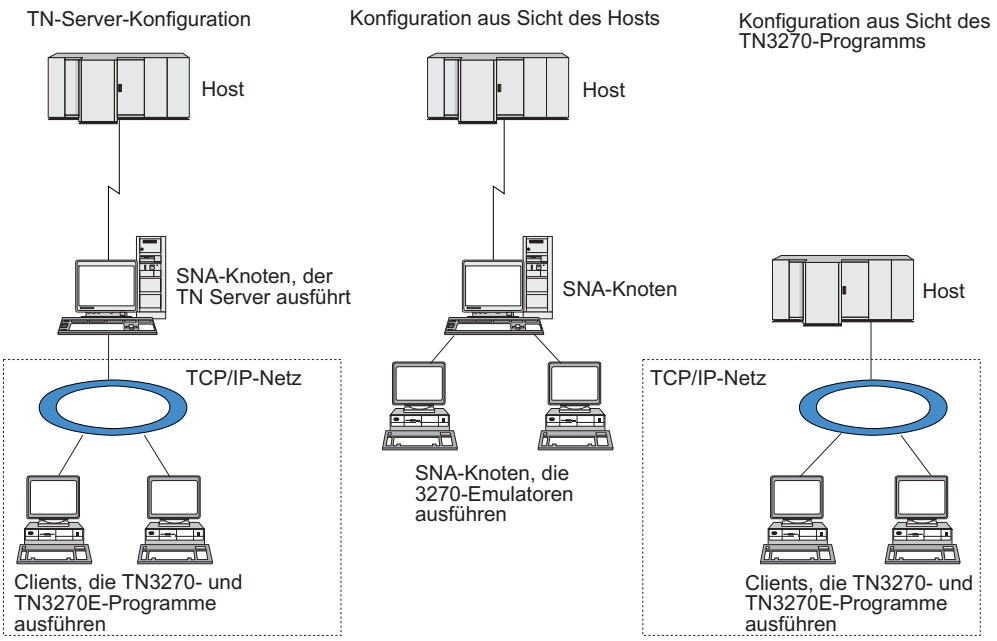


*Abbildung 11. TN Server*

Für jeden Benutzer von TN Server, der mit dem Feature TN3270 Server eine Verbindung zu Communications Server für Linux herstellt, ist normalerweise der Zugriff auf eine 3270-LU konfiguriert, so dass der Benutzer auf eine Hostsitzung beschränkt ist. Sie müssen einem Benutzer von TN Server jedoch nicht eine einzelne dedizierte 3270-LU zuordnen, sondern können für ihn auch den Zugriff auf einen Pool von 3270-LUs konfigurieren. Dadurch können Benutzer auf so viele TN-Server-Sitzungen zugreifen wie LUs im Pool verfügbar sind.

Bevor Sie den Zugriff auf TN Server konfigurieren können, müssen Sie die folgenden Konfigurationsschritte ausführen:

- Definieren Sie den lokalen Knoten wie im Abschnitt „Knoten konfigurieren" auf Seite 80 beschrieben.
- Konfigurieren Sie einen Port und eine Verbindungsstation für abhängigen Verkehr zwischen dem lokalen Knoten und dem Host. Gehen Sie dazu wie im Abschnitt „Konnektivität konfigurieren" auf Seite 82 beschrieben vor.

Führen Sie die folgenden Schritte aus, um den Zugriff auf TN Server zu konfigurieren:

- Definieren Sie die 3270-LUs auf dem lokalen Knoten, die für die Kommunikation mit dem Host verwendet werden. Hinweise zum Hinzufügen der LUs finden Sie im Abschnitt „3270-LUs definieren".
- Wenn Sie LU-Pools verwenden wollen, definieren Sie diese wie im Abschnitt „LU-Pool definieren" auf Seite 105 beschrieben.

## 3270-LUs definieren

Stellen Sie vor dem Konfigurieren der 3270-LU die folgenden Informationen zusammen:

- LU-Name (Dies ist ein lokaler Bezeichner, der nicht mit der Hostkonfiguration übereinstimmen muss.)
- LU-Nummer (bzw. bei einem Bereich von LUs die LU-Nummern)
- LU-Typ (Modell des 3270-Datensichtgeräts oder 3270-Drucker)

- Poolname (wenn Sie die LU zu einem Pool hinzufügen)

Führen Sie im Knotenfenster die folgenden Schritte aus, um eine LU des Typs 0–3 für eine bereits definierte Verbindungsstation zu konfigurieren:

1. Wählen Sie im Konnektivitätsteilfenster die Verbindungsstation zum Host aus.
2. Klicken Sie auf den Knopf **Neu**.
3. Wählen Sie in der daraufhin erscheinenden Dialoganzeige den LU-Typ (**Neue 3270-Anzeige-LU** oder **Neue 3270-Drucker-LU**) aus.

   Wenn Sie diesen Eintrag auswählen und auf **OK** klicken, zeigt Communications Server für Linux den Dialog für LUs des Typs 0-3 an.
4. Geben Sie in den Feldern der Dialoganzeige die entsprechenden Werte ein.
5. Klicken Sie auf **OK**, um die LU zu definieren.

   Die LU wird im Konnektivitätsteilfenster des Knotenfensters unterhalb der Verbindungsstation zum Host angezeigt.

## LU-Pool definieren

Für 3270 können Sie LU-Pools definieren, um die Benutzerkonfiguration zu vereinfachen und beim Aufbauen von Hostsitzungen mehr Flexibilität zu haben. Sie können beispielsweise mehrere 3270-LUs in einem Pool definieren und dann mehrere TN3270-Clients für die Verwendung dieses Pools konfigurieren. Dadurch wird die Konfiguration von 3270-Sitzungen einfacher, und alle Clients können jede beliebige LU des Pools benutzen.

**Anmerkung:** Sie können einer bestimmten LU oder einem LU-Pool einen TN3270-Client zuordnen.

- Wenn Sie den Client einer bestimmten LU zuordnen, die in einem Pool enthalten ist, verwendet der Client diese LU, sofern sie verfügbar ist. Andernfalls verwendet der Client eine beliebige freie LU aus dem Pool, als hätten Sie den Client dem LU-Pool und nicht dieser speziellen LU zugeordnet.
- Falls der Client nur eine angegebene LU verwenden soll, so dass die Client-Sitzung nicht aufgebaut wird, wenn die LU bereits benutzt wird, müssen Sie sicherstellen, dass die LU nicht in einem Pool enthalten ist.

Die LU-Pools für den lokalen CS-Linux-Knoten werden im Fenster für LU-Pools angezeigt. Dieses Fenster listet die auf dem lokalen System konfigurierten LU-Pools auf. Sie können in diesem Fenster LUs auswählen und zu einem LU-Pool hinzufügen.

Zu einem Pool für 3270 können Sie LUs der folgenden Typen hinzufügen (ein Pool darf keine Mischung verschiedener LU-Typen enthalten):

- 3270-Anzeige-LU
- unbeschränkte LU

Bevor Sie LUs zu einem Pool hinzufügen, müssen Sie die LUs auf dem lokalen Knoten definieren.

Führen Sie im Knotenfenster die folgenden Schritte aus, um einen LU-Pool zu konfigurieren:

1. Wählen Sie im Menü **Fenster** den Eintrag **LU-Pools** aus.

   Communications Server für Linux zeigt das Fenster für LU-Pools an.

2. Klicken Sie auf den Knopf **Neu**.

   Communications Server für Linux zeigt den Konfigurationsdialog für LU-Pools an.

   Im rechten Feld sind LUs aufgelistet, die noch keinem Pool zugeordnet sind. Jede dieser LUs kann in den neuen Pool integriert werden.
3. Wählen Sie die LU oder LUs aus, die Sie zum Pool hinzufügen wollen, und klicken Sie auf den Knopf **Neu**, um die ausgewählten LUs in das linke Feld zu verschieben.

   Wenn Sie eine LU aus dem linken Feld entfernen wollen, wählen Sie die LU aus und klicken Sie auf den Knopf **Entfernen**.
4. Klicken Sie auf **OK**, um den LU-Pool zu definieren.

   Alle im linken Feld enthaltenen LUs werden zum LU-Pool hinzugefügt.

   Der Pool wird im Fenster für LU-Pools angezeigt.

## TN3270 Server konfigurieren

Bevor Sie TN3270 Server konfigurieren, benötigen Sie die folgenden Informationen:

- Information, ob der Server nur TN3270 oder auch TN3270E unterstützt (Eine Unterstützung für TN3270E bedeutet automatisch auch Unterstützung für TN3270.)
- Information, ob ein TN3270E-Client eine bestimmte LU anfordern kann
- Name der Anzeige- und der Drucker-LU (bzw. die Namen der LU-Pools) für jeden Client (Die Namen von Drucker-LUs sind nur für die TN3270E-Unterstützung erforderlich.)
- TCP/IP-Name oder TCP/IP-Adresse des Clients, wenn nur bestimmte Clients zulässig sind oder bestimmte Clients auf spezifische LUs beschränkt werden sollen
- Nummer des TCP/IP-Ports auf dem TN-Server-Knoten
- Information, ob SSL-Datenverschlüsselung, Client-Authentifizierung und Serverauthentifizierung erforderlich sind (Diese Option ist nur verfügbar, wenn Sie die zusätzliche, zur Unterstützung dieser Option erforderliche Software installiert haben.)

Zum Zuordnen einer Anzeige-LU zu einer Drucker-LU benötigen Sie außerdem die Namen dieser LUs. Ein TN-Server-Zuordnungseintrag definiert eine Zuordnung zwischen einer Drucker-LU und einer Anzeige-LU, auf deren Basis das TN3270E-Protokoll die beiden verbinden kann. Wenn der Server keine Unterstützung für TN3270E oder Drucker-LUs bietet, müssen Sie keinen Zuordnungseintrag definieren.

Der TN-Server-Standardeintrag definiert Parameter, die in allen TN3270-Client-Sitzungen verwendet werden. Sie können für jeden Server einen gesonderten Standardeintrag definieren.

Führen Sie im Knotenfenster die folgenden Schritte aus, um TN3270 Server zu konfigurieren:

1. Definieren Sie wie folgt einen TN-Server-Zugriffseintrag:
   a. Wählen Sie im Menü **Dienste** den Eintrag **TN-Server** aus.

      Communications Server für Linux zeigt daraufhin das TN-Server-Fenster an, in dessen oberem Teilfenster alle konfigurierten TN-Server-Zugriffseinträge und in dessen unterem Teilfenster alle TN-Server-Zuordnungseinträge aufgelistet sind.

b. Wählen Sie das Teilfenster mit den TN3270-Zugriffseinträgen aus und klicken Sie auf den Knopf **Neu**.

   Communications Server für Linux zeigt den Dialog für TN-Server-Zugriff an.

c. Geben Sie in den Feldern der Dialoganzeige die entsprechenden Werte ein.

d. Klicken Sie auf **OK**, um den TN-Server-Zugriffseintrag zu definieren. Der Eintrag wird im TN-Server-Fenster angezeigt.

2. Definieren Sie wie folgt einen TN-Server-Zugordnungseintrag:

   a. Wählen Sie im TN-Server-Fenster das Teilfenster mit den Zuordnungseinträgen aus und klicken Sie auf den Knopf **Neu**.

      Communications Server für Linux zeigt den Dialog für TN-Server-Zuordnungseinträge an.

   b. Geben Sie in den Feldern der Dialoganzeige die entsprechenden Werte ein.

   c. Klicken Sie auf **OK**, um den TN-Server-Zuordnungseintrag zu definieren. Der Eintrag wird im TN-Server-Fenster angezeigt.

3. Falls Sie Druckerantworten erzwingen möchten, geben Sie für alle TN3270-Sitzungen eine Keepalive-Methode an. Geben Sie außerdem an, wie auf den externen LDAP-Server mit der Liste zur Überprüfung der Berechtigung von TN3270-Clients zugegriffen werden soll, oder verwenden Sie TN3270-SLP (Service Location Protocol). Diese Angaben können Sie im Dialog mit den erweiterten Parametern für TN Server machen.

Weitere Informationen zum Konfigurieren der SSL-Unterstützung für TN Server finden Sie auf den Support-Webseiten zu IBM Communications Server unter der Adresse http://www.ibm.com/software/network/commserver/support/.

## TN Redirector konfigurieren

Das CS-Linux-Feature TN Redirector bietet TCP/IP-Hostdurchgriff auf TN3270-, TN3270E-, TN5250- und VT-Clients, die unter der Bezeichnung Telnet-Clients zusammengefasst werden. Der Telnet-Benutzer kommuniziert über eine TCP/IP-Verbindung mit Communications Server für Linux und Communications Server für Linux wiederum über eine weitere TCP/IP-Verbindung mit dem Host. Auf diese Weise kann bei Bedarf eine SSL-Sicherheitsprüfung (Secure Sockets Layer) durchgeführt werden, ohne diese auf die gesamte Benutzerhostverbindung zu erstrecken. Beispiele:

- Wenn Clients zu Communications Server für Linux eine Verbindung über ein TCP/IP-LAN ohne erforderliche Überprüfung herstellen, jedoch eine Verbindung zu einem fernen Host herstellen, der SSL erfordert, können Sie SSL für die TCP/IP-Verbindung zwischen Communications Server für Linux und dem Host verwenden. Auf diese Weise wird die Sicherheit für alle Clients überprüft. Die einzelnen Clients müssen keine Sicherheitsangaben machen.
- Wenn Communications Server für Linux an demselben Standort wie der Host installiert ist, die Clients die Verbindung jedoch von externen Standorten aus aufbauen, können Sie SSL für die Client-Verbindungen zu Communications Server für Linux verwenden und müssen die SSL-Software nicht auf dem Host installieren.

## TN Redirector konfigurieren

Bevor Sie den Zugriff auf TN Redirector konfigurieren können, müssen Sie den lokalen Knoten wie im Abschnitt „Knoten konfigurieren" auf Seite 80 beschrieben definieren. Außerdem benötigen Sie die folgenden Informationen:

- Wenn nur bestimmte Clients zulässig sind, benötigen Sie den TCP/IP-Namen oder die TCP/IP-Adresse des Clients.
- die Nummer des vom Client für die Verbindung zum TN-Redirector-Knoten verwendeten TCP/IP-Ports
- den TCP/IP-Namen oder die TCP/IP-Adresse des Hosts
- die Nummer des vom TN-Redirector-Knoten für die Verbindung zum Host verwendeten TCP/IP-Ports
- die Information, ob zwischen dem Client und dem TN-Redirector-Knoten SSL-Datenverschlüsselung, Client-Authentifizierung und Serverauthentifizierung erforderlich sind (Diese Option ist nur verfügbar, wenn Sie die zusätzliche, zur Unterstützung dieser Option erforderliche Software installiert haben.)
- die Information, ob zwischen dem TN-Redirector-Knoten und dem Host SSL-Datenverschlüsselung erforderlich ist

Der TN-Redirector-Standardeintrag definiert Parameter, die für alle TN-Redirector-Sitzungen verwendet werden. Sie können für jede Client-TCP/IP-Port-Nummer einen gesonderten Standardeintrag definieren.

Führen Sie im Knotenfenster die folgenden Schritte aus, um einen TN-Redirector-Zugriffseintrag zu konfigurieren:

1. Wählen Sie im Menü **Dienste** den Eintrag **TN-Server** aus.

   Communications Server für Linux zeigt daraufhin das TN-Server-Fenster an, in dem alle konfigurierten Zugriffseinträge und Zuordnungseinträge für TN3270 Server sowie alle Zugriffseinträge für TN Redirector aufgelistet sind.
2. Wählen Sie das Teilfenster mit den TN-Redirector-Zugriffseinträgen aus und klicken Sie auf den Knopf **Neu**.

   Communications Server für Linux zeigt den Dialog für TN-Redirector-Zugriff an.
3. Geben Sie in den Feldern der Dialoganzeige die entsprechenden Werte ein.
4. Klicken Sie auf **OK**, um den TN-Redirector-Zugriffseintrag zu definieren. Der Eintrag wird im TN-Redirector-Teilfenster des TN-Server-Fensters angezeigt.

**Anmerkung:** Obwohl TN Redirector keine der SNA-Ressourcen des Knotens verwendet, muss der SNA-Knoten für die Verwendung von TN Redirector aktiv sein.

## Communications Server für Linux inaktivieren

Durch Inaktivierung der Software Communications Server für Linux werden automatisch der CS-Linux-Knoten und die zugehörigen Konnektivitätskomponenten gestoppt. Nach Inaktivierung von Communications Server für Linux können alle Prozesse (z. B. eine LUA-Anwendung) auf diesem Server keine CS-Linux-Ressourcen mehr verwenden.

Sie sollten in der Regel nur einzelne Dienste stoppen, wenn diese von den Benutzern nicht mehr benötigt werden. Eine Inaktivierung des Systems ist nur anzuraten, wenn keine CS-Linux-Aktivität vorliegt.

Wenn Sie Communications Server für Linux inaktivieren müssen, warnen Sie die Benutzer, dass Sie Communications Server für Linux stoppen wollen, und geben Sie Ihnen Zeit, die gerade laufenden Aktivitäten vor Inaktivierung der Software zu beenden.

Wenn Sie die Software Communications Server für Linux inaktivieren, werden Anwendungen, die die API APPC, CSV, LUA, NOF oder MS benutzen, durch einen Rückkehrcode `COMM_SUBSYSTEM_ABENDED` und CPI-C-Anwendungen durch einen Rückkehrcode `CM_PRODUCT_SPECIFIC_ERROR` benachrichtigt.

Geben Sie zum Inaktivieren der Software Communications Server für Linux an der Linux-Eingabeaufforderung den folgenden Befehl ein:

**sna stop**

Wenn Communications Server für Linux erfolgreich inaktiviert wurde, gibt **sna stop** den Exit-Code `0` zurück. Jeder andere Exit-Code gibt an, dass ein Fehler aufgetreten ist und die Software Communications Server für Linux nicht inaktiviert wurde. Weitere Informationen zu den Werten von Exit-Codes finden Sie im *Communications Server for Linux Diagnostics Guide*.

# Communications Server für Linux automatisch starten

Das Aktivieren von Communications Server für Linux bis zur Betriebsbereitschaft kann als ein Prozess mit mehreren Schritten betrachtet werden:

- Aktivieren der Software Communications Server für Linux
- Initialisieren des SNA-Knotens
- Aktivieren der Ports und Verbindungsstationen, die auf dem Knoten konfiguriert sind.

Jeder dieser Schritte kann einzeln verwaltet werden. Gegebenenfalls können alle Schritte zur Boot-Zeit ausgeführt werden. Im verbleibenden Teil dieses Abschnitts sind diese Schritte beschrieben. Außerdem wird erläutert, wie die Schritte zur Boot-Zeit gesteuert werden können.

## Communications Server für Linux aktivieren

Für den Betrieb von Communications Server für Linux müssen mehrere Kernel-Module geladen werden. Diese Module werden geladen, wenn Sie die Software Communications Server für Linux zum ersten Mal aktivieren. Bei einer Änderung der Kernel-Ausführungsstufe werden die Module wieder entladen.

Communications Server für Linux erfordert außerdem, dass eine Reihe von Dämonen (Programmen) aktiv ist. Sie können Communications Server für Linux erst konfigurieren oder verwenden, wenn diese Dämonen aktiv sind.

- Setzen Sie den Befehl **sna start** ab, um die Dämonen zu starten und die Software Communications Server für Linux zu aktivieren.
- Setzen Sie den Befehl **sna stop** ab, um die Dämonen zu stoppen und die Software Communications Server für Linux zu inaktivieren.

## SNA-Knoten initialisieren

Wenn die Software Communications Server für Linux aktiviert wurde, können Sie den SNA-Knoten und seine Ressourcen konfigurieren. In der Regel werden Sie dazu das Motif-Verwaltungsprogramm xsnaadmin verwenden. Der Knoten kann jedoch erst verwendet werden, nachdem er initialisiert wurde. Sie können ihn im Befehlszeilenverwaltungsprogramm mit dem Befehl **snaadmin init_node** oder im Motif-Verwaltungsprogramm xsnaadmin initialisieren.

## Ports und Verbindungsstationen aktivieren

Ports und Verbindungsstationen können so konfiguriert werden, dass sie unter verschiedenen Umständen gestartet werden:

- Nur per Bedienereingriff
- Bedarfsgesteuert (wenn eine Anwendung gestartet wird, die eine Ressource der Verbindung verwendet)
- Beim Start des Knotens (wenn der Befehl **snaadmin init_node** abgesetzt oder der Knoten im Motif-Verwaltungsprogramm gestartet wird).

Der Start durch den Bediener ist die Standardeinstellung. Sie können diese Einstellung für einen bestimmten Port bzw. eine bestimmte Verbindung ändern. Verwenden Sie dazu das Befehlszeilenverwaltungsprogramm oder das Motif-Verwaltungsprogramm.

**Anmerkung:** Wenn ein Port gestartet wurde, kann er Anrufe von anderen Computern empfangen, jedoch keine abgehenden Anrufe durchführen. Das Starten einer Verbindungsstation bedeutet, dass Communications Server für Linux versucht, Kontakt zum fernen Computer aufzunehmen.

## Communications Server für Linux beim Warmstart starten

Communications Server für Linux wird wie andere Linux-Dienste beim Warmstart aktiviert. Das heißt, nach einem Warmstart wird standardmäßig der Befehl **sna start** abgesetzt, der SNA-Knoten jedoch nicht gestartet.

Diese Initialisierung wird im Boot-Initialisierungs-Script von Communications Server für Linux **/etc/rc.d/init.d/snastart** ausgeführt. Wie für Start-Scripts üblich, ist dieses Script mit **/etc/rc?.d/init.d/snastart** für die verschiedenen Boot-Ebenen verknüpft.

Sie können **/etc/rc.d/init.d/snastart** bearbeiten und die Aktionen beim Warmstart ändern. Die häufigste Änderung ist das Hinzufügen der Knoteninitialisierung. Der Befehl hierfür, **snaadmin init_node**, ist bereits in der Datei enthalten, jedoch auf Kommentar gesetzt. Sie müssen somit nur das Kommentarzeichen vor dem Befehl entfernen. Wenn Sie diesen Befehl aufnehmen, lösen Sie auch die Aktivierung von Ports und Verbindungsstationen aus, deren Aktivierung beim Start des Knotens konfiguriert ist.

Anwendungen, die Communications Server für Linux verwenden, sollten erst nach der Initialisierung des Knotens gestartet werden. Gegebenenfalls können Sie diese Anwendungen automatisch beim Booten starten und alle weiteren **snaadmin**-Befehle, die zur Boot-Zeit ausgeführt werden sollen, auf eine der beiden folgenden Arten hinzufügen:

- Fügen Sie die Befehle am Ende von **/etc/rc.d/init.d/snastart** nach dem Befehl **snaadmin init_node** hinzu.
- Erstellen Sie ein Script **/etc/rc?.d/init.d** mit einer Nummer größer als 95. Dadurch wird sichergestellt, dass das Script nach dem Start von Communications Server für Linux ausgeführt wird und die Befehle zu diesem Script hinzugefügt werden.

**Anmerkung:** Änderungen, die Sie an der Datei **/etc/rc.d/init.d/snastart** vornehmen, werden nicht gespeichert, wenn Sie für Communications Server für Linux ein Upgrade auf eine neuere Version durchführen. Vergewissern Sie sich stets, dass Sie eine Kopie der Änderungen haben, damit Sie sie nach einem Upgrade erneut anwenden können.

# Kapitel 9. Informationsquellen für Communications Server für Linux und SNA

In diesem Kapitel werden die verschiedenen Veröffentlichungen der SNA-Bibliothek erläutert, die Informationen zur SNA-Technologie sowie zu zahlreichen Netzprodukten und Services von IBM enthalten. Außerdem wird erläutert, welche Informationen über Netzforen verfügbar sind.

## SNA-Bibliothek

Die SNA-Bibliothek enthält Marketingbroschüren, Bücher, Benutzerhandbücher und Lernprogramme mit Einführungsinformationen sowie weiterführende Informationen zu folgenden Themen:

- SNA-Theorie
- SNA-Produkte
- Produktimplementierung
- System- und Netzkonfigurationen
- SNA-Anwendungsprogramme und -APIs
- Gesamtplanung, Leistung und Optimierung
- Problemanalyse
- Netzverwaltung
- Netzsicherheit

Sie können alle IBM Veröffentlichungen bei Ihrem IBM Ansprechpartner oder bei der örtlichen IBM Niederlassung anfordern.

Informationen zu zusätzlichen Veröffentlichungen erhalten Sie beim zuständigen IBM Ansprechpartner.

## Informationen im Netz

Zur Förderung des Informationsaustausches sponsert IBM elektronische Foren und Bulletin Boards. IBM unterhält Homepages im Internet und stellt Onlinedokumentationen zur Verfügung, auf die über das World Wide Web zugegriffen werden kann.

**Produktunterstützung über IBMLink**

Das Forum IBMLink wird in IBM Netzen organisiert. Es soll Kunden mit IBM Lizenzprodukten helfen, technische Probleme zu lösen, und Fragen zu Systemen und Netzen klären. IBM Mitarbeiter beantworten Fragen und vermitteln Onlinediskussionen zwischen IBM Kunden.

Weitere Informationen zu IBMLink finden Sie unter http://www.ibmlink.ibm.com.

**Informationen auf IBM Homepages**

Im Internet bieten verschiedene IBM Homepages Zugang zu Foren. Ausführliche Hilfe erhalten Sie über die Haupthomepage von IBM, von der aus Sie zu Informationszentren im Internet und im World Wide Web navigieren können. Die Adresse der Haupthomepage ist http://www.ibm.com.

Über die Adresse http://www.ibm.com/software/network können Sie auf Informationen zur IBM Software für den Netzbetrieb, einschließlich Communications Server für Linux, zugreifen. Gezielte Informationen zu Communications Server für Linux finden Sie unter http://www.ibm.com/software/network/commserver.

Weitere ausführliche Hinweise zur Unterstützung für Communications Server für Linux bietet die Seite http://www.ibm.com/software/network/commserver/support.

**Informationen zum Herunterladen**

Benutzer können Redbook-Veröffentlichungen aus dem World Wide Web (http://www.redbooks.ibm.com) herunterladen.

Informationen zu IBM Software können Sie unter http://www.ibm.com/software abrufen. Von dieser Seite aus sind Verbindungen zu Seiten für Communications Server für Linux und alle weiteren IBM Softwareserver verfügbar.

## Empfohlene Literatur

Wenn Sie Ihre Kenntnisse zur SNA vertiefen wollen, finden Sie in den folgenden Veröffentlichungen Informationen zur Theorie von SNA und zur praktischen Anwendung von Communications Server für Linux. Diese Veröffentlichungen sind sowohl für Anfänger als Einstieg in die SNA-Materie als auch für Fachleute zur umfassenden Vertiefung des Themas geeignet.

- *Systems Network Architecture: Technical Overview* (IBM Form GC30–3073)
- *IBM Communications Server für Linux Verwaltungshandbuch*

Falls Sie weitere Fragen zu spezifischen Fachgebieten haben, wenden Sie sich an den zuständigen IBM Ansprechpartner.

# Anhang. Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden. Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Dienstleistungen von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Dienstleistungen können auch andere ihnen äquivalente Produkte, Programme oder Dienstleistungen verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte der IBM verletzen. Die Verantwortung für den Betrieb von Fremdprodukten, Fremdprogrammen und Fremddienstleistungen liegt beim Kunden.

Für in dieser Veröffentlichung beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieser Veröffentlichung ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Director of Licensing
IBM Europe, Middle East & Africa
Tour Descartes
2, avenue Gambetta
92066 Paris La Defense Cedex
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Die Änderungen werden in Überarbeitungen oder in Technical News Letters (TNLs) bekanntgegeben. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter dienen lediglich als Benutzerinformationen und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängigen, erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Corporation
P.O. Box 12195
3039 Cornwallis Road
Research Triangle Park, NC 27709-2195, USA

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des im Handbuch aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt im Rahmen der Allgemeinen Geschäftsbedingungen der IBM, der Internationalen Nutzungsbedingungen der IBM für Programmpakete oder einer äquivalenten Vereinbarung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer gesteuerten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Gewährleistung, dass diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen. Diese Daten stellen deshalb keine Leistungsgarantie dar.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufes. Diese Beispiele enthalten Namen von Personen, Firmen, Marken oder Produkten. Alle diese Namen sind frei erfunden; Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

COPYRIGHTLIZENZ: Diese Veröffentlichung enthält Beispielanwendungsprogramme, die in Quellensprache geschrieben sind. Sie dürfen diese Beispielprogramme kostenlos kopieren, ändern und verteilen, wenn dies zu dem Zweck geschieht, Anwendungsprogramme zu entwickeln, verwenden, vermarkten oder zu verteilen, die mit der Anwendungsprogrammierschnittstelle konform sind, für die diese Beispielprogramme geschrieben werden. Diese Beispiele wurden nicht unter allen denkbaren Bedingungen getestet. IBM kann deshalb nicht garantieren, dass die Zuverlässigkeit, Wartungsfreundlichkeit und Funktion dieser Programme gegeben ist. Sie dürfen diese Beispielprogramme kostenlos kopieren, Ändern und verteilen, wenn dies zu dem Zweck geschieht, Anwendungsprogramme zu entwickeln, verwenden, vermarkten oder zu verteilen, die mit der Anwendungsprogrammierschnittstelle konform sind, für die diese Beispielprogramme geschrieben werden.

Kopien oder Teile der Beispielprogramme bzw. daraus abgeleiteter Code müssen folgenden Copyrightvermerk beinhalten: Teile des vorliegenden Codes wurden aus Beispielprogrammen der IBM Corp. abgeleitet. 

## Marken

Folgende Namen sind in gewissen Ländern (oder Regionen) Marken der IBM Corporation:

| | |
|---|---|
| Advanced Peer-to-Peer Networking | Power5 |
| AIX | pSeries |
| Application System/400 | S/390 |
| AS/400 | SP |
| CICS | System/370 |
| IBM | System/390 |
| MQSeries | SAA |
| MVS | Systems Application Architecture |
| MVS/ESA | VTAM |
| MVS/XA | WebSphere |
| NetView | z/OS |
| OpenPower | z9 |
| OS/2 | zSeries |

Folgende Namen sind in gewissen Ländern Marken oder eingetragene Marken anderer Unternehmen:

Java und alle von Java abgeleiteten Marken sind in gewissen Ländern Marken von Sun Microsystems, Inc.

Microsoft, Windows, Windows NT und das Windows-Logo sind in gewissen Ländern Marken der Microsoft Corporation.

Intel, das Intel-Logo, Intel Inside, das Logo Intel Inside, Intel Centrino, das Logo Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium und Pentium sind in gewissen Ländern (oder Regionen) Marken oder eingetragene Marken der Intel Corporation oder deren Tochtergesellschaften.

UNIX ist in gewissen Ländern (oder Regionen) eine eingetragene Marke von The Open Group.

Linux ist in gewissen Ländern (oder Regionen) eine Marke von Linus Torvalds.

Andere Namen von Unternehmen, Produkten und Services können Marken oder Servicemarken anderer Unternehmen sein.

# Literaturverzeichnis

Die folgenden Veröffentlichungen von IBM enthalten zusätzliche Informationen zu den in diesem Handbuch behandelten Themen. Die Veröffentlichungen sind in folgende Themenbereiche unterteilt:

- Communications Server für Linux Version 6.2.2
- Systemnetzwerkarchitektur (SNA)
- Hostkonfiguration
- z/OS Communications Server
- Transmission Control Protocol/Internet Protocol (TCP/IP)
- X.25
- Advanced Program-to-Program Communication (APPC)
- Programmierung
- andere IBM Produkte für den Netzbetrieb

Zu den Handbüchern der CS-Linux-Bibliothek sind Kurzbeschreibungen vorhanden. Zu anderen Handbüchern sind nur Titel, Bestellnummer und in einigen Fällen der im vorliegenden Handbuch verwendete Kurztitel angegeben.

## Veröffentlichungen zu Communications Server für Linux Version 6.2.2

Die Bibliothek zu Communications Server für Linux enthält die nachstehend genannten Handbücher. Softcopies dieser Dokumentationen sind auf CD-ROM verfügbar. Informationen zum Aufrufen der Softcopy-Dateien von CD-ROM finden Sie in der Veröffentlichung *Einstieg in IBM Communications Server für Linux*. Für die Installation dieser Softcopy-Handbücher benötigen Sie (in Abhängigkeit von den installierten Landessprachen) 9-15 MB Festplattenspeicherplatz.

- *Einstieg in IBM Communications Server für Linux* (IBM Form GC12-3362)

  Dieses Handbuch enthält eine allgemeine Einführung in Communications Server für Linux und Informationen zu unterstützten Netzkenndaten sowie zu Installation, Konfiguration und Betrieb.

- *IBM Communications Server für Linux Verwaltungshandbuch* (IBM Form SC12-3363)

  Dieses Handbuch gibt einen Überblick über SNA und Communications Server für Linux und enthält Informationen zu Konfiguration und Betrieb von Communications Server für Linux.

- *IBM Communications Server for Linux Administration Command Reference* (IBM Form SC31-6770-02)

  Dieses Handbuch enthält Informationen zu SNA- und CS-Linux-Befehlen.

- *IBM Communications Server for Linux CPI-C Programmer's Guide* (IBM Form SC31-6774-02)

  Dieses Handbuch enthält Informationen für erfahrene "C"- oder Java-Programmierer zum Schreiben von SNA-Transaktionsprogrammen mit der CS-Linux-API CPI Communications.

- *IBM Communications Server for Linux APPC Programmer's Guide* (IBM Form SC31-6773-02)

  Dieses Handbuch enthält die für das Schreiben von Anwendungsprogrammen mit APPC (Advanced Program-to-Program Communication) erforderlichen Informationen.

- *IBM Communications Server for Linux LUA Programmer's Guide* (IBM Form SC31-6776-02)

  Dieses Handbuch enthält die für das Schreiben von Anwendungen mit der herkömmlichen Anwendungsprogrammierschnittstelle für LU-Anwendungen LUA erforderlichen Informationen.
- *IBM Communications Server for Linux CSV Programmer's Guide* (IBM Form SC31-6775-02)

  Dieses Handbuch enthält die für das Schreiben von Anwendungsprogrammen mit der API (Anwendungsprogrammierschnittstelle) Common Service Verbs (CSV) erforderlichen Informationen.
- *IBM Communications Server for Linux MS Programmer's Guide* (IBM Form SC31-6777-02)

  Dieses Handbuch enthält die für das Schreiben von Anwendungen mit der API Management Services (MS) erforderlichen Informationen.
- *IBM Communications Server for Linux NOF Programmer's Guide* (IBM Form SC31-6778-02)

  Dieses Handbuch enthält die für das Schreiben von Anwendungen mit der API Node Operator Facility (NOF) erforderlichen Informationen.
- *IBM Communications Server for Linux Diagnostics Guide* (IBM Form SC31-6779-02)

  Dieses Handbuch enthält Informationen zur Behebung von SNA-Netzfehlern.
- *IBM Communications Server for Linux APPC Application Suite User's Guide* (IBM Form SC31-6772-02)

  Dieses Handbuch enthält Informationen zu APPC-Anwendungen, die zusammen mit Communications Server für Linux eingesetzt werden können.
- *IBM Communications Server für Linux Glossar* (IBM Form GC12-3365-01)

  Dieses Handbuch enthält eine umfangreiche Liste von Begriffen und Definitionen, die in allen Veröffentlichungen der Bibliothek zu IBM Communications Server für Linux verwendet werden.

## Veröffentlichungen zur Systemnetzwerkarchitektur (SNA)

Die folgenden Handbücher enthalten Informationen zu SNA-Netzen:

- *Systems Network Architecture: Format and Protocol Reference Manual—Architecture Logic for LU Type 6.2* (IBM Form SC30-3269)
- *Systems Network Architecture: Formats* (IBM Form GA27-3136)
- *Systems Network Architecture: Guide to SNA Publications* (IBM Form GC30-3438)
- *Systems Network Architecture: Network Product Formats* (IBM Form LY43-0081)
- *Systems Network Architecture: Technical Overview* (IBM Form GC30-3073)
- *Systems Network Architecture: APPN Architecture Reference* (IBM Form SC30-3422)
- *Systems Network Architecture: Sessions between Logical Units* (IBM Form GC20-1868)
- *Systems Network Architecture: LU 6.2 Reference—Peer Protocols* (IBM Form SC31-6808)
- *Systems Network Architecture: Transaction Programmer's Reference Manual for LU Type 6.2* (IBM Form GC30-3084)
- *Systems Network Architecture: 3270 Datastream Programmer's Reference* (IBM Form GA23-0059)
- *Networking Blueprint Executive Overview* (IBM Form GC31-7057)
- *Systems Network Architecture: Management Services Reference* (IBM Form SC30-3346)

## Veröffentlichungen zur Hostkonfiguration

Die folgenden Handbücher enthalten Informationen zur Hostkonfiguration:

- *ES/9000, ES/3090 IOCP User's Guide Volume A04* (IBM Form GC38-0097)
- *3174 Establishment Controller Installation Guide* (IBM Form GG24-3061)
- *3270 Information Display System 3174 Establishment Controller: Planning Guide* (IBM Form GA27-3918)
- *OS/390 Hardware Configuration Definition (HCD) User's Guide* (IBM Form SC28-1848)

## Veröffentlichungen zu z/OS Communications Server

Die folgenden Handbücher enthalten Informationen zu z/OS Communications Server:

- *z/OS V1R7 Communications Server: SNA Network Implementation Guide* (IBM Form SC31-8777)
- *z/OS V1R7 Communications Server: SNA Diagnostics* (Band 1: IBM Form GC31-6850, Band 2: IBM Form GC31-6851)
- *z/OS V1R6 Communications Server: Resource Definition Reference* (IBM Form SC31-8778)

## Veröffentlichungen zu TCP/IP

Die folgenden Handbücher enthalten Informationen zum Netzprotokoll TCP/IP (Transmission Control Protocol/Internet Protocol):

- *z/OS V1R7 Communications Server: IP Configuration Guide* (IBM Form SC31-8775)
- *z/OS V1R7 Communications Server: IP Configuration Reference* (IBM Form SC31-8776)
- *z/VM V5R1 TCP/IP Planning and Customization* (IBM Form SC24-6125)

## Veröffentlichungen zu X.25

Die folgenden Handbücher enthalten Informationen zum Netzprotokoll X.25:

- *Communications Server for OS/2 Version 4 X.25 Programming* (IBM Form SC31-8150)

## Veröffentlichungen zu APPC

Die folgenden Handbücher enthalten Informationen zu APPC (Advanced Program-to-Program Communication):

- *APPC Application Suite V1 User's Guide* (IBM Form SC31-6532)
- *APPC Application Suite V1 Administration* (IBM Form SC31-6533)
- *APPC Application Suite V1 Programming* (IBM Form SC31-6534)
- *APPC Application Suite V1 Online Product Library* (IBM Form SK2T-2680)
- *APPC Application Suite Licensed Program Specifications* (IBM Form GC31-6535)
- *z/OS V1R2.0 Communications Server: APPC Application Suite User's Guide* (IBM Form SC31-8809)

## Veröffentlichungen zur Programmierung

Die folgenden Handbücher enthalten Informationen zur Programmierung:

- *Common Programming Interface Communications CPI-C Reference* (IBM Form SC26-4399)
- *Communications Server for OS/2 Version 4 Application Programming Guide* (IBM Form SC31-8152)

## Veröffentlichungen zu anderen IBM Produkten für den Netzbetrieb

Die folgenden Handbücher enthalten Informationen zu anderen Themen mit Bezug zu Communications Server für Linux:

- *SDLC Concepts* (IBM Form GA27-3093)
- *Local Area Network Concepts and Products: LAN Architecture* (IBM Form SG24-4753)
- *Local Area Network Concepts and Products: LAN Adapters, Hubs and ATM* (IBM Form SG24-4754)
- *Local Area Network Concepts and Products: Routers and Gateways* (IBM Form SG24-4755)
- *Local Area Network Concepts and Products: LAN Operating Systems and Management* (IBM Form SG24-4756)
- *IBM Network Control Program Resource Definition Guide* (IBM Form SC30-3349)

# Index

## Numerische Stichwörter



## A



## B



## C



## D

# E



# F



# G



# H



# I



# J



# K

# L



# M



# N



# O



# P

# Q



# R



# S



# T

# U



# V



# W



# X



# Z

# Antwort

**IBM Communications Server für Linux**
**Einstieg**
**Version 6.2.2**

**IBM Form GC12-3362-01**

Anregungen zur Verbesserung und Ergänzung dieser Veröffentlichung nehmen wir gerne entgegen. Bitte informieren Sie uns über Fehler, ungenaue Darstellungen oder andere Mängel.

Zur Klärung technischer Fragen sowie zu Liefermöglichkeiten und Preisen wenden Sie sich bitte entweder an Ihre IBM Geschäftsstelle, Ihren IBM Geschäftspartner oder Ihren Händler.

**Unsere Telefonauskunft ″HALLO IBM″ (Telefonnr.: 0180 3 313233) steht Ihnen ebenfalls zur Klärung allgemeiner Fragen zur Verfügung.**

Kommentare:

Danke für Ihre Bemühungen.

Sie können ihre Kommentare betr. dieser Veröffentlichung wie folgt senden:
- Als Brief an die Postanschrift auf der Rückseite dieses Formulars
- Als E-Mail an die folgende Adresse: ibmterm@de.ibm.com

| | |
|---|---|
| Name | Adresse |
| Firma oder Organisation | |
| Rufnummer | E-Mail-Adresse |

**Antwort**
GC12-3362-01

IBM

IBM Deutschland GmbH
SW TSC Germany

70548 Stuttgart

GC12-3362-01

Programmnummer: 5724-i33

GC12-3362-01