

IBM Communications Server for Data Center  
Deployment für AIX  
7.1

*Einstieg*



**Note**

Before using this information and the product it supports, be sure to read the general information under [Appendix B, “Notices,” on page 103](#).

**Siebente Ausgabe (Januar 2021)**

Diese Ausgabe bezieht sich auf IBM Communications Server for Data Center Deployment für AIX 7.1, Programmnummer 5725-H32, und, sofern in neuen Ausgaben oder TNs nichts anderes angegeben ist, auf alle folgenden Releases und Änderungen.

Veröffentlichungen können über den zuständigen IBM Ansprechpartner oder die zuständige IBM Geschäftsstelle bezogen werden. Veröffentlichungen sind nicht bei der unten angegebenen Adresse erhältlich.

IBM nimmt Ihre Kommentare gerne entgegen. Am Ende dieser Veröffentlichung befindet sich ebenfalls ein Vordruck für ein Antwortschreiben. Fehlt der Vordruck, können Sie das Antwortschreiben an folgende Adresse richten:

- International Business Machines Corporation
- Department CGMD
- P.O. Box 12195
- Research Triangle Park, North Carolina
- 27709-2195
- USA

Elektronisch können Sie Ihre Kommentare an folgende Adresse schicken:

- IBMLink: CIBMORCF at RALVM17
- IBM Mail: USIB2HPD at IBMMAIL
- Internet: USIB2HPD@vnet.ibm.com
- Fax: 1-800-227-5088

Werden an IBM Informationen eingesandt, gewährt der Einsender IBM ein nicht ausschließliches Recht zur beliebigen Verwendung oder Verteilung dieser Informationen, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

---

# Inhaltsverzeichnis

**Tabellen.....**..... **vii**

**Abbildungsverzeichnis.....**..... **ix**

**Willkommen bei IBM Communications Server for Data Center Deployment für AIX.....**..... **xi**

Benutzung des Handbuchs.....	xi
Orientierungshilfe.....	xi
Typografische Konventionen.....	xii
Verwendete Abkürzungen.....	xii
Neuerungen.....	xiv
Neue Funktionen.....	xiv
Gesperrte Funktionen.....	xv
Informationsquellen.....	xv

**Kapitel 1. Informationen zu IBM Communications Server for Data Center Deployment für AIX.....**..... **1**

IBM Communications Server for Data Center Deployment für AIX - Features und Programmpakete.....	1
IBM Communications Server for Data Center Deployment für AIX.....	1
Erweiterte Netzfeatures.....	5
Features und Vorteile.....	10
Vielseitige Bausteine.....	10
Client-Server-Betrieb.....	11
Problemlose Konfiguration.....	11
Zusätzliche Schnittstellenoptionen für Verwaltung.....	12
Verbesserte Leistung.....	12
Sicherheitsoptionen.....	12
Flexible Netzverwaltung.....	13
Zuverlässigkeit, Verfügbarkeit und Wartungsfreundlichkeit.....	13
Netzintegration, Wachstum und Veränderungen.....	14

**Kapitel 2. Netz mit IBM Communications Server for Data Center Deployment für AIX planen.....**..... **15**

Schritte bei der Netzplanung.....	15
Funktionsanforderungen für das Netz.....	15
Konfiguration von CS/AIX planen.....	16
Ressourcenanforderungen für Installation und Betrieb.....	16
IPV4- und IPV6-Adressen.....	21
Kompatibilität plattformübergreifender Konfigurationen gewährleisten.....	22
Namenskonventionen.....	22

**Kapitel 3. CS/AIX auf AIX-Servern installieren.....**..... **25**

Lizenzierung und Konfektionierung von CS/AIX.....	25
Mechanismen der Lizenzierung für CS/AIX.....	25
Angebote CS/AIX-Lizenzprogrammpakete.....	26
Installation von CS/AIX vorbereiten.....	28
Dateigruppen für Datenübertragungssteuerung installieren.....	28
Details der Produktinstallation anzeigen.....	28

Sprachumgebungsvariable ändern.....	29
Vorversionen von CS/AIX migrieren.....	29
Hinweise.....	29
Lizenzprogramm CS/AIX installieren.....	30
Installationsmethoden.....	30
WebSphere Application Server konfigurieren.....	33
Sicherheitszertifikat für WebSphere Application Server konfigurieren.....	33
WebSphere Application Server konfigurieren.....	33
Serverkonfigurationsdatei installieren.....	34
Prozeduren für den Installationsabschluss.....	34
Client-Server-Betrieb.....	35
PDF-Handbücher anzeigen.....	35
Aktuelle Releaseinformationen.....	35
SSL für die Verwendung mit TN Server oder TN Redirector konfigurieren.....	35
Webserver für das Webverwaltungsprogramm konfigurieren.....	36
CS/AIX-Konfigurationsdateien sichern.....	36
Sicherungskopie der CS/AIX-Konfigurationsdateien zurückschreiben.....	37
Konfigurationsdateien reinitialisieren.....	37
<b>Kapitel 4. IBM Remote API Clients unter Linux installieren.....</b>	<b>39</b>
Hardware- und Softwarevoraussetzungen.....	39
Hardwarevoraussetzungen.....	39
Version des Betriebssystems Linux.....	39
Java.....	40
GSKit.....	40
Details der Produktinstallation anzeigen.....	40
UmgebungsvARIABLEN für CS/AIX definieren.....	40
Sprachumgebungsvariable setzen.....	40
Remote API Client für Linux installieren.....	41
HTTPS-Sicherheitszertifikate mit dem GSKit konfigurieren.....	42
Remote API Client für Linux deinstallieren.....	43
<b>Kapitel 5. IBM Remote API Clients für Linux auf System z installieren.....</b>	<b>45</b>
Hardware- und Softwarevoraussetzungen.....	45
Hardwarevoraussetzungen.....	45
Version des Betriebssystems Linux.....	45
Java.....	45
GSKit.....	45
Details der Produktinstallation anzeigen.....	45
UmgebungsvARIABLEN für CS/AIX definieren.....	46
Sprachumgebungsvariable setzen.....	46
Remote API Client für Linux auf System z installieren.....	46
HTTPS-Sicherheitszertifikate mit dem GSKit konfigurieren.....	48
Remote API Client für Linux auf System z deinstallieren.....	49
<b>Kapitel 6. IBM Remote API Clients unter AIX installieren.....</b>	<b>51</b>
Hardware- und Softwarevoraussetzungen.....	51
Hardwarevoraussetzungen.....	51
Betriebssystemversion.....	51
Java.....	51
GSKit.....	51
UmgebungsvARIABLEN für CS/AIX definieren.....	51
Sprachumgebungsvariable ändern.....	52
Remote API Client für AIX installieren.....	52
Dateien für die Installation von Remote API Client auf die AIX-Workstation kopieren.....	52
Remote API Client von der CD installieren.....	53
HTTPS-Sicherheitszertifikate mit dem GSKit konfigurieren.....	53

Remote API Client für AIX deinstallieren.....	54
<b>Kapitel 7. Installation von Remote API Client für Windows planen und ausführen.....</b>	<b>55</b>
Hardware- und Softwarevoraussetzungen.....	55
Zugriff auf das Setup-Programm.....	55
Remote API Client mit dem Setup-Programm unter Windows installieren.....	56
Erweiterte Optionen für die Konfiguration von Remote API Client.....	59
Remote API Client über die Befehlszeile installieren.....	59
HTTPS-Sicherheitszertifikate mit dem GSKit konfigurieren.....	62
Remote API Client nach der Installation anpassen.....	63
Software Remote API Client erneut installieren.....	63
Remote API Client deinstallieren.....	64
Remote API Client über die Befehlszeile deinstallieren.....	64
Hilfe.....	65
<b>Kapitel 8. CS/AIX konfigurieren und verwenden.....</b>	<b>67</b>
CS/AIX-Konfiguration planen.....	68
Planungsblätter.....	68
Aufgabenblätter.....	68
Umgebungsvariablen für CS/AIX definieren.....	69
Motif-Verwaltungsprogramm verwenden.....	69
Pfad zu CS/AIX-Programmen angeben.....	69
CS/AIX aktivieren.....	69
CS/AIX mit dem Motif-Verwaltungsprogramm verwalten.....	70
Client-Server-Funktionen konfigurieren.....	74
Knoten konfigurieren.....	74
Konnektivität konfigurieren.....	76
SDLC-Verbindung für abhängigen Datenverkehr konfigurieren.....	77
Ethernet-Verbindung für die Unterstützung von abhängigem und unabhängigem Datenverkehr konfigurieren.....	78
Enterprise-Extender-Verbindung konfigurieren.....	79
LUs der Typen 0-3 konfigurieren.....	79
LUs der Typen 0-3 definieren.....	80
LU-Pool definieren.....	80
APPC-Kommunikation konfigurieren.....	81
Einfaches APPN-Netz konfigurieren.....	82
Abhängiges APPC konfigurieren.....	86
Konfiguration für CPI Communications.....	86
LUA konfigurieren.....	87
SNA Gateway konfigurieren.....	87
Implizite untergeordnete LUs unterstützen.....	89
Untergeordnete LUs definieren.....	89
DLUR konfigurieren.....	90
DLUR-Unterstützung auf dem lokalen Knoten konfigurieren.....	91
Durchgriff-DLUR-Unterstützung für untergeordnete Knoten konfigurieren.....	92
TN Server konfigurieren.....	92
3270-LUs definieren.....	94
LU-Pool definieren.....	95
TN3270 Server konfigurieren.....	96
TN Redirector konfigurieren.....	97
TN Redirector konfigurieren.....	97
CS/AIX inaktivieren.....	98
<b>Kapitel 9. Informationsquellen für CS/AIX und SNA.....</b>	<b>99</b>
SNA-Bibliothek.....	99
Über das Netz zugängliche Informationen.....	99

Empfohlene Literatur.....	100
<b>Anhang A. How to send your comments to IBM.....</b>	<b>101</b>
Email feedback template.....	101
If you have a technical problem.....	101
<b>Anhang B. Notices.....</b>	<b>103</b>
Trademarks.....	104
<b>Literaturverzeichnis.....</b>	<b>107</b>
CS/AIX-Veröffentlichungen.....	107
IBM Redbooks.....	108
Veröffentlichungen zum Betriebssystem AIX.....	108
Veröffentlichungen zur Systemnetzwerkarchitektur (SNA).....	109
Veröffentlichungen zur Hostkonfiguration.....	109
Veröffentlichungen zu z/OS Communications Server.....	109
Veröffentlichungen zu TCP/IP.....	109
Veröffentlichungen zu X.25.....	109
Veröffentlichungen zu APPC.....	110
Veröffentlichungen zur Programmierung.....	110
Veröffentlichungen zu anderen IBM Produkten für den Netzbetrieb.....	110
<b>Index.....</b>	<b>111</b>

---

# Tabellen

1. Orientierungshilfe für den Einstieg.....	xi
2. Typografische Konventionen.....	xii



---

# Abbildungsverzeichnis

1. Verbindung mehrerer untergeordneter AIX-Computer mit einem Host über SNA Gateway.....	6
2. Branch Extender.....	7
3. TN Server.....	9
4. Knotenfenster.....	71
5. CS/AIX-Symbolleiste.....	73
6. CS/AIX-Knoten, der direkt mit einem Host kommuniziert.....	75
7. CS/AIX-Knoten in einem APPN-Netz.....	75
8. SNA Gateway.....	88
9. CS/AIX-Knoten, der DLUR bereitstellt.....	91
10. Für TN Server konfigurierter CS/AIX-Knoten.....	93
11. TN Server.....	94



# Willkommen bei IBM Communications Server for Data Center Deployment für AIX

---

Das vorliegende Handbuch gibt eine Einführung in IBM Communications Server for Data Center Deployment für AIX(CS/AIX), Lizenzprogrammnummer 5725-H32, mit dessen Hilfe ein Server mit dem Betriebssystem Advanced Interactive Executive (AIX) von IBM Daten mit anderen Knoten in einem SNA-Netz (Systemnetzwerkarchitektur) austauschen kann. CS/AIX ist das umfassendste derzeit verfügbare Produkt für den SNA-Netzbetrieb von Workstations mit dem Betriebssystem AIX.

IBM Communications Server for Data Center Deployment für AIX ist für die Ausführung auf einer AIX-Workstation konzipiert, die mit einem oder mehreren Netz(en) verbunden ist. CS/AIX Version 7.1 kann auf jedem IBM Power System ausgeführt werden, das von AIX ab Version 7.2 unterstützt wird. Im vorliegenden Handbuch wird für diese Systeme, auf denen das Betriebssystem AIX installiert ist, der Begriff AIX-Workstation verwendet.

CS/AIX 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 AIX interessieren.

Tabelle 1 auf Seite xi können Sie entnehmen, wo Sie die gewünschten Informationen zu CS/AIX finden.

*Tabelle 1. Orientierungshilfe für den Einstieg*

Sie möchten ...	Lesen Sie ...
sich über CS/AIX informieren	<a href="#">Kapitel 1, „Informationen zu IBM Communications Server for Data Center Deployment für AIX“, auf Seite 1</a>
die Verwendung von CS/AIX in Ihrem Netz planen	<a href="#">Kapitel 2, „Netz mit IBM Communications Server for Data Center Deployment für AIX planen“, auf Seite 15</a>
CS/AIX auf AIX-Servern installieren	<a href="#">Kapitel 3, „CS/AIX auf AIX-Servern installieren“, auf Seite 25</a>
Remote API Clients für Linux (Intel (32 Bit), Intel/AMD (64 Bit) oder pSeries) installieren	<a href="#">Kapitel 4, „IBM Remote API Clients unter Linux installieren“, auf Seite 39</a>
Remote API Clients unter Linux für System z installieren	<a href="#">Kapitel 5, „IBM Remote API Clients für Linux auf System z installieren“, auf Seite 45</a>
Remote API Clients unter AIX installieren	<a href="#">Kapitel 6, „IBM Remote API Clients unter AIX installieren“, auf Seite 51</a>

*Tabelle 1. Orientierungshilfe für den Einstieg (Forts.)*

<b>Sie möchten ...</b>	<b>Lesen Sie ...</b>
Remote API Clients unter Windows installieren	<a href="#">Kapitel 7, „Installation von Remote API Client für Windows planen und ausführen“, auf Seite 55</a>
CS/AIX konfigurieren	<a href="#">Kapitel 8, „CS/AIX konfigurieren und verwenden“, auf Seite 67</a>
Hinweise zur CS/AIX-Dokumentation und zu anderen Publikationen, einschließlich Onlineinformationen, erhalten	<a href="#">Kapitel 9, „Informationsquellen für CS/AIX und SNA“, auf Seite 99</a>
die Bemerkungen und Informationen zu Marken lesen	<a href="#">Anhang B, „Notices“, auf Seite 103</a>

## Typografische Konventionen

[Tabelle 2 auf Seite xii](#) gibt einen Überblick über die in diesem Handbuch verwendeten typografischen Darstellungen.

*Tabelle 2. Typografische Konventionen*

<b>Element</b>	<b>Typografiebeispiel</b>
Hervorgehobene Wörter	<b>Sichern Sie Dateien vor dem Löschen</b>
Handbuchtitel	<i>Verwaltungshandbuch für IBM Communications Server for Data Center Deployment für AIX</i>
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:

AIW	APPN Implementers Workshop
AIX	Advanced Interactive Executive
ANR	Automatic Network Routing
API	Application Programming Interface (Anwendungsprogrammierschnittstelle)
APPC	Advanced Program-to-Program Communication
APPN	Advanced Peer-to-Peer Networking
ATM	Asynchronous Transfer Mode (asynchroner Übertragungsmodus)
BOS	Base Operating System (Basisbetriebssystem)
ZNK	Zweignetzknoten
CICS	Customer Information Control System
COS	Class of Service (Serviceklasse)
CPI-C	Common Programming Interface for Communications
CSV	Common Service Verb
DB2	DATABASE 2

---

DDLU	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
FDDI	Fiber Distributed Data Interface
FTP	File Transfer Protocol
HPR	High-Performance Routing
IEEE	Institute of Electrical and Electronics Engineers
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
MPQP	Multiprotocol Quad Port
MS	Management Services (Verwaltungsdienste)
NMVT	Network Management Vector Transport
NOF	Node Operator Facility
OS/2	Operating System/2
OSI	Open Systems Interconnection
PU	Physical Unit (physische Einheit)
RFC	Request For Comments
RISC	Reduced Instruction Set Computer
RLE	Run-Length Encoding (Verschlüsselung für Ausführungshäufigkeit)
RTP	Rapid Transport Protocol
SAA	Systems Application Architecture
SAP	Service Access Point
SDLC	Synchronous Data Link Control (Steuerung für synchrone Datenübertragung)
SLP	Service Location Protocol
SMIT	Systems Management Interface Tool
SMP	Symmetric Multiprocessing (symmetrischer Mehrprozessorbetrieb)
SNA	Systems Network Architecture (Systemnetzwerkarchitektur)

---

---

SNMP-MIB	Simple Network Management Protocol - Management Information Base
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TN	Telnet
TP	Transaction Program (Transaktionsprogramm)
VT	Virtual Terminal (Virtuelles Terminal)
VTAM	Virtual Telecommunications Access Method
WAN	Wide Area Network (Weitverkehrsnetz)

---

## Neuerungen

CS/AIX Version 7.1 ist ein Nachfolger des Produkts CS/AIX Version 7.0, das weiterhin unterstützt wird.

### Neue Funktionen

Die folgenden Funktionen sind in diesem Release von CS/AIX neu hinzugekommen:

- Anzeige der Anzahl der Anwendungen, die im Windows-Client verwendet werden.

Das Überwachungsprogramm für Windows-Clients `sxclappl1.exe` wurde erweitert und zeigt jetzt die Anzahl der Anwendungen (APC, LUA, PCOMM usw.) an, die von diesem Windows-Client verwendet werden.

- Erweiterungen für die Zuordnung von fest codierten LU-Aliassen in Clientanwendungen zu LU-Aliassen in einer Serverdomäne.

Einige Anwendungen sind für die Verwendung bestimmter LU-Aliasse fest codiert. Wenn Sie so eine Anwendung auf zwei oder mehr Remote API Clients ausführen, ordnet diese Funktion diesen LU-Aliassen bestimmte LUs auf dem Server zu (jeweils eine andere LU pro Anwendungskopie). Damit können Anwendungen, die aus reinen SNA-Stack-Implementierungen migriert werden, für bestimmte LU-Aliasse auf dem Server konfiguriert werden, und teilweise von den Funktionen der Implementierung in der Serverdomäne profitieren, indem alle Serverressourcen in dieser Domäne verwendet werden. In diesem Release sind weitere Konfigurationsmöglichkeiten für diese Funktion hinzugekommen.

- Hinzugefügter Aufrufzeitgeber für Domänenserver.

Diese Funktion ermöglicht einen schnelleren Ausweichbetrieb und eine schnellere Wiederherstellung bei einer Client-Server-Konfiguration mit mehreren Servern.

- Möglichkeit der Definition von Bereichen für LUs der Typen Typ 0-3 mit zwei Dezimalziffern im Namen.

Diese Funktion erhöht die Flexibilität bei der Benennung von LU-Pools.

- Unterstützung für den TN3270 Intrusion Detection Service.

Diese Funktion ermöglicht die Zusammenarbeit mit der Erweiterung für VTAM bei der Erkennung bestimmter Verstöße im 3270-Datenstrom.

- Unterstützung für Docker-Container.

Diese Funktion ermöglicht die Ausführung des Remote API Client für Linux oder AIX in Docker-Containern.

- Unterstützung für die neuesten Verschlüsselungswerte.

Der TN3270 Server und der TN Redirector des Produkts unterstützen die Verschlüsselungsstandards TLS 1.0, 1.1, 1.2 und 1.3 sowie die zugehörigen Algorithmen und Cipher Suites. Informationen zur aktuellen Verschlüsselungsunterstützung finden Sie in der README-Datei.

- Möglichkeit der Verwendung von Hexadezimaladressen für IPv6-Verbindungen von Verbindungsnetzen.

Wenn Sie ein Verbindungsnetz in einem IPv6-Netz für HPR/IP definieren, kann ein zusätzlicher Parameter angegeben werden, um anzugeben, ob für die IP-Adressierung des Verbindungsnetzes nur IPv6-

DNS-Namen oder nur IPv6-Adressen verwendet werden. Standardmäßig werden nur IPv6-DNS-Namen verwendet.

## Gesperrte Funktionen

In diesem Release wurden keine Funktionen gesperrt.

## Informationsquellen

---

Das Literaturverzeichnis enthält weitere Bücher der CS/AIX-Bibliothek sowie Bücher mit zusätzlichen Informationen zu SNA, zum Betriebssystem AIX und zu weiteren zugehörigen Produkten.



# Kapitel 1. Informationen zu IBM Communications Server for Data Center Deployment für AIX

Dieses Kapitel enthält Informationen zu den CS/AIX-Programmpaketen. Darüber hinaus werden die Funktionen, Features und Vorteile von CS/AIX beschrieben.

## IBM Communications Server for Data Center Deployment für AIX - Features und Programmpakete

CS/AIX Version 7.1 ist eine DFV-Software, die unter dem Betriebssystem AIX ausgeführt wird. Zum Lieferumfang der Software gehören die in den Abschnitten „IBM Communications Server for Data Center Deployment für AIX“ auf Seite 1 und „Erweiterte Netzfeatures“ auf Seite 5 beschriebenen Features.

### IBM Communications Server for Data Center Deployment für AIX

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

CS/AIX stellt die folgenden Dienste bereit:

#### Netzunterstützung

CS/AIX 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 Host(s) übernommen werden. Alle anderen Knoten im Netz sind von der Steuerung durch einen Host abhängig.

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

##### Peer-zu-Peer-Netze

In verteilten Verarbeitungsumgebungen unterstützt CS/AIX Version 7.1 APPN-Netze. In diesen Peer-zu-Peer-Netzen nehmen AIX-Computer ihre Verarbeitungsfunktion wahr und kommunizieren direkt als Peers miteinander. Peer-zu-Peer-Netze nutzen in vollem Umfang die Fähigkeiten des AIX-Computers, der in zunehmendem Maße kostspielige Hosts ersetzt.

Ein APPN-Netz besteht aus Peerknoten der folgenden Arten:

- APPN-Netzknoten (zuständig für Übertragungssteuerung, dynamische Routenberechnung und Auswahldienste sowie Netzverwaltungsdienste)
- APPN-Endknoten (verwendet APPN-Netzknotendienste für die Kommunikation mit Peerknoten)
- LEN-Knoten (kommuniziert direkt mit Nachbarknoten oder als Scheinnachbarknoten konfigurierten Knoten)

**Anmerkung:** Hosts können als Peerknoten in einem APPN-Netz fungieren, wenn für die Kommunikation mit AIX-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 CS/AIX zahlreiche 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 17](#).) 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. (ATM-Unterstützung kann über eine emulierte LAN-Schnittstelle in einem Token-Ring- oder Ethernet-Netz bereitgestellt werden.)

### Weitverkehrsnetze

Für WAN-Konnektivität stehen die folgenden synchronen Verbindungen für die Kommunikation über etablierte Telefonleitungen zur Auswahl:

- EIA-232D
- Smart Modem
- X.21
- EIA-422A
- V.25bis
- V.35

CS/AIX unterstützt auch die X.25-Datenübertragungssteuerung mit Paketvermittlung. (Diese Verbindungstypen erfordern zusätzliche Produkte, die gesondert erworben werden müssen.)

## IP-Integration

Falls Ihr zentrales Unternehmensnetz auf IP basiert, können Sie das Netz mit dem Feature Enterprise Extender (HPR/IP) von CS/AIX in die SNA integrieren, so dass Ihre SNA-Anwendungen über das IP-Netz kommunizieren können. Die Client-/Serverunterstützung bietet auch SNA-über-TCP/IP-Konnektivität, die die rechenzentrenübergreifende Cloudverfügbarkeit, mobile Verfügbarkeit und Hochverfügbarkeit unterstützt.

## 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.

CS/AIX unterstützt verschiedene LU-Typen für verschiedene Anwendungsklassen.

- In einem Unterbereichsnetz unterstützt CS/AIX 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 AIX-Computer ein IBM Terminal der Produktfamilie 3270 emulieren kann. Über die anderen LU-Typen können Anwendungen an der verteilten Verarbeitung teilnehmen oder mit verschiedenen Druckern oder interaktiven Workstations kommunizieren.

CS/AIX 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/AIX-Knoten müssen dennoch definiert werden.) Auf diese Weise wird der Aufwand für die Erstkonfiguration auf dem Host verringert und eine spätere Erweiterung vereinfacht.

CS/AIX 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/AIX-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 CS/AIX 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 CS/AIX gestattet darüber hinaus den Transport des Datenverkehrs von abhängigen LUs über ein APPN-Netz.

- Mit der Primary-RUI-Unterstützung kann eine CS/AIX-Anwendung untergeordnete abhängige LU-Einheiten, die über ein LAN/WAN angeschlossen sind, wie 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. CS/AIX kann Tausende von Sitzungen unterstützen. CS/AIX bietet auch Unterstützung für U-förmige Sitzungen (die als "Transparenz zwischen lokalem und fernem Sitzungspartner" bezeichnet wird), bei denen sich die primären und sekundären LUs auf demselben AIX-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 CS/AIX 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 CS/AIX 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**

CS/AIX bietet Anwendungsprogrammierschnittstellen (APIs) für die Entwicklung von Anwendungen für bestimmte LU-Typen, für verteilte Verarbeitung, für Netzverwaltung und für die Verwaltung von CS/AIX selbst. In diesem Release stellt CS/AIX eine 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 Unterprogramme 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 abhängiger 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 CS/AIX auch eine CPI-C-Anwendungsprogrammierschnittstelle für Java-Anwendungen bereit. Weitere Informationen hierzu finden Sie im *IBM Communications Server for Data Center Deployment on AIX or Linux CPI-C Programmer's Guide*. Sofern nichts anderes angegeben ist, beziehen sich alle Hinweise auf CPI-C in den CS/AIX-Handbüchern auch auf CPI-C für Java.

Weitere für CS/AIX 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 CS/AIX 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/AIX-Ressourcen

Anwendungen, die die CS/AIX-APIs verwenden, können so kompiliert und verknüpft werden, dass sie entweder im 32-Bit-Modus oder im 64-Bit-Modus ausgeführt werden können.

Weitere Informationen zu APIs finden Sie im Programmierungshandbuch zur jeweiligen API (siehe Literaturverzeichnis).

### **Client-Server-Unterstützung**

Computer, auf denen CS/AIX 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 CS/AIX 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/AIX-Domäne bereit. Server müssen AIX-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. Clients können in Linux- oder AIX-Containern oder auf AIX-WPARs ausgeführt werden. (Ein AIX-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/AIX-Domäne. Alternativ können sie mit HTTPS über einen WebSphere-Server kommunizieren, der die Clientverbindungen mit Sicherheitszertifikaten authentifiziert. Normalerweise wird HTTPS verwendet, wenn die Clients ihre Verbindung über ein öffentliches Netz herstellen.

In einer Domäne mit mehreren CS/AIX-Servern befindet sich auf einem Server die Controllerkopie der Konfigurationsdatei für die CS/AIX-Domäne. Dieser Server ist der Controller-Server. Die anderen Ser-

ver in der Domäne können als Ausweichserver definiert werden oder Peerserver bleiben. Die Domänenkonfigurationsdatei wird auf die Ausweichserver kopiert, wenn diese gestartet werden oder wenn sich die Controllerkopie ändert, so dass sich auf allen Ausweichservern eine Kopie mit den aktuellen Informationen befindet. Ein Peer-Server erhält bei Bedarf Domänenkonfigurationsdaten vom Controller-Server, kann jedoch nicht als Ausweichserver agieren.

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

### **Unterstützung für verteilte Anwendungen**

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

CS/AIX unterstützt folgende Arten verteilter Anwendungen:

- APPC -Anwendungen (APPC wird auch als LU 6.2 bezeichnet)
- zwei bekannte Anwendungen für verteilte Verarbeitung:
  - Customer Information Control System (CICS)
  - DATABASE 2 ( DB/2), entwickelt für LU 6.2 (abhängig und unabhängig)

CICS und (das Verwaltungssystem für relationale Datenbanken) DB2 sind SAA-konforme Anwendungen, die schnell an die verschiedensten Umgebungen angepasst werden können. Die Anwendungen CICS und DB2 werden zusammen von 90 % der 500 größten US-Konzerne eingesetzt. Sie sind leistungsstarke Transaktionsprogramme, die Tausende von Knoten parallel bedienen können. In der Regel werden CICS und DB2 verwendet, um von verschiedenen Standorten aus auf Daten zu greifen und diese Daten aktualisieren und in einem zentralen Repository speichern zu können.

## **Erweiterte Netzfeatures**

Zum Basisprodukt CS/AIX Version 7.1 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 ermöglicht TCP/IP-Hostdurchgriff auf TN3270-, TN3270E-, TN5250- und VT-Clients, die unter der Bezeichnung Telnet-Clients zusammengefasst werden.
- Der Remote-API-Client-Server ermöglicht einen redundanten Zugriff mit hoher Verfügbarkeit mittels Cloud-ähnlicher Unterstützung für verteilte Windows-, AIX- und Linux-Clients. Clients können in Linux- oder AIX-Containern oder auf AIX-WPARs ausgeführt werden.

**Anmerkung:** Neuerungen bei hoch verfügbaren Netzadapters und Betriebssystemen konzentrieren sich auf IP-Netz-Funktionen. CS/AIX bietet SNA-über-IP-Konnektivität zu Servern mit Enterprise Extender,

TN3270 Server, TN Redirector und Remote API Client. Wenn Sie Ihr SNA-Netz modernisieren möchten, wird empfohlen, diese Features zu verwenden, um diese Neuerungen optimal nutzen zu können. Traditionelle Netzwerkkonnektivität mit SNA über LAN- oder WAN-Verbindungen kann nur von einigen der Neuerungen profitieren.

## 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/AIX-Computer als Gateway fungieren, das mehrere untergeordnete Computer in einem SNA-Netz mit einer oder mehreren Host-PUs verbindet. Sehen Sie sich dazu Abbildung 1 auf Seite 6 an. 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.

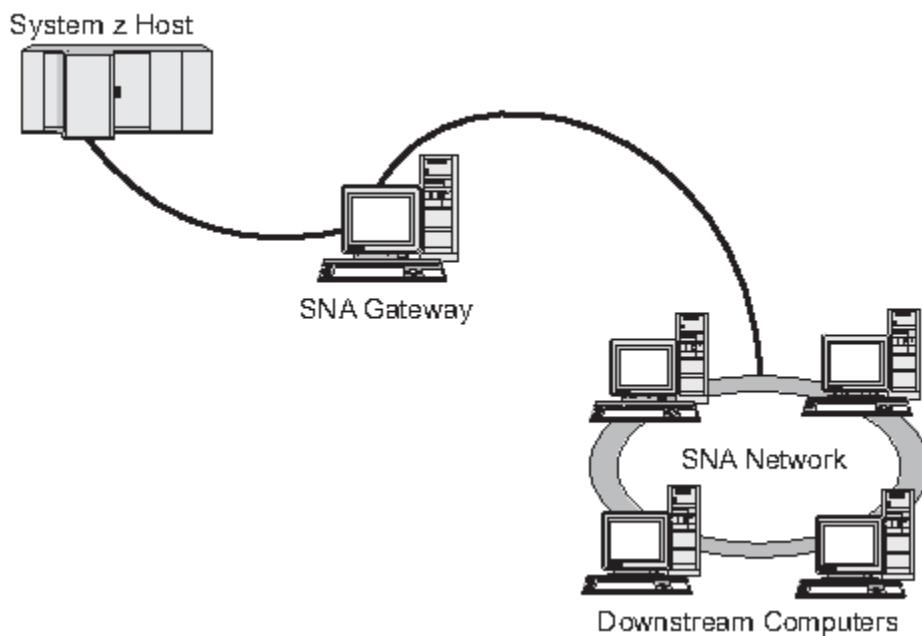


Abbildung 1. Verbindung mehrerer untergeordneter AIX-Computer mit einem Host über SNA Gateway

## Unterstützung für primäre LU

Durch die Unterstützung für primäre LU kann eine AIX-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. CS/AIX 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 primären-LU-Anwendungen muss der Knoten mit untergeordneten LUs (oder einer Schablone für untergeordnete PUs) 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 an LAN- und WAN-Ports verwendet werden. Im *IBM Communications Server for Data Center Deployment on AIX or 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 [Abbildung 2 auf Seite 7](#) dargestellte APPN-Feature Branch Extender bietet eine Lösung für diese Probleme an.

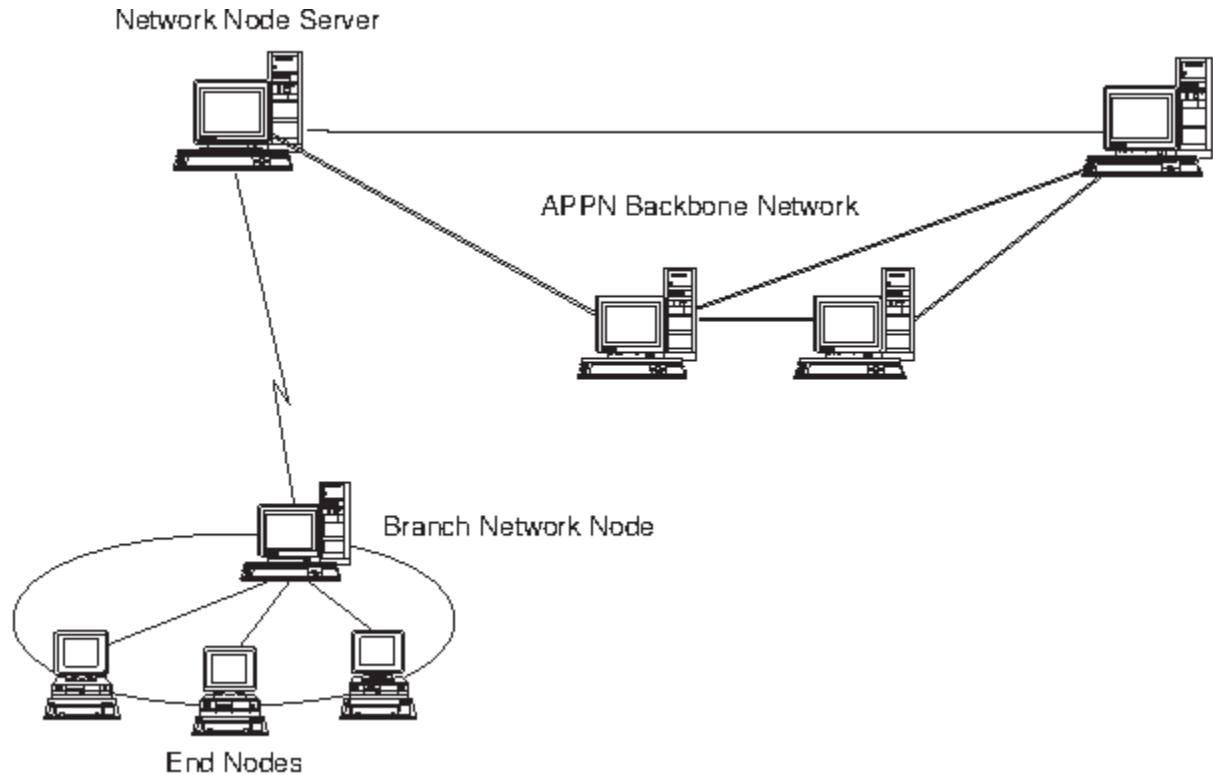


Abbildung 2. Branch Extender

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 Netzknosten 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 Netzknottenserver 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 Netzknosten übertragen.)
  - Der Zweignetzknoten registriert alle Ressourcen im Zweignetz auf seinem Netzknottenserver, 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 AIX- bzw. 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 Vorteile der APPN- und der IP-Konnektivität nutzen können.

Enterprise Extender wird in CS/AIX 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 kommunizieren (im Gegensatz zum SNA-Netz), werden als "TN3270-Programme" bezeichnet (Telnet-3270-Emulationsprogramme).

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.

CS/AIX TN Server ermöglicht TN3270-Benutzern den Zugriff auf 3270-Hosts. Über TN Server können TN3270-Benutzer eine Hostverbindung gemeinsam mit CS/AIX 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 CS/AIX ist in [Abbildung 3 auf Seite 9](#) veranschaulicht.

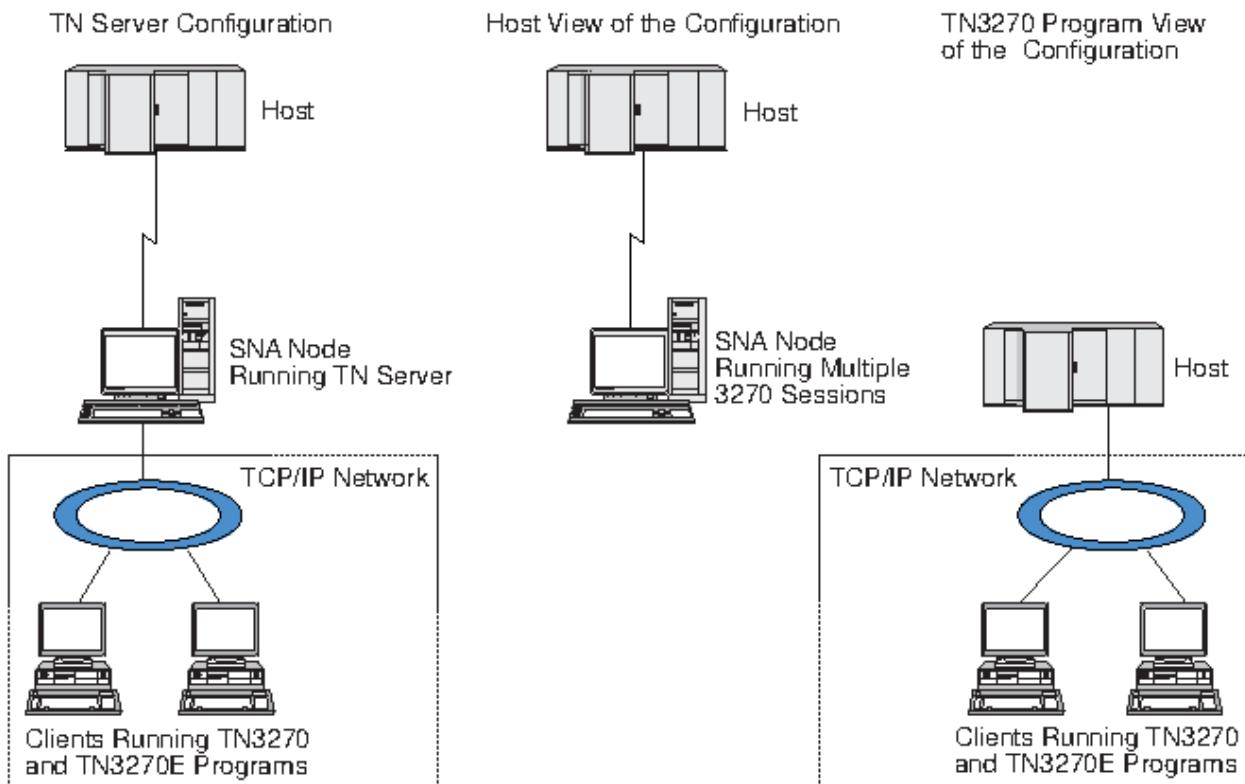


Abbildung 3. TN Server

Das Feature TN Server von CS/AIX ermöglicht die Zuordnung eines TN3270-Benutzers zu einer 3270-LU unter CS/AIX. 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.

CS/AIX TN Server unterstützt alle TN3270-Client-Emulationsprogramme, die die in den IETF-RFCs 1123, 1576, 1646, 1647 und 2355 definierten Protokolle richtig implementieren.

### **Sicherheitsfeatures**

CS/AIX TN Server 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 Clientauthentifizierung 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 Clientauthentifizierung 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.

### **Service Location Protocol (SLP)**

CS/AIX TN Server unterstützt außerdem das Service Location Protocol (SLP) mit Funktionen für Servicepositionen und Lastausgleich. Wenn Sie SLP verwenden, gibt jeder TN-Server Folgendes bekannt:

## Features und Vorteile

- die von ihm unterstützten Funktionen (in diesem Fall TN3270)
- seine aktuelle Auslastung (basiert auf dem Prozentsatz der zurzeit verwendeten verfügbaren LUs; kann jedoch auch mit einem Faktor berechnet werden, der andere Unterschiede zwischen TN-Servern berücksichtigt)

Ein SLP-fähiger TN3270-Client kann dann eine Verbindung zu dem für ihn am besten geeigneten Server herstellen. (Dies ist der am wenigsten ausgelastete Server, der die erforderlichen Funktionen anbietet.) Zu diesem Zweck kann der Client direkte Abfragen an TN-Server senden. Er kann aber auch einen Verzeichnisagenten abfragen, der die von TN-Servern zugänglich gemachten Informationen sammelt.

Ein großes SLP-Netz kann in Bereiche unterteilt werden. (Die Aufteilung geschieht in der Regel nach geografischen Regionen oder Abteilungen.) In einem solchen Fall werden Informationen zu einem TN-Server nur für TN3270-Clients und Verzeichnisagenten zugänglich gemacht, die sich in demselben Bereich wie der TN-Server befinden. Auf diese Weise können Sie steuern, welche bzw. wie viele TN3270-Clients die Dienste der einzelnen TN-Server nutzen können.

**Anmerkung:** Der Server, auf dem der TN Server ausgeführt wird, muss die IPV4-Adressierung unterstützen. Das bedeutet, er muss eine IPV4-Adresse haben (obwohl er auch eine IPV6-Adresse haben kann). Dies ist notwendig, weil SLP UDP-Broadcasts verwendet, die bei einer Installation, die nur IPV6 unterstützt, nicht verfügbar sind.

## TN Redirector

Das CS/AIX-Feature TN Redirector stellt Durchgriffsdiensste für 3270-, 5250- oder VT-Sitzungen über TCP/IP bereit. Der Telnet-Benutzer kommuniziert über eine TCP/IP-Verbindung mit CS/AIX und CS/AIX kommuniziert dann über eine weitere TCP/IP-Verbindung mit dem Host.

CS/AIX TN Redirector unterstützt mit der SSL-Software (Secure Sockets Layer) die Datenverschlüsselung sowie die Server- und die Clientauthentifizierung, 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 CS/AIX 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 CS/AIX und dem Host verwenden. Auf diese Weise wird die Sicherheit für alle Clients überprüft. Die einzelnen Clients müssen keine Sicherheitsangaben machen.
- Wenn CS/AIX an demselben Standort wie der Host installiert ist, die Clients die Verbindung jedoch von externen Standorten aus aufbauen, können Sie SSL für die Clientverbindungen zu CS/AIX verwenden und müssen die SSL-Software nicht auf dem Host installieren.

## Features und Vorteile

---

Die Features und Vorteile von CS/AIX reichen von der vereinfachten Konfiguration über die verbesserte Problemanalyse bis hin zur Erhöhung des Durchsatzes im Netz.

## Vielseitige Bausteine

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

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

Durch APIs für Netzverwaltung kann der AIX-Computer als MS-Eingangspunkt konfiguriert werden und bietet dann Unterstützung für die verteilte Netzverwaltung. Auf Verbindungsebene kann der AIX-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 for Data Center Deployment für AIX“ auf Seite 1 und „Installationsvoraussetzungen“ auf Seite 17.)

## 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 Clientdurchsatz 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 mehrerer 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 Verwaltungstools von CS/AIX ermöglicht eine transparente Verwaltung aller Domänenressourcen von jedem Computer in der Domäne.
- SNA-Anwendungen können über Internetprotokolle miteinander verbunden werden, die für die Überwindung von Firewalls sowie für Authentifizierung und Sicherheit TCP/IP und HTTPS verwenden.
- Clientanwendungen können mobil sein. Communications Server kann die Benutzer verfolgen, so dass der Host die Anwendung überall kontaktieren kann.
- Remotebenutzer, die eine Anwendung in einer Farm von Windows-Terminal-Server (WTS), Citrix-Server oder UNIX-X-Server ausführen, können sich von jedem Server der Farm verbinden. Die Hostanwendung kann sich selbst dann mit dem Remotebenutzer wieder verbinden, wenn der Benutzer zwischen mehreren Servern wechselt.
- Clientanwendungen können in Containern ausgeführt werden, die eine Verbindung zu einem Server für SNA-Ressourcen herstellen, die für die Verbindung von Sitzungen mit fernen SNA-Knoten erforderlich sind.

## Problemlose Konfiguration

CS/AIX 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/AIX-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/AIX-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 Hilfeseiten mit übersichtlichen Informationen zu SNA und CS/AIX, Referenzinformationen zu CS/AIX-Dialoganzeigen und Anleitungen zur Ausführung bestimmter Aufgaben bereit.

### Webverwaltungsprogramm

Zu CS/AIX gehört auch ein Webverwaltungsprogramm, das ähnliche Funktionen wie das Motif-Verwaltungsprogramm bereitstellt. Mit diesem Programm können Sie CS/AIX von Ihrem Browser aus verwalten und müssen keine X- oder Telnet-Sitzung mit dem CS/AIX-Server starten. Dies ist besonders hilfreich, wenn die Leistungen für Ihre Verbindungen langsam und störungsanfällig sind.

### 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 optimal 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 Schnittstellenoptionen für Verwaltung

Das Motif-Verwaltungsprogramm wird als Schnittstelle für die Konfiguration und Verwaltung von CS/AIX empfohlen. Für CS/AIX 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/AIX-Ressourcen verwendet werden. Sie können snaadmin direkt an einer AIX-Eingabeaufforderung ausführen oder in eine Shell-Prozedur integrieren.

#### System Management Interface Tool (SMIT)

Die SMIT-Schnittstelle ist für AIXwindows-Umgebungen in der grafischen Motif-Version und für ASCII-Terminals in der zeichenorientierten Version verfügbar. In beiden Versionen zeigt SMIT Dialoge für eine komfortable Eingabe von Konfigurations- und Betriebsdaten an.

#### API NOF

Die API NOF für CS/AIX 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 CS/AIX schreiben.

## Verbesserte Leistung

CS/AIX verbessert die ohnehin hohe Leistungsfähigkeit von SNA-Netzen und verwendet Serviceklassen. Darüber hinaus optimiert CS/AIX 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 CS/AIX sowohl HPR (High-Performance Routing) als auch ISR (Intermedia-te 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 Zwischenknoten umgehen kann.
- Ein weiterer Mechanismus zur Steuerung des Datenverkehrs, die angepasste Nachrichtendosierung auf Sitzungsebene, greift bei Überlastung automatisch durch Steuerung der Geschwindigkeit ein, mit der LUs Nachrichteneinheiten an Partner-LUs senden.

## Sicherheitsoptionen

Da Netze immer komplexer werden und die Architektur immer offener wird, steht auch das Thema Sicherheit mehr im Vordergrund. Bei SNA-Netzen mit CS/AIX 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 Clientverbindungen mit Sicherheitszertifikaten authentifiziert. (Dieses Feature erfordert neben dem Standardpro-

dukt CS/AIX zusätzliche Software. Weitere Informationen hierzu finden Sie im Abschnitt „[Installationsvoraussetzungen](#)“ auf Seite 17)

- 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.
- Auf der Verbindungsebene bieten Glasfaserkabel ein zusätzliches Maß an Sicherheit. Bei diesem Übertragungsmedium gibt es (im Gegensatz zur normalen elektrischen Leitung) keine Signallecks. Leitungen dieser Art können somit nicht so leicht "angezapft" werden.
- CS/AIX TN Server und TN Redirector unterstützen mit der SSL-Software (Secure Sockets Layer) die Datenverschlüsselung sowie die Server- und die Clientauthentifizierung zwischen dem CS/AIX-Server und TN3270- oder Telnet-Clients. (Dieses Feature erfordert neben dem Standardprodukt CS/AIX zusätzliche Software. Weitere Informationen hierzu finden Sie im Abschnitt „[Installationsvoraussetzungen](#)“ auf Seite 17)

## Flexible Netzverwaltung

CS/AIX verwendet zwei Arten von Netzverwaltungsschemata:

- MDS-NMVT (Multiple Domain Support - Network Management Vector Transport) kann als zentrales, verteiltes oder hierarchisches Verwaltungsschema eingesetzt werden. 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.

- Simple Network Management Protocol-Management Information Base (SNMP-MIB) basiert auf einer Agentenmanagerarchitektur und ist ein verteilter Verwaltungsservice, der an APPN-Netze angepasst wurde. Dieses Verwaltungsschema umfasst mehrere Komponenten: mindestens einen SNMP-Agenten, einen Manager und eine MIB-Datenbank. Diese Komponenten befinden sich normalerweise auf verschiedenen Knoten.
  - Ein SNMP-Agent ist ein Prozess, der auf einem verwalteten System ausgeführt wird und dessen Status überwacht. Der Agent verwaltet eine MIB-Datenbank für das verwaltete System.
  - Der Manager ist eine Anwendung, die beim Agenten Informationen von der MIB abfragt und die Antworten verarbeitet. Der Manager kann vom Agenten auch nicht erwartete Daten (SNMP-Alarmnachrichten) empfangen. Manager und Agent kommunizieren über das SNMP-Protokoll miteinander.

APPN-Netzmanager können aus der APPN-SNMP-MIB Informationen für die Netzanalyse und die Behebung von Fehlern anfordern.

CS/AIX verwendet Agentensoftware, die die APPN-MIB unterstützt. Weitere Informationen zur APPN-MIB finden Sie im *Verwaltungshandbuch für IBM Communications Server for Data Center Deployment für AIX* und auf der AIW-Homepage von IBM unter <http://www.networking.ibm.com/app/aiwhome.htm>.

## Zuverlässigkeit, Verfügbarkeit und Wartungsfreundlichkeit

Zur Aufrechterhaltung eines zuverlässigen Systembetriebs stellt CS/AIX eine Reihe von Anzeigefunktionen und Fehlerbestimmungstools 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 Fehlermeldungen, 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 CS/AIX 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 CS/AIX integriert, so dass Sie die gesamte CS/AIX-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 CS/AIX 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 und Remote API Client bieten außerdem einen Mechanismus für die Integration von SNA- und TCP/IP-Netzen an. Der Remote API Client unterstützt zudem Container für cloudbasierte Anwendungsimplementierungen.

# Kapitel 2. Netz mit IBM Communications Server for Data Center Deployment für AIX planen

Dieses Kapitel bietet einen Überblick über die Schritte bei der Planung eines Netzes, in dem CS/AIX ausgeführt wird. Darüber hinaus finden Sie hier eine Zusammenfassung der Funktionen, die Sie für einen AIX-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 CS/AIX und AIX.

Zur Planung eines Netzes gehört das Abwegen 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 CS/AIX konfiguriert werden kann, um die von Ihnen gewünschten Funktionen bereitzustellen.
- Kalkulieren Sie die erforderlichen Ressourcen und die damit zusammenhängenden Kosten für die Installation von CS/AIX zur Unterstützung Ihrer Leistungs- und Kapazitätsanforderungen und von CS/AIX-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?
- Müssen die SNA-Anwendungen in Containern ausgeführt werden? Wenn ja, ist ein Client-Server-System erforderlich, da sich der Server nicht in einem Container befinden kann.
- Wird CS/AIX als Client-Server-System ausgeführt? Wenn ja, werden alle Computer in einer CS/AIX-Domäne arbeiten oder müssen mehrere separate Domänen definiert werden?
- Wird in der CS/AIX-Domäne mehr als ein Server benötigt, um den Lastausgleich für Konnektivitätsressourcen zu ermöglichen? Wenn ja, welcher Server soll dann der Controllerkonfigurationsserver sein? Müssen Ausweichkonfigurationsserver bereitgestellt werden?
- Wird HTTPS-Unterstützung für die Verbindung von Remote API Clients zu CS/AIX-Servern benötigt?
- Werden Benutzeranwendungen auf dem Server oder auf AIX-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?
- Muss CS/AIX IPV4- und/oder IPV6-Verbindungen unterstützen?

## Schritte bei der Netzplanung

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

## Konfiguration von CS/AIX planen

Wie CS/AIX 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 CS/AIX 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 Peerknoten zu kommunizieren)
- LEN-Knoten (die direkt mit Nachbarknoten oder als Scheinnachbarknoten konfigurierten Knoten kommunizieren)
- Hostterminalemulation mit LU 2
- 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 CS/AIX beispielsweise als APPN-Netzknoten konfigurieren, der Routingdienste 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 CS/AIX 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/AIX-Funktionen müssen folgende Fragen beantwortet werden:

- Welche Qualifikation müssen die Mitarbeiter haben?
- Welches AIX-Workstationmodell wird benötigt?
- Welches Übertragungsmedium wird voraussichtlich verwendet?
- Welches sind die Installationsvoraussetzungen für die ausgewählte Konfiguration?
- Wie viel Hauptspeicher und Seitenwechselbereich ist für die Verarbeitung erforderlich?
- Mit welcher Antwortzeit ist bei dem angenommenen Datenverkehrsaufkommen zu rechnen?

Die Beantwortung dieser Fragen hilft Ihnen bei der Festlegung der Ressourcenarten, die CS/AIX verwendet, wenn das Produkt für die Unterstützung einer oder mehrerer der im Abschnitt „[Funktionsanforderungen für das Netz](#)“ auf [Seite 15](#) beschriebenen Funktionen konfiguriert wird. Die Beantwortung der Fragen hilft Ihnen darüber hinaus, das Verhältnis zwischen CS/AIX-Funktionen, AIX-Ressourcen und Netzressourcen besser zu verstehen.

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

## Personalanforderungen

Zum Installieren, Ausführen und Optimieren von CS/AIX ist folgendes Personal erforderlich:

- Netzadministratoren, die das Netz planen, neue Einheiten hinzufügen und die Gesamtnetzleistung gewährleisten und verbessern
- Systemadministratoren, die CS/AIX und die zugrunde liegende Hardware installieren bzw. warten und Systeme für die Netzverbindung konfigurieren
- Programmierer, die angepasste Anwendungen wie Transaktionsprogramme und Netzverwaltungs Routinen entwickeln

Die Netz- und Systemadministratoren müssen mit der Hardware, auf der CS/AIX ausgeführt wird, und mit dem Betriebssystem AIX 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 oder System Management Interface Tool (SMIT) für AIX
- TCP/IP, falls die Verwendung von Client-Server-Funktionen, TN Server oder Enterprise Extender geplant ist
- Windows, Red Hat Enterprise Linux, SuSE Linux Enterprise Server, Ubuntu Linux und AIX. Der Remote API Client kann unter jedem dieser Betriebssysteme ausgeführt werden.
- WebSphere Application Server, falls zum CS/AIX-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 CS/AIX verfügbar sind, vertraut sein.

## **IBM Power-Modelle**

IBM Communications Server for Data Center Deployment für AIX ist für die Ausführung auf einer AIX-Workstation konzipiert, die mit einem oder mehreren Netz(en) verbunden ist. CS/AIX Version 7.1 kann auf jedem IBM Power 8 System oder Power 9 System ausgeführt werden, das von AIX ab Version 7.2 unterstützt wird. (Der Server darf nicht auf einer System- oder Anwendungs-WPAR ausgeführt werden. Er muss in der globalen Umgebung ausgeführt werden.)

Weitere Informationen zu den relativen CPU-Geschwindigkeiten der verschiedenen IBM Power Systems finden Sie im Internet unter <http://www.ibm.com/it-infrastructure/power>.

## **Übertragungsmedien**

CS/AIX wird möglicherweise neben anderen Übertragungsprotokollen auf demselben Übertragungsmedium (wie SDLC oder Ethernet) ausgeführt. Aus diesem Grund muss die Bandbreite der Bitübertragungsschicht für alle Protokolle und Anwendungen, die auf demselben Übertragungsmedium ausgeführt werden, ausreichend sein.

**Anmerkung:** CS/AIX kann die Token-Ring-, Ethernet- und X.25-Adapter zusammen mit anderen Protokollen wie TCP/IP verwenden. Es ist möglicherweise erforderlich, eindeutige SAP-Adressen für jedes verwendete Protokoll anzugeben. CS/AIX kann auch einen MPQP-Adapter (Multiprotocol Quad Port), jedoch keinen MPQP-Port nutzen.

## **Installationsvoraussetzungen**

Die Funktionen, die Sie CS/AIX (aus dem Abschnitt „Funktionsanforderungen für das Netz“ auf Seite 15) zuordnen, bestimmen gleichzeitig die Installationsvoraussetzungen. Dieser Abschnitt bietet einen Überblick über die für die Installation von CS/AIX erforderlichen Computerressourcen. Weitere Informationen hierzu finden Sie in der zu den einzelnen Produkten gelieferten Dokumentation. (Das Literaturverzeichnis enthält hierzu eine Liste mit Büchern.)

### **Verbindungshardware**

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

Die Installation einer AIX-Power-Systems-Workstation in einem oder mehreren Netz(en) erfordert, dass die Verbindungen nicht in Widerspruch zu dem ausgewählten Übertragungsprotokoll des Netzes

## Schritte bei der Netzplanung

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 AIX TCP/IP erforderlichen Adapter.

CS/AIX unterstützt DFV-Adapter für die folgenden Verbindungsprotokolle:

- Token-Ring
- Ethernet (Standard oder IEEE 802.3)
- SDLC
  - IBM 2-Port PCI
  - IBM 4-Port MPQP

Die folgenden Verbindungsprotokolle erfordern Produkte oder Features, die nicht im Lieferumfang von CS/AIX enthalten sind:

- X.25 (erfordert das Produkt AIXLink/X.25)
- ATM mit emulierter LAN-Schnittstelle (Token-Ring oder Ethernet) über einen IBM AIX-ATM-Adapter
- Frame Relay mit einer emulierten Token-Ring-Schnittstelle

Informationen zu Adapters, die mit CS/AIX getestet wurden, finden Sie auf der Webseite [http://www.ibm.com/software/network/commserver/about/comp\\_products/adapter\\_csaix.html](http://www.ibm.com/software/network/commserver/about/comp_products/adapter_csaix.html).

Wenn Sie Fragen bezüglich des passenden Adapters oder der erforderlichen Hardware haben, wenden Sie sich an Ihren IBM Vertriebsbeauftragten.

### Software: AIX-Server

Bevor Sie CS/AIX auf Ihrer AIX-Workstation installieren und verwenden können, muss auf der Workstation die folgende Software installiert sein:

- Eine der folgenden Versionen des AIX-Basisbetriebssystems:
  - AIX ab Version 7.2
- Entsprechende DLC-Unterstützung (für die Installation nicht erforderlich, jedoch für die Verwendung von CS/AIX). Weitere Informationen zu DLCs finden Sie im Abschnitt „Dateigruppen für Datenübertragungssteuerung installieren“ auf Seite 28.
- Unterstützung für Motif Version 1.2 (Diese Unterstützung ist Teil des AIX-Basisbetriebssystems und erforderlich, wenn Sie die SSL-Funktionen von CS/AIX TN Server und/oder TN Redirector nutzen oder das Motif-Verwaltungsprogramm verwenden möchten.)
- Java-Software (ist erforderlich, wenn Sie Java CPI-C verwenden möchten). Das neueste, unter <http://www.ibm.com/developerworks/java/jdk> verfügbare Java SDK erfüllt alle Voraussetzungen.

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

- Wenn Sie Anwendungen mit CS/AIX-APIs im 64-Bit-Modus ausführen möchten, wird die AIX-Option `bos.64bit` vorausgesetzt. Sie müssen diese Option installieren und mit dem Befehl `smit lo-ad64bit` konfigurieren, um sicherzustellen, dass sie vor der Ausführung von 64-Bit-Anwendungen geladen wird. Falls Sie auf diesem Computer 64-Bit-Anwendungen kompilieren und verknüpfen möchten, die auf einem anderen Computer ausgeführt werden sollen (was bei der Verwendung verschiedener Computer für die Anwendungsentwicklung und das Testen von Anwendungen der Fall ist), ist die Option `bos.64bit` nicht erforderlich.
- Software AIX Certificate and SSL Base Runtime. Die Software AIX Certificate and SSL Base Runtime ist auf einem Server erforderlich, wenn Sie die SSL-Funktion von TN Server oder TN Redirector ver-

wenden möchten. Die Software ist auf dem Installationsdatenträger enthalten und wird automatisch mit CS/AIX installiert.

- GSKit. Das Global Security Kit ist auf einem Client erforderlich, wenn dieser via HTTPS eine Verbindung zu CS/AIX herstellt. Weitere Informationen zur Beschaffung und Installation der GSKit-Software enthält die README-Datei auf dem Clientinstallationsdatenträger.
- Ein Webserver mit Unterstützung für Java-Servlets (ist für das Webverwaltungsprogramm erforderlich). Mit CS/AIX wurde IBM HTTP Server (IHS) Version 6.0.1 getestet.

Falls Sie einen anderen Webserver verwenden möchten oder diesen Webserver installieren, nachdem Sie CS/AIX installiert haben, müssen Sie CS/AIX-Verzeichnisse mit den Verzeichnissen des Webservers verknüpfen. Ausführliche Informationen hierzu finden Sie im Abschnitt „Webserver für das Webverwaltungsprogramm konfigurieren“ auf Seite 36. (Falls der oben angegebene Webserver bereits installiert ist, konfiguriert der CS/AIX-Installationsprozess die erforderlichen Verknüpfungen automatisch.)

- Ein Webbrower mit Unterstützung für Java (ist für das Webverwaltungsprogramm erforderlich). Folgende Webbrower wurden mit CS/AIX getestet:
  - Microsoft Internet Explorer ab Version 4 SP1
  - Netscape Navigator ab Version 4.06

### **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/AIX-Servern herstellen, benötigen Sie WebSphere Application Server, um diesen Clients den HTTPS-Zugriff auf die Server zu ermöglichen.

CS/AIX arbeitet mit WebSphere Application Server Version 8. 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 AIX-Computer wie CS/AIX Server installiert werden.) Weitere Informationen zur Installation von WebSphere Application Server finden Sie in der zugehörigen Dokumentation. Um WebSphere zusammen mit CS/AIX verwenden zu können, müssen Sie ein zusätzliches CS/AIX-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 CS/AIX, die das gesamte Spektrum der Konfigurationen und Dienste unterstützen soll, muss über den für das Betriebssystem AIX erforderlichen Mindestspeicher und zusätzlich über 64 MB Hauptspeicher sowie über einen Plattspeicherplatz von 200 MB verfügen. Während der Installation sind zusätzlich 250 MB temporärer Speicher erforderlich.

Nachrichten und Hilfetexte werden in mehreren verschiedenen Landessprachen bereitgestellt. Sie müssen die Dateigruppen für mindestens eine Landessprache installieren. Bei Bedarf können Sie weitere Dateigruppen installieren. Pro Sprache ist (je nach Sprache) ein Plattspeicherplatz von 2,5 bis 4 MB erforderlich.

Falls Sie die Dokumentation zu CS/AIX als Softcopy (PDF) installieren wollen, benötigen Sie zusätzlichen Festplattspeicherplatz. Auch hier sind Versionen in verschiedenen Landessprachen verfügbar. Für die Installation der Handbücher in amerikanischem Englisch benötigen Sie 28 MB Plattspeicherplatz. Für jede weitere Sprachversion sind bis zu 17 MB Plattspeicherplatz erforderlich.

**Anmerkung:** In den hier genannten Anforderungen sind der Hauptspeicher- und Plattspeicherbedarf für andere Lizenzprogramme, Benutzeranwendungen und Daten nicht enthalten. Sprechen Sie alle Systemvoraussetzungen sowie den Hauptspeicher- und Plattspeicherbedarf 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 CS/AIX von vielen verschiedenen Faktoren abhängig, die je nach Funktion und Umgebung der AIX-Workstation variieren. Wenn Sie jedoch die Grundre-

gel 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.

Weitere Informationen zur Nutzung, Zuordnung und Optimierung von Ressourcen für die Knotenfunktion finden Sie im Internet unter <https://www.ibm.com/products/communications-server-for-data-center>.

## Hauptspeicher- und Speicherbedarf für den Betrieb

In diesem Abschnitt wird der Hauptspeicher- und Speicherbedarf für eine Workstation mit CS/AIX erläutert.

### Speicherpuffer (mbufs)

AIX verwendet Speicherpuffer (mbufs), um die Kommunikation zwischen DFV-Subsystemen und AIX-DLCs zu ermöglichen. Der mbuf-Pool ist eine gemeinsam genutzte Ressource, die auf Systemebene verwaltet werden muss. CS/AIX verwendet mbufs zum Senden und Empfangen von Daten über das Netz. Hierbei handelt es sich lediglich um eines der Subsysteme, die mbufs verwenden. Die mbuf-Auslastung durch CS/AIX kann die Leistung anderer Subsysteme wie TCP/IP, NFS oder DCE beeinflussen. Den mbuf-Bedarf sollten Sie mit Ihrem Netzadministrator absprechen.

### Haupt- und Plattenspeicher und Speicher für Seitenwechsel

CS/AIX 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.
- Speicherpuffer belegen nur primären Speicher.
- Die ausführbaren Daten, Konfigurationsdateien und Softcopyveröffentlichungen zu CS/AIX 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 mbuf-Belegung. Der Plattenspeicherbedarf ist von dem für TPs, Sitzungen und den damit zusammenhängenden Prozessen erforderlichen Seitenwechselbereich 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

CS/AIX erfordert mindestens 20 AIX-Prozesse.

## Antwortzeit

Die Antwortzeit für die erwarteten Datenverkehrsaufkommen zu bestimmen, ist aufgrund der Vielzahl von Bedingungen im Netzbetrieb nicht möglich. Da es auch keine knappe Formel zur Darstellung der Antwortzeit gibt, wird sie am besten anhand experimenteller Daten ermittelt, die Sie für Ihr Netz extrapoliieren können.

Auf den Webseiten zu IBM Communications Server unter <https://www.ibm.com/products/communications-server-for-data-center> finden Sie verschiedene Netzkonfigurationen mit einer Darstellung des Einflusses, den Faktoren wie das Modell der AIX-Workstation oder die Anzahl aktiver Sitzungen auf die Antwortzeit haben. Diese Angaben sollen Sie bei der Abschätzung der Antwortzeit für Ihr Netz unterstützen.

## IPV4- und IPV6-Adressen

Computer, auf denen CS/AIX Version 7.1 ausgeführt wird, können unter Beachtung der folgenden Einschränkungen IPV4- oder IPV6-Adressen verwenden.

- Alle Server in einer Client-Server-Domäne müssen dasselbe Adressformat (IPV4 oder IPV6) verwenden.
  - Wenn die Server IPV4 verwenden, müssen Clients auch IPV4 verwenden.
  - Wenn die Server IPV6 verwenden, können Clients IPV6 oder IPV4 verwenden.
- Falls CS/AIX IPV4 verwendet, müssen TN-Clients, die eine Verbindung zum TN-Server herstellen, ebenfalls IPV4 verwenden. Wenn CS/AIX IPV6 verwendet, können TN-Clients entweder IPV6 oder IPV4 verwenden. Standardmäßig akzeptiert der TN-Server Verbindungen von beiden Clienttypen. Sie können ihn jedoch (mit dem Parameter *listen\_local\_address* im Befehlszeilenverwaltungsprogramm oder in einer NOF-Anwendung) so konfigurieren, dass er an einer bestimmten IP-Adresse empfangsbereit ist, um ihn auf einen Clientverbindungstyp zu beschränken.
- Für TN Redirector gilt, dass beide TCP/IP-Verbindungen (vom Client zu CS/AIX und von CS/AIX zum Host) IPV4 verwenden müssen, wenn CS/AIX IPV4 verwendet.

Verwendet CS/AIX IPV6, gelten für die TCP/IP-Verbindung vom Client zu CS/AIX dieselben Regeln wie für TN Server. Für die Verbindung von CS/AIX zum Host kann IPV6 oder IPV4 verwendet werden. Es ist nicht erforderlich, dass die beiden Verbindungen dasselbe Adressformat verwenden.

- Wenn Sie SLP verwenden, muss der TN Server die IPV4-Adressierung unterstützen. Das bedeutet, der Server muss eine IPV4-Adresse haben (obwohl er auch eine IPV6-Adresse haben kann). Dies ist notwendig, weil SLP UDP-Broadcasts verwendet, die bei einer Installation, die nur IPV6 unterstützt, nicht verfügbar sind.
- Für Enterprise Extender (HPR/IP) gilt, dass die Ports an beiden Enden der Verbindung dasselbe Adressformat verwenden müssen (IPV4 oder IPV6).
  - Wenn CS/AIX IPV4 verwendet, kann die Software nur Verbindungen zu fernen Systemen herstellen, die für die Unterstützung von IPV4 konfiguriert sind.
  - Verwendet CS/AIX IPV6, können Sie die Software so konfigurieren, dass sie für eine Enterprise-Extender-Verbindung IPV4 oder IPV6 verwendet. Die Option, die Sie auswählen, muss mit der Konfiguration auf dem fernen System übereinstimmen.

Darüber hinaus müssen alle Verbindungen an einem Enterprise-Extender-Port dasselbe Adressformat (IPV4 oder IPV6) verwenden. Falls Verbindungen mit anderen Adressformaten zu unterstützen sind, müssen Sie gesonderte Ports verwenden. Gleiches gilt, dass alle Enterprise-Extender-Ports in einem Verbindungsnetz dasselbe Adressformat verwenden müssen.

Mit dem Befehl `ifconfig -a` können Sie überprüfen, ob auf einem CS/AIX-Server IPV4 oder IPV6 ausgeführt wird. Sehen Sie sich in der Befehlsausgabe die IP-Adresse(n) an. Es handelt sich um IPV4-Dezimaladressen in Schreibweise mit Punkten und/oder IPV6-Hexadezimaladressen. Der funktional entsprechende Befehl für einen Remote API Client für Windows ist `ipconfig` (ohne Befehlszeilenoptionen). Falls Sie das IP-Adressformat des Computers ändern müssen, informieren Sie sich in der Dokumentation zu dem von Ihnen verwendeten Betriebssystem.

Wenn Sie für ein vorhandenes CS/AIX-System wie im Abschnitt „Vorversionen von CS/AIX migrieren“ auf Seite 29 beschrieben ein Upgrade durchführen und dabei gleichzeitig zu IPV6-Adressen wechseln

## Kompatibilität plattformübergreifender Konfigurationen gewährleisten

möchten, ist es egal, mit welchem der beiden Prozesse Sie beginnen. Die neue Funktionalität der IPV6-Adressen können Sie jedoch erst nach Abschluss beider Prozesse nutzen.

- Bei einem Client-Server-System müssen Sie für alle Server in der Domäne gleichzeitig den Wechsel von IPV4 zu IPV6 vollziehen. Versuchen Sie nicht, mit einer gemischten Domäne mit IPV4- und IPV6-Servern zu arbeiten.
- Da im Rahmen des Upgrades auf CS/AIX ein gleichzeitiges Upgrade aller Server ratsam ist, können Sie den Wechsel zu IPV6-Adressen beim Upgrade der einzelnen Server vollziehen. Alternativ dazu können Sie die Änderung in IPV6 auf allen Servern vor oder nach dem Upgrade durchführen.
- Nachdem Sie auf allen Servern den Wechsel zu IPV6-Adressen vollzogen haben, können Sie für Remote API Clients die Änderung in IPV6-Adressen durchführen, sofern dies erforderlich ist. IPV4-Clients können auch mit IPV6-Servern zusammenarbeiten, so dass Sie nicht alle Clients gleichzeitig ändern müssen.

Falls Sie ein neues System mit CS/AIX installieren, können Sie es ggf. ausschließlich mit IPV6-Adressen für alle Server und Clients installieren, sofern Ihnen dies angemessen erscheint. Sie können aber auch zunächst IPV4-Adressen verwenden und später den Wechsel zu IPV6-Adressen vollziehen. (Beachten Sie dabei die oben angegebenen Einschränkungen für Client-Server-Domänen.)

## Kompatibilität plattformübergreifender Konfigurationen gewährleisten

SNA-Produkte, die auf verschiedenen Plattformen ausgeführt werden, z. B. IBM Personal Communications, IBM Host-On-Demand oder VTAM auf einem Host, können unter bestimmten Voraussetzungen zusammen mit CS/AIX verwendet werden.

Im Allgemeinen funktioniert das aktuelle Release eines Produkts für den SNA-Netzbetrieb mit CS/AIX, so lange es PU-2.1-Knoten und mindestens eine der von CS/AIX 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.

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.
- 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 Registriungsstandards 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. CS/AIX auf AIX-Servern installieren

In diesem Kapitel ist die Installation von CS/AIX auf AIX-Computern beschrieben. Hier finden Sie auch Anweisungen für die Verwaltung der CS/AIX-Konfigurationsdaten.

## Anmerkung:

1. Für die Installation von CS/AIX benötigen Sie die Root-Berechtigung.
2. Bevor Sie CS/AIX verwenden können, müssen Sie eine Datenübertragungssteuerung (DLC) hinzufügen. Die DLC verwaltet den DFV-Adapter. Weitere Informationen können Sie der Beschreibung zum Befehl `mkdev` in der Veröffentlichung *AIX Commands Reference* entnehmen. Sie können auch im SMIT-Menü Einheiten die Option Kommunikation auswählen. (Zusätzliche Informationen hierzu finden Sie in der Veröffentlichung *AIX Communications Programming Concepts*.)
3. Bei AIX-Systemen, die WPAR-Umgebungen unterstützen, darf der Server nicht auf einer System- oder Anwendungs-WPAR und nicht in einem Container ausgeführt werden. Er muss in der globalen Umgebung ausgeführt werden. (Die Remote API Clients können auf Anwendungs-WPARs oder in Containern ausgeführt werden.)

## Lizenzierung und Konfektionierung von CS/AIX

Die folgenden Abschnitte enthalten Informationen zur Lizenzierung des Produkts CS/AIX und zu den Programm paketen.

### Mechanismen der Lizenzierung für CS/AIX

Dieser Abschnitt soll dem Leser einen besseren Einblick in die Lizenzierungsmechanismen vermitteln. Das Dokument *License Information* für CS/AIX enthält die vollständigen Vertragsbedingungen. Zusätzlich gibt es Beispieldaten zur weiteren Klarstellung der Lizenzierung für die verschiedenen Konnektivitäts- und Funktionstypen von CS/AIX. Sie finden diese Informationen unter <https://www.ibm.com/products/communications-server-for-data-center>.

Es ist zu berücksichtigen, dass zu CS/AIX mehrere Komponenten gehören.

Für jede Maschine bzw. jeden SP-Knoten, auf dem alle oder einige Komponenten von CS/AIX installiert werden, benötigen Sie eine gesonderte Programm lizenz.

Bei der Lizenzierung für CS/AIX wird zwischen der Programm lizenz (Serverlizenz) und Benutzerlizenzen unterschieden.

- Ein Benutzer ist als eine Person definiert. Für jeden gleichzeitig angemeldeten Benutzer, der direkt oder indirekt auf CS/AIX zugreift und das Produkt nutzt, müssen Sie eine Benutzerlizenz kaufen. Um eine indirekte Verwendung handelt es sich beispielsweise, wenn ein Multiplexing- oder Anwendungsserver (z. B. CICS, DB2, WebSphere oder Ihre eigene Geschäftsanwendung) eine Verbindung zu CS/AIX herstellt, über die mehrere gleichzeitig angemeldete Benutzer Zugriff haben. In dem Fall ist für jeden der gleichzeitig angemeldeten Benutzer eine Benutzerlizenz erforderlich.
- Bei Anwendungsprogrammen, die keinem bestimmten Benutzer zugeordnet sind, wird für jede aktive Verbindung einer übergeordneten oder untergeordneten Einheit zum CS/AIX-Knoten eine Benutzerlizenz benötigt. In einer APPN-Umgebung wird eine aktive Verbindung zu einem Nachbarknoten als eine Verbindung gewertet.

### CS/AIX mit einer Node-Lock-Lizenz aktivieren

Für die Aktivierung oder Inaktivierung von CS/AIX werden Node-Lock-Lizenzen verwendet. (Node-Lock-Lizenzen werden nicht von einem Lizenzserver im Netz, sondern auf einem bestimmten Knoten verwaltet.)

Eine Node-Lock-Lizenz kann eine permanente Lizenz sein oder ein temporärer Schlüssel, mit dem der Bediener CS/AIX für eine begrenzte Zeit nutzen kann (z. B. als Einführungsangebot oder zu Demonstrationszwecken). Mit dem Kauf des Produkts CS/AIX erwerben Sie eine permanente Node-Lock-Lizenz, die bei der Produktinstallation automatisch in der nodelock-Lizenzdatei des Systems installiert wird.

Bei der Installation von CS/AIX von einem Demonstrationsdatenträger, z. B. von einem CD-Showcase-Datenträger, wird das Produkt mit einem temporären Schlüssel installiert. Zur vollständigen Aktivierung des Produkts müssen Sie über Ihren IBM Vertriebskanal eine CS/AIX-Lizenz erwerben. Wenn Sie ein Upgrade für einen temporären Schlüssel durchführen möchten, können Sie einfach den permanenten Schlüssel vom CS/AIX-Installationsdatenträger installieren. Das Produkt muss nicht erneut installiert werden.

Gehen Sie wie folgt vor, um den Schlüssel von der CS/AIX-Installations-CD zu extrahieren:

1. Setzen Sie den Befehl smit bffcreate ab. In dem daraufhin angezeigten SMIT-Dialog können Sie das LPP-Image vom Installationsdatenträger extrahieren. Notieren Sie den Namen der Datei, die erstellt wird. Der Name sollte sna.7.1.0.0.I oder ähnlich lauten.
2. Extrahieren Sie den Schlüssel mit den folgenden Befehlen aus dem LPP-Image:

```
cd /tmp
restore -f /usr/sys/inst.images/installpp/ppc/Dateiname ./usr/lib/sna/install/
license.sna
```

Ersetzen Sie *Dateiname* durch den in Schritt 1 notierten Dateienamen.

3. Kopieren Sie den Schlüssel mit dem folgenden Befehl in die Datei /var/ifor/nodelock. Achten Sie darauf, den Verknüpfungsoperator >> zu verwenden, um den Schlüssel in die Datei einzubinden. (Verwenden Sie **nicht** den Operator >, da mit diesem alle alten Schlüssel überschrieben werden.)

```
cat /tmp/usr/lib/sna/install/license.sna >> /var/ifor/nodelock
```

## Verwendung von CS/AIX-Ressourcen überwachen

Es gibt zwei Möglichkeiten der Lizenzierung für Communications Server for Data Center Deployment, einschließlich CS/AIX: Prozessor-Value-Unit (PVU) oder Lizzenzen für gleichzeitig angemeldete Benutzer. Es wird nur jeweils eine Lizenzmethode verwendet. Bei der PVU-Lizenzierung richtet sich die Lizenz nach der Anzahl der Kerne, die für die Ausführung von CS/AIX-Servern zugeordnet sind. Wenn Sie virtuelle Maschinen verwenden, können 2 oder mehr Kerne 1 oder mehr Server-Images von CS/AIX ausführen. Daher ist es notwendig, die PVU-Nutzung mit IBM Tivoli License Manager (ITLM) zu überwachen. Bei der Lizenzierung für gleichzeitig angemeldete Benutzer protokolliert der CS/AIX-Server die Anzahl gleichzeitiger Datensitzungen, die vom TN3270-Client, den TN-Redirector-Ports sowie den APPC- und LU0-3-Anwendungen genutzt werden. Der Gesamtwert wird alle 30 Minuten in der Datei /var/sna/ad8a7aebe-fee4d8e9554c14f5f734b7b.slmtag protokolliert.

## Angebotene CS/AIX-Lizenzyprogrammpakete

Das Lizenzprogramm CS/AIX besteht aus mehreren Paketen (installierbaren Images), die jeweils mindestens eine Dateigruppe enthalten. Eine Dateigruppe ist die kleinste installierbare Produkteinheit. AIX pflegt für jede Dateigruppe die Release- und Versionsangabe. (Lesen Sie hierzu die Informationen zum AIX-Befehl ls1pp im Abschnitt „[Details der Produktinstallation anzeigen](#)“ auf Seite 28.) Das Lizenzprogramm kann auch Updatedateien enthalten.

**Anmerkung:** Informationen zum Speicherbedarf finden Sie im Abschnitt „[Installationsvoraussetzungen](#)“ auf Seite 17.

Die folgenden Dateigruppen sind erforderlich, wenn Sie CS/AIX installieren. Diese beiden Pakete müssen zusammen installiert werden:

### sna-Paket

#### sna.rte

CS/AIX-Basisprogramm

sna.rte64 wird für sna.rte vorausgesetzt.

**sna.rte64**

Dateigruppen für 64-Bit-API-Unterstützung

sna.rte wird für sna.rte64 vorausgesetzt.

**Dateigruppen für SSL-Unterstützung**

Zur SSL-Unterstützung für TN Server oder TN Redirector steht die folgende Dateigruppe zur Verfügung:

**gskta.rte**

AIX Certificate and SSL Base Runtime

**sna.gsk\_jre**

JRE für den Zertifikatsschlüsselmanager

**GSKIT8.gskssl132**

GSKit-SSL-Paket

**GSKIT8.gskcrypt32**

GSKit-Verschlüsselungspaket

## Features von CS/AIX

Im Lieferumfang von CS/AIX sind die folgenden Features enthalten, die Sie bei Bedarf installieren können.

**sna.xsna**

Motif-Verwaltungsprogramm

sna.rte, X11.base.rte und X11.Dt.helprun werden für sna.xsna vorausgesetzt.

**sna.wa**

Webverwaltungsprogramm

sna.rte wird für sna.wa vorausgesetzt.

**sna.docs.Sprache.data**

Onlinedokumentation. *Sprache* steht hier für die Sprache, in der die Dokumente angezeigt werden sollen (z. B. fr\_FR für Französisch).

**sna.man.en\_US.rte.data, sna.man.en\_US.xsna.data**

AIX-Man-Pages für CS/AIX-Befehle

**Paket sna.msg.Sprache**

CS/AIX-Nachrichtenkatalog mit Nachrichten und Hilfedateien zu Dialoganzeigen in der angegebenen Sprache für die Laufzeitumgebung. Sie benötigen die folgende Dateigruppe:

**sna.msg.Sprache.rte**

Nachrichten und Hilfedateien zu Dialoganzeigen für die CS/AIX-Basisfeatures. *Sprache* steht hier für die Sprache, in der die Nachrichten angezeigt werden sollen. Wählen Sie eine der folgenden Sprachenkennungen aus:

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

Falls Sie ein Produkt in mehreren Sprachen installieren möchten, müssen Sie die bevorzugte (primäre) Sprache zuerst installieren. Wenn Sie beispielsweise Englisch (US) als Primärsprache installieren möchten, geben Sie Folgendes an:

```
sna.msg.en_US.rte
```

sna.rte wird für sna.msg.Sprache.rte vorausgesetzt.

### Communications.Bnd

Paketdefinition für die einfache Installation (siehe Abschnitt „[Installationsmethoden](#)“ auf Seite 30)

## Installation von CS/AIX vorbereiten

Wenn Sie CS/AIX installieren wollen, muss AIX ab Version 7.2 aktiv sein. (Der Server darf nicht auf einer System- oder Anwendungs-WPAR und nicht in einem Container ausgeführt werden. Er muss in der globalen Umgebung ausgeführt werden.) Führen Sie dann die folgenden Schritte aus:

- Installieren und konfigurieren Sie die für die Kommunikation über das Netz erforderlichen DLCs. Lesen Sie hierzu die Beschreibung im Abschnitt „[Dateigruppen für Datenübertragungssteuerung installieren](#)“ auf Seite 28. (Die Installation und Konfiguration von DLCs ist eine der Voraussetzungen für die Verwendung von CS/AIX. Sie können die DLCs auch im Anschluss an CS/AIX installieren.)
- Wenn Sie das Webverwaltungsprogramm nutzen möchten und noch keinen geeigneten Webserver installiert haben, sollten Sie den Webserver jetzt installieren. Die von CS/AIX unterstützten Webserver sind im Abschnitt „[Installationsvoraussetzungen](#)“ auf Seite 17 aufgelistet. Führen Sie die zur Webserver-Software gelieferten Installationsanweisungen aus.
- Stellen Sie sicher, dass die Produktdialoge und Nachrichten korrekt verarbeitet und angezeigt werden können, indem Sie die Umgebungsvariable LANG richtig einstellen. Lesen Sie hierzu die Beschreibung im Abschnitt „[Sprachumgebungsvariable ändern](#)“ auf Seite 29.

## Dateigruppen für Datenübertragungssteuerung installieren

CS/AIX benötigt für die Kommunikation über das Netz mindestens eine AIX-DLC-Dateigruppe. Folgende DLC-Dateigruppen sind verfügbar:

- bos.dlc.token für Token-Ring-Verbindungsstationen
- bos.dlc.ether für Standard-Ethernet-Verbindungsstationen
- bos.dlc.8023 für 802.3-Ethernet-Verbindungsstationen
- bos.dlc.qllc für X.25-Verbindungsstationen
- bos.dlc.sdlc für SDLC-Verbindungsstationen

Alle bos.dlc-Dateigruppen gehören zum Paket `bos.dlc.usr` des AIX-Basisbetriebssystems. DLCs müssen einzeln installiert werden.

**Anmerkung:** Weitere Informationen zu AIX-DLCs finden Sie in der Veröffentlichung *AIX Communications Programming Concepts*.

## Details der Produktinstallation anzeigen

Geben Sie einen der folgenden Befehle ein, um die Installationshistorie für CS/AIX (und einige zugehörige Produkte) anzuzeigen:

Eingabe:	Für Produkt:
<code>1slpp -h sna.rte</code>	IBM Communications Server for Data Center Deployment für AIX

Wenn Sie die vorläufigen Programmkorrekturen (PTFs) anzeigen möchten, die seit der Installation des Produkts angewendet wurden, geben Sie den Befehl mit der Option -ha und nicht mit der Option -h ein.

## Sprachumgebungsvariable ändern

Wenn Sie CS/AIX 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.

## Vorversionen von CS/AIX migrieren

---

### Hinweise

Beachten Sie die folgenden Hinweise, wenn Sie für eine frühere Version von CS/AIX ein Upgrade auf CS/AIX Version 7.1 durchführen möchten.

1. Wenn Sie CS/AIX in einer Client-Server-Konfiguration mit zwei oder mehr Servern ausführen, sollten Sie für alle Server gleichzeitig das Upgrade auf Version 7.1 durchführen, bevor Sie das Upgrade für die Remote API Clients in Angriff nehmen.
  - Während der Migration der Server können Sie auf einem Server mit einer früheren Version weder das Motif-Verwaltungsprogramm noch das Befehlszeilenverwaltungsprogramm verwenden, um Ressourcen auf einem Server mit Version 7.1 anzuzeigen oder zu verwalten.
  - Version 6.3.1.0 und aktuellere Versionen des Remote API Client funktionieren mit einem vorhandenen Server. Dies gilt jedoch nur, wenn das Betriebssystem auf dem Client nicht für die Verwendung von IPV6 konfiguriert ist.
  - Frühere Versionen des Remote API Client funktionieren mit CS/AIX Version 7.1.
  - Insbesondere ältere Clients unter Betriebssystemen, für die mit CS/AIX Version 7.1 keine Clients ausgeliefert werden (z. B. 32-Bit-Windows-Betriebssysteme), funktionieren weiter mit CS/AIX Version 7.1.
2. Mehrere Datenstrukturen der API NOF wurden in Version 6.2.3.0 so geändert, dass sie das für IPV6-Adressen erforderliche längere Adressformat akzeptieren. Wenn Sie in einer vorhandenen NOF-Anwendung, die vor Version 6.2.3.0 erstellt wurde, eines der folgenden Verben und/oder eine der folgenden Angaben verwenden, müssen Sie die Anwendung somit nicht erneut kompilieren, um sie mit CS/AIX Version 7.1 verwenden zu können. (Dies gilt auch, wenn Sie nicht die neue Funktionalität der IPV6-Adressen nutzen.)
  - DEFINE\_LS, DEFINE\_PORT, QUERY\_LS, QUERY\_PORT bei Verwendung mit einer Enterprise-Extender-Verbindungsstation (HPR/IP) oder einem Enterprise-Extender-Port (HPR/IP)
  - DEFINE\_TN3270\_ACCESS, DELETE\_TN3270\_ACCESS, QUERY\_TN3270\_ACCESS
  - DEFINE\_TN3270\_EXPRESS\_LOGON, QUERY\_TN3270\_EXPRESS\_LOGON
  - DEFINE\_TN3270\_SSL\_LDAP, QUERY\_TN3270\_SSL\_LDAP
  - DEFINE\_TN\_REDIRECT, QUERY\_TN\_REDIRECT\_DEF
  - QUERY LU\_0\_TO\_3 (für einen beliebigen LU-Typ)
  - TN\_REDIRECT\_INDICATION
3. Falls Sie die neue Funktionalität der IPV6-Adressen von Version 7.1 nutzen möchten, müssen Sie sicherstellen, dass die CS/AIX-Server für die Verwendung von IPV6-Adressen konfiguriert sind. Weitere Details hierzu enthält der Abschnitt „[IPV4- und IPV6-Adressen](#)“ auf Seite 21.

## Lizenzprogramm CS/AIX installieren

---

Nachdem Sie die vorausgesetzte Software installiert haben, können Sie mit der Installation von CS/AIX beginnen. Gehen Sie dazu wie folgt vor:

1. Melden Sie sich mit Root-Berechtigung an.
2. Installieren und konfigurieren Sie die zugehörige AIX-DLC für den ausgewählten DFV-Adapter. Verwenden Sie zum Konfigurieren der DLC den Befehl `mkdev` (siehe Veröffentlichung *AIX Commands Reference*) oder die Option Kommunikation im SMIT-Menü Einheiten (siehe Veröffentlichung *AIX Communications Programming Concepts*).
3. Installieren Sie CS/AIX wie im Abschnitt „[Installationsmethoden](#)“ auf Seite 30 beschrieben. Wählen Sie die zu installierenden Features (und die zugehörigen Nachrichtendateigruppen) aus, oder wählen Sie die Option ALLE aus, um CS/AIX mit allen im Lieferumfang enthaltenen Features zu installieren.  
Wenn Sie ein Feature auswählen und das Feld *Vorausgesetzte Software installieren* auf JA setzen, wird außerdem `sna .rte` (das CS/AIX-Basisprogramm) installiert.
4. Falls Sie die Software AIX Certificate and SSL Base Runtime installiert haben, weil Sie TN Server oder TN Redirector mit dem Feature SSL verwenden möchten, müssen Sie die SSL-Software nach der Installation von CS/AIX konfigurieren. Weitere Informationen hierzu finden Sie im Abschnitt „[SSL für die Verwendung mit TN Server oder TN Redirector konfigurieren](#)“ auf Seite 35.
5. Passen Sie die Konfigurationsdaten von CS/AIX nach Bedarf an. (Hinweise hierzu finden Sie in [Kapitel 8, „CS/AIX konfigurieren und verwenden“](#), auf Seite 67 oder im *Verwaltungshandbuch für IBM Communications Server for Data Center Deployment für AIX*).
6. Starten Sie CS/AIX. Nach der Installation geschieht dies automatisch, wenn die Maschine neu gebootet wird.

```
cd /  
sna start
```

### Anmerkung:

1. Bei automatischer Installation von CS/AIX werden die SNA-Einheitentreiber auf dem lokalen Knoten rekonfiguriert.
2. Nach der Installation von CS/AIX können Sie Adapter installieren. Nach dem Hinzufügen eines Adapters müssen Sie CS/AIX nicht erneut installieren. Sie können den Adapter jedoch erst nach Installation der entsprechenden DLC verwenden.

## Installationsmethoden

Sie können das Lizenzprogramm CS/AIX mit einer der folgenden Methoden installieren:

- einfache Installation
- auf dem lokalen System
- über das Netz (falls der lokale Knoten ein Netzserver ist)

### CS/AIX mit Easy Install installieren

Es ist einfacher, ganze Softwarepakete zu installieren. Ein Softwarepaket umfasst eine Reihe von Softwareprodukten für einen bestimmten Verwendungszweck. In den folgenden Abschnitten ist die Installation von CS/AIX mit diesem Feature beschrieben. Easy Install kann an der Systemkonsole oder fern und auf einem X Window System oder von einem ASCII-Terminal aus durchgeführt werden.

Installieren Sie CS/AIX wie im Abschnitt „[„Einfache Installation mit SMIT“](#) auf Seite 30 bzw. „[„Einfache Installation mit Common Desktop Environment“](#) auf Seite 31 beschrieben auf dem lokalen Knoten.

### Einfache Installation mit SMIT

1. Melden Sie sich mit Root-Berechtigung an.

2. Geben Sie den folgenden Befehl ein:
  - smit install\_bundle
3. Drücken Sie die Taste PF4 oder klicken Sie in Motif auf die Schaltfläche Liste, um eine Liste der Installationseinheiten und -verzeichnisse für den Installationsdatenträger anzuzeigen.
4. Wählen Sie Datenträgerdefiniert aus, und drücken Sie die Eingabetaste.
5. Wählen Sie Ihre Eingabeeinheit aus, und drücken Sie die Eingabetaste.

### ***Einfache Installation mit Common Desktop Environment***

1. Öffnen Sie vom Bedienfeld auf dem Desktop aus den Anwendungsmanager.
2. Öffnen Sie den Ordner Systemverwaltung.
3. Öffnen Sie Easy Install.
4. Wählen Sie Ihre Eingabeeinheit aus.
5. Wählen Sie das datenträgerdefinierte Paket aus.
6. Klicken Sie auf die Schaltfläche Installieren/Aktualisieren.

### ***Manuelle Installation auf dem lokalen Knoten***

Installieren Sie CS/AIX wie im Abschnitt „Manuelle Installation mit SMIT“ auf Seite 31 bzw. „Manuelle Installation mit Common Desktop Environment“ auf Seite 32 beschrieben auf dem lokalen System.

#### ***Manuelle Installation mit SMIT***

1. Legen Sie den Installationsdatenträger in das entsprechende Laufwerk der AIX-Workstation ein.
2. Melden Sie sich mit Root-Berechtigung an.
3. Vergewissern Sie sich, dass die Umgebungsvariable LANG Ihres Systems nicht auf C gesetzt ist. Wenn Sie mit Nachrichten in Englisch (US) arbeiten möchten, setzen Sie die Variable LANG auf en\_US. Weitere Informationen zum Anzeigen oder Ändern der Umgebungsvariablen LANG enthält der Abschnitt „SprachumgebungsvARIABLE ändern“ auf Seite 29.
4. Geben Sie in der AIX-Befehlszeile den folgenden Befehl ein:

`smit install`

Dieser Befehl ruft SMIT mit einer menügeführten Umgebung für die Installation auf.

5. Wählen Sie in den SMIT-Installationsmenüs die folgenden Optionen aus, um eine Standardinstallation für auswählbare Software mit Aktualisierungen auszuführen:
  - a. Software installieren und aktualisieren
  - b. Auswählbare Software installieren/aktualisieren (benutzerspezifische Installation)
  - c. Gesamte verfügbare Software installieren/aktualisieren

Diese Folge von Menüoptionen ist mit dem folgenden Direktaufrufbefehl vergleichbar:

`smit install_selectable_all`

6. Wählen Sie in dem daraufhin angezeigten Dialog den Einheitennamen für den Installationsdatenträger als Quelleneinheit für das Installationsverfahren aus. (Drücken Sie auf der zeichenorientierten Schnittstelle für SMIT die Taste PF4 oder klicken Sie in Motif auf die Schnittstelle Liste, um eine Liste der Einheitennamen aufzurufen.)
7. Wählen Sie das CS/AIX-Basisprogramm sna.rte, den CS/AIX-Nachrichtenkatalog sna.msg.Sprache.rte sowie weitere Features und Updates für das Lizenzprogramm (mit den jeweils zugehörigen Dateigruppen für Nachrichten) aus. Wenn Sie alle Features vom Installationsdatenträger installieren möchten, wählen Sie die Option ALLE aus.

Das Installationsdienstprogramm zeigt nach jedem erfolgreich beendeten Installationsabschnitt Statusnachrichten an.

## Lizenzprogramm CS/AIX installieren

8. Wenn Sie die Software AIX Certificate and SSL Base Runtime installieren möchten, um TN Server oder TN Redirector mit dem SSL-Feature verwenden zu können, wählen Sie außerdem die Dateigruppe für AIX Certificate and SSL Base Runtime aus.

Das Installationsdienstprogramm zeigt nach jedem erfolgreich beendeten Installationsabschnitt Statusnachrichten an.

Wenn Sie diese Software installiert haben, müssen Sie die SSL-Software nach der Installation von CS/AIX konfigurieren. Weitere Informationen hierzu finden Sie im Abschnitt „[SSL für die Verwendung mit TN Server oder TN Redirector konfigurieren](#)“ auf Seite 35.

9. Passen Sie die Konfigurationsdaten von CS/AIX an. (Hinweise hierzu finden Sie in Kapitel 8, „[CS/AIX konfigurieren und verwenden](#)“, auf Seite 67 oder im *Verwaltungshandbuch für IBM Communications Server for Data Center Deployment für AIX*).

### Anmerkung:

1. Bei automatischer Installation von CS/AIX werden die SNA-Einheitentreiber auf dem lokalen Knoten rekonfiguriert.
2. Informationen zu Benutzerlizenzen für CS/AIX finden Sie im Abschnitt „[Mechanismen der Lizenzierung für CS/AIX](#)“ auf Seite 25.

## Manuelle Installation mit Common Desktop Environment

1. Legen Sie den Installationsdatenträger in das entsprechende Laufwerk der AIX-Workstation ein.
2. Melden Sie sich mit Root-Berechtigung an.
3. Vergewissern Sie sich, dass die Umgebungsvariable LANG Ihres Systems nicht auf C gesetzt ist. Wenn Sie mit Nachrichten in Englisch (US) arbeiten möchten, setzen Sie die Variable LANG auf en\_US. Weitere Informationen zum Anzeigen oder Ändern der Umgebungsvariablen LANG enthält der Abschnitt „[Sprachumgebungsvariable ändern](#)“ auf Seite 29.
4. Öffnen Sie vom Bedienfeld auf dem Desktop aus den Anwendungsmanager.
5. Öffnen Sie den Ordner Systemverwaltung.
6. Öffnen Sie den Ordner Installationsmanager.
7. Wählen Sie Ihre Eingabeeinheit aus.
8. Wählen Sie alle angezeigten Objekte aus, um den gesamten Inhalt des Datenträgers zu installieren. Sie können aber auch die Anzeige erweitern und einzelne Objekte auswählen, um die Installationsoptionen für Communications Server für AIX anzupassen.
9. Klicken Sie auf das Symbol Installieren, um mit der Installation zu beginnen.
10. Passen Sie die Konfigurationsdaten von CS/AIX an. (Hinweise hierzu finden Sie in Kapitel 8, „[CS/AIX konfigurieren und verwenden](#)“, auf Seite 67 oder im *Verwaltungshandbuch für IBM Communications Server for Data Center Deployment für AIX*).

### Anmerkung:

1. Bei automatischer Installation von CS/AIX werden die SNA-Einheitentreiber auf dem lokalen Knoten rekonfiguriert.
2. Informationen zu Benutzerlizenzen für CS/AIX finden Sie im Abschnitt „[Mechanismen der Lizenzierung für CS/AIX](#)“ auf Seite 25.

## Installation über ein Netz mit Network Installation Management

Gehen Sie wie folgt vor, um CS/AIX über ein Netz zu installieren:

1. In der Veröffentlichung *AIX Version 7.2 Installation Guide and Reference* finden Sie Informationen zum Konfigurieren des NIM-Servers und zum Laden von Dateien auf den Client.
2. Vergewissern Sie sich, dass die Umgebungsvariable LANG Ihres Systems nicht auf C gesetzt ist. Wenn Sie mit Nachrichten in Englisch (US) arbeiten möchten, setzen Sie die Variable LANG auf en\_US. Weitere

re Informationen zum Anzeigen oder Ändern der Umgebungsvariablen LANG enthält der Abschnitt „Sprachumgebungsvariable ändern“ auf Seite 29.

3. Geben Sie in der AIX-Befehlszeile den folgenden Befehl ein:

```
smit nim
```

Dieser Befehl ruft SMIT mit einer menügeführten Umgebung für die Installation auf.

4. Befolgen Sie die angezeigten Anweisungen und geben Sie in den SMIT-Installationsmenüs die angeforderten Informationen für die Ausführung einer Netzinstallation ein. Wählen Sie die Dateien aus, die `sna.rte` enthalten, sowie weitere Features und Updates für das Lizenzprogramm. Das Installationsdienstprogramm zeigt nach jedem erfolgreich beendeten Installationsabschnitt Statusnachrichten an.

**Anmerkung:**

1. Der CS/AIX-Nachrichtenkatalog `sna.msg.Sprache.rte` wird automatisch zusammen mit CS/AIX installiert, wenn die Option *Zugehörige sprachenspezifische Dateigruppen einbeziehen?* auf die Standardeinstellung JA gesetzt ist.
2. Bei automatischer Installation von CS/AIX werden die SNA-Einheitentreiber auf dem lokalen Knoten rekonfiguriert.
3. Informationen zu Benutzerlizenzen für CS/AIX finden Sie im Abschnitt „[Mechanismen der Lizenzierung für CS/AIX](#)“ auf Seite 25.

## WebSphere Application Server konfigurieren

Wenn Sie mit einem Client-Server-System arbeiten, in dem Remote API Clients über HTTPS eine Verbindung zu CS/AIX-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 17.

In den folgenden Abschnitten ist beschrieben, mit welchen Schritten Sie WebSphere für die Verwendung mit CS/AIX konfigurieren müssen:

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

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

## 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 Clientauthentifizierung durchgesetzt wird. Informieren Sie sich hierüber in der Dokumentation zu WebSphere Application Server. Wenn die Clientauthentifizierung 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 Clientzertifikats verifiziert werden kann.

## WebSphere Application Server konfigurieren

Führen Sie die folgenden Schritte aus, um WebSphere Application Server für die gemeinsame Verwendung mit CS/AIX 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 die Schaltfläche '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 Controllerkonfiguration 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 Kontrollkästchen. 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 CS/AIX benötigt WebSphere Application Server eine Liste der CS/AIX-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 33 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/AIX-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 CS/AIX erforderlich sein können.

## **Client-Server-Betrieb**

CS/AIX wird nach der Installation als eigenständiger Server (mit allen Komponenten auf einem AIX-System) ausgeführt. Falls Sie CS/AIX als Server in einer Client-Server-Domäne ausführen möchten, lesen Sie die diesbezüglichen Anweisungen im Kapitel 'Client-Server-System mit CS/AIX verwalten' im *Verwaltungshandbuch für IBM Communications Server for Data Center Deployment für AIX*.

## **PDF-Handbücher anzeigen**

Die auf dem Installationsdatenträger für dieses Produkt enthaltenen Handbücher liegen im Portable Document Format (PDF) vor. Das Softcopyformat 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 `/usr/share/man/info/Sprache/sna` installiert. Die HTML-Datei SNABOOKS.HTM in diesem Verzeichnis enthält einen Hypertext-Link zu jedem Handbuch. Die Handbücher sind außerdem im Verzeichnis `/DOCS` des Installationsdatenträgers mit CS/AIX enthalten.

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

## **Aktuelle Releaseinformationen**

Der neueste Stand der README-Informationsdatei zum Produkt befindet sich im Verzeichnis `/usr/lpp/sna/` und enthält Informationen zu allen Produktänderungen, die nach Veröffentlichung der Bibliothek zu CS/AIX vorgenommen wurden. Immer, wenn Sie Produktupdates erhalten, sollten Sie nach zugehörigen Informationen in der README-Datei suchen.

Mit SMIT können Sie wie folgt auf die README-Datei zugreifen:

1. Rufen Sie nach der Installation von CS/AIX Version 7.1 das SMIT-Hauptmenü für CS/AIX auf. Geben Sie dazu in der Befehlszeile den folgenden Befehl ein:

```
smit sna
```

Daraufhin wird das SMIT-Hauptmenü für CS/AIX angezeigt.

2. Wählen Sie in diesem Menü Produktinformationen aus. SMIT zeigt daraufhin den Dialog 'Produktinformationen' an.
3. Wählen Sie eine der Optionen in diesem Dialog aus, um die zugehörige README-Datei aufzurufen.

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

Falls Sie die Software AIX Certificate and SSL Base Runtime installiert haben, weil Sie TN Server oder TN Redirector mit dem Feature SSL verwenden möchten, müssen Sie die SSL-Software nach der Installation von CS/AIX 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 bilden zusammen einen Datensatz in einer Schlüsselringdatenbank, die auf dem CS/AIX-Server mit TN Server oder TN Redirector gespeichert wird. CS/AIX verwendet die Datenbank für die Implementierung von SSL.

Geben Sie zum Verwalten der Schlüsselringdatenbank an der AIX-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 `sna-keyman` beenden und den CS/AIX-Knoten stoppen. Starten Sie dann den CS/AIX-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
```

## Webserver für das Webverwaltungsprogramm konfigurieren

Wenn Sie das Webverwaltungsprogramm mit einem Webserver verwenden, der nicht im Abschnitt „Installationsvoraussetzungen“ auf Seite 17 aufgelistet ist, oder den Webserver nach CS/AIX installieren, müssen Sie Verknüpfungen zwischen CS/AIX-Verzeichnissen und den Verzeichnissen des Webservers konfigurieren, damit der Webserver die erforderlichen Dateien findet. Erstellen Sie diese Verknüpfungen mit dem Befehl `ln`.

- Das Verzeichnis 'servlets' des Webservers muss mit `/usr/lib/sna/WebAdmin/Server` verknüpft werden.
- Das Unterverzeichnis SnaAdmin des Webserververzeichnisses für öffentliche HTML muss mit `/usr/lib/sna/WebAdmin/Client` verknüpft werden.

Weitere Informationen zum Konfigurieren des Webservers können Sie der Textdatei `/usr/lpp/sna.wa/README` entnehmen, die zusammen mit dem CS/AIX-Webverwaltungspaket installiert wird.

## CS/AIX-Konfigurationsdateien sichern

CS/AIX erstellt automatisch Sicherungskopien der Knoten-, Domänen- und TN3270-Einheitendaten (`tn3270dev.dat`) sowie der TP-Konfigurationsdatei, wenn Sie (mit einem der CS/AIX-Verwaltungstools) Änderungen vornehmen, die sich auf diese Dateien auswirken. Wenn Sie beispielsweise eine Änderung vornehmen, die Einfluss auf die Knotenkonfigurationsdatei (`sna_node.cfg`) hat, erstellt CS/AIX eine Sicherungsdatei mit dem Namen `sna_node.bkn`, wobei *n* entweder die Zahl 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 AIX
- vor Installation einer neuen Version von CS/AIX
- nach Erstellung einer neuen Konfiguration

Führen Sie zum Sichern von Konfigurationsdateien die folgenden Befehle aus:

```
cd /etc/sna
/bin/ls -1 sna*cfg sna.net sna_tps ibmcs.* | backup -i -v -q -f Einheitenname
```

Hier steht *Einheitenname* für den Pfad- und Dateinamen einer Einheit, die die Daten aus den zu sichern Dateien empfangen soll. Es ist am günstigsten, Dateien auf externen Datenträgern wie Disketten oder Bändern zu sichern.

## Sicherungskopie der CS/AIX-Konfigurationsdateien zurückzuschreiben

Gehen Sie wie folgt vor, um die Konfigurationsdateien von CS/AIX, die Sie wie im Abschnitt „[CS/AIX-Konfigurationsdateien sichern](#)“ auf Seite 36 beschrieben gesichert haben, zurückzuschreiben:

1. Vergewissern Sie sich, dass CS/AIX nicht aktiv ist. Dies können Sie durch Eingabe des folgenden Befehls überprüfen:

```
snaadmin status_node
```

Wenn CS/AIX aktiv ist, zeigt der Befehl Informationen zum Status des lokalen Knotens an. Andernfalls wird die Nachricht angezeigt, dass CS/AIX nicht aktiv ist.

Sollte CS/AIX aktiv sein, geben Sie zum Inaktivieren den folgenden Befehl ein:

```
sna stop
```

2. Geben Sie den folgenden Befehl ein:

```
cd /etc/sna
restore -x -f 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/sna.

## Konfigurationsdateien reinitialisieren

Werden Konfigurationsdateien von CS/AIX 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 CS/AIX wieder so konfigurieren, als wäre das Produkt 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/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 CS/AIX 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 CS/AIX gelieferte leere Domänenkonfigurationsdatei kopiert):

```
cp -p /usr/lib/sna/samples/empty.cfg /etc/sna/sna_domn.cfg
```

Dieser Befehl erstellt eine neue Domänenkonfigurationsdatei, die für den Start von CS/AIX erforderlich ist.

5. Wenn Sie die SSL-Schlüsselringdatenbankdatei gelöscht haben, geben Sie zum erneuten Erstellen dieser Datei den folgenden Befehl ein (der die zu CS/AIX gelieferte Beispieldatei kopiert):

```
cp -p /usr/lib/sna/samples/ibmcs.* /etc/sna
```

6. Geben Sie den folgenden Befehl ein, um CS/AIX 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, „CS/AIX konfigurieren und verwenden“](#), auf [Seite 67](#) oder im [Verwaltungshandbuch für IBM Communications Server for Data Center Deployment für AIX](#).

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

# Kapitel 4. IBM Remote API Clients unter Linux installieren

Dieses Kapitel beschäftigt sich mit der Installation von IBM Remote API Client für 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/AIX-Servern (oder CS-Linux-Servern, jedoch nicht zu beiden gleichzeitig) herstellen. (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 AMD64- bzw. Intel-EM64T-Computern (x86\_64, 64-Bit) und Power-Systems-Computern (ppc64le) ausgeführt werden. Falls Sie IBM Remote API Client auf einem System z (s390x) installieren möchten, lesen Sie [Kapitel 5, „IBM Remote API Clients für Linux auf System z installieren“, auf Seite 45.](#)

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 Clienttyp:

Clienttyp	Verzeichnis auf der CD
AMD64 / Intel EM64T x86_64 (64 Bit)	/ibm-commserver-clients/linux-x86_64
Power (ppc64le)	/ibm-commserver-clients/linux-ppc64le

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

Falls Sie ein Upgrade für eine frühere Version von CS/AIX und der Remote API Clients durchführen, sollten Sie das Upgrade für alle Server vor dem Upgrade der Remote API Clients durchführen. Weitere Details hierzu enthält der Abschnitt „[Vorversionen von CS/AIX migrieren](#)“ auf Seite 29.

## 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 Clienttyp die entsprechende Hardware und die Antwort von `uname -m` für diese Hardware angegeben.

Clienttyp	Hardware	uname-Antwort
AMD64 / Intel EM64T (64-Bit)	x86_64 (System mit AMD64 oder Intel EM64T)	x86_64
pSeries	Power System	ppc64le

### 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 7 und 8
- SUSE Linux Enterprise Server 12 und 15
- Ubuntu Linux LTS 18.04 und 20.04

## Hardware- und Softwarevoraussetzungen

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/AIX-Server zugreifen soll, benötigen Sie GSKit-Software, um den HTTPS-Zugriff auf die Server über einen WebSphere-Server zu aktivieren. Weitere Informationen zur Beschaffung und Installation der GSKit-Software enthält die README-Datei auf dem Installationsdatenträger.

## Details der Produktinstallation anzeigen

Sie können Informationen zum Remote API Client und zu den bereits installierten zugehörigen Softwarepaketen anzeigen. Verwenden Sie den folgenden Befehl, um alle auf RHEL- und SLES-Systemen 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*.

Für Ubuntu lauten die entsprechenden Befehle *dpkg -l* und *dpkg -l Paketname*.

## Umgebungsvariablen für CS/AIX definieren

Der Betrieb von CS/AIX wird mit einer Reihe von Umgebungsvariablen gesteuert, die Sie vor der Aktivierung der Software CS/AIX auf dem Client festlegen müssen. Am einfachsten ist es, die Variablen in einer Textdatei festzulegen, die CS/AIX beim Start liest.

Erstellen Sie eine Textdatei mit dem Namen *environment* im Konfigurationsverzeichnis */etc/opt/ibm/sna* von CS/AIX und legen Sie in jeder Zeile eine Umgebungsvariable fest. Beispiel:

```
export LANG=en_US
export PATH='$PATH:/usr/bin'
export LD_LIBRARY_PATH=/usr/lib:/usr/lib/sna
export LD_RUN_PATH=/usr/lib:/usr/lib/sna
```

## 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
en_US	Englisch (Vereinigte Staaten)
ja_JP	Japanisch (PC)
de_DE	Deutsch

Kennung	Sprache
es_ES	Spanisch
fr_FR	Französisch
ko_KR	Koreanisch
pt_BR	Portugiesisch
zh_CN	Chinesisch (vereinfacht, EUC)
zh_TW	Chinesisch (traditionell)

## Remote API Client für 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 für Linux deinstallieren](#)“ auf Seite 43 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
```

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-x86\_64 für einen 64-Bit-Intel-Client (x86\_64). Ersetzen Sie das Verzeichnis ggf. durch /linux-ppc64le.

```
cd ibm-commserver-clients/linux-x86_64
./installibmccli
```

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 rpm/deb-Pakete.

4. Erstellen Sie die Clientnetzdatendatei, um die CS/AIX-Server anzugeben, zu denen der Client eine Verbindung herstellen darf. Wenn Sie die erweiterte Unterstützung für die Verfolgung von LUs und die Zuordnung von Aliasnamen der lokalen LU aktivieren möchten, sind weitere Konfigurationsschritte erforderlich. Mit dieser Unterstützung können Clients dynamischer integriert und LU-Ressourcen in einer Serverdomäne verwaltet werden. Weitere Details hierzu können Sie im *Verwaltungshandbuch für IBM Communications Server for Data Center Deployment für AIX* im Abschnitt 'Remote API Clients verwalten' nachlesen.
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
```

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
```

**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 42.

Außerdem müssen Sie die Clientnetzdatendatei aktualisieren und den WebSphere-Server angeben, der die HTTPS-Unterstützung bereitstellt. Weitere Details hierzu können Sie im *Verwaltungshandbuch für IBM Communications Server for Data Center Deployment für AIX* im Abschnitt 'Remote API Clients verwalten' nachlesen.

## HTTPS-Sicherheitszertifikate mit dem GSKit konfigurieren

Wenn der Client mit HTTPS auf CS/AIX-Server zugreifen soll, muss das GSKit-Schlüsselverwaltungsprogramm auf dem Client installiert sein. Weitere Informationen zur Beschaffung und Installation der GSKit-Software enthält die README-Datei auf dem Installationsdatenträger.

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 Clientsicherheitszertifikaten 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 Clientzertifikat erstellen. Ein solches Zertifikat bietet jedoch nicht das erforder-

liche 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-Schlüsselverwaltungsprogramm.

## **Remote API Client für Linux deinstallieren**

---

Sie können Remote API Client für Linux mit den folgenden Befehlen deinstallieren (verwenden Sie unter Ubuntu Linux `dpkg -r`):

```
/usr/bin/sna stop  
rpm -e ibm-commserver-cli  
/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 für Linux auf System z installieren

In diesem Kapitel ist die Installation von IBM Remote API Client für Linux auf System z beschrieben. 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/AIX-Servern (oder CS-Linux-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/linux-systemz`.

Falls Sie ein Upgrade für eine frühere Version von CS/AIX und der Remote API Clients durchführen, sollten Sie das Upgrade für alle Server vor dem Upgrade der Remote API Clients durchführen. Weitere Details hierzu enthält der Abschnitt „[Vorversionen von CS/AIX migrieren](#)“ auf Seite 29.

## Hardware- und Softwarevoraussetzungen

### Hardwarevoraussetzungen

IBM Remote API Client erfordert ein System vom Typ System z (64-Bit), das von einer der im Abschnitt „[Version des Betriebssystems Linux](#)“ auf Seite 45 aufgelisteten Linux-Distributionen unterstützt wird.

Überprüfen Sie mit dem Befehl `uname -m` die CPU-Klasse. Der Befehl muss `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 7 und 8
- SUSE Linux Enterprise Server 12 und 15
- Ubuntu Linux LTS 18.04 und 20.04

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/AIX-Server zugreifen soll, benötigen Sie GSKit-Software, um den HTTPS-Zugriff auf die Server über einen WebSphere-Server zu aktivieren. Weitere Informationen zur Beschaffung und Installation der GSKit-Software enthält die README-Datei auf dem Installationsdatenträger.

### Details der Produktinstallation anzeigen

Sie können Informationen zum Remote API Client und zu den bereits installierten zugehörigen Softwarepaketen anzeigen. Verwenden Sie den folgenden Befehl, um alle unter RHEL oder SLES 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`.

Für Ubuntu lauten die entsprechenden Befehle `dpkg -l` und `dpkg -l Paketname`.

## Umgebungsvariablen für CS/AIX definieren

Der Betrieb von CS/AIX wird mit einer Reihe von Umgebungsvariablen gesteuert, die Sie vor der Aktivierung der Software CS/AIX auf dem Client festlegen müssen. Am einfachsten ist es, die Variablen in einer Textdatei festzulegen, die CS/AIX beim Start liest.

Erstellen Sie eine Textdatei mit dem Namen `environment` im Konfigurationsverzeichnis `/etc/opt/ibm/sna` von CS/AIX und legen Sie in jeder Zeile eine Umgebungsvariable fest. Beispiel:

```
export LANG=en_US
export PATH='$PATH:/usr/bin'
export LD_LIBRARY_PATH=/usr/lib:/usr/lib/sna
export LD_RUN_PATH=/usr/lib:/usr/lib/sna
```

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

## Remote API Client für Linux auf 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 für Linux auf System z deinstallieren](#)“ auf Seite 49 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-7.1.0.0-s390x.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-7.1.0.0-s390x.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 CS/AIX 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 das `rpm/deb`-Paket.

5. Erstellen Sie die Clientnetzdatendatei, um die CS/AIX-Server anzugeben, zu denen der Client eine Verbindung herstellen darf. Wenn Sie die erweiterte Unterstützung für die Verfolgung von LUs und die Zuordnung von Aliasnamen der lokalen LU aktivieren möchten, sind weitere Konfigurationsschritte erforderlich. Mit dieser Unterstützung können Clients dynamischer integriert und LU-Ressourcen in einer Serverdomäne verwaltet werden. Weitere Details hierzu können Sie im *Verwaltungshandbuch für IBM Communications Server for Data Center Deployment für AIX* im Abschnitt 'Remote API Clients verwalten' nachlesen.

6. 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
```

7. 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
```

8. Nach Abschluss der Installation können Sie die während der Installation erstellte `tgz`-Datei 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 48.

Außerdem müssen Sie die Clientnetzdatendatei aktualisieren und den WebSphere-Server angeben, der die HTTPS-Unterstützung bereitstellt. Weitere Details hierzu können Sie im *Verwaltungshandbuch für IBM Communications Server for Data Center Deployment für AIX* im Abschnitt 'Remote API Clients verwalten' nachlesen.

## HTTPS-Sicherheitszertifikate mit dem GSKit konfigurieren

---

Wenn der Client mit HTTPS auf CS/AIX-Server zugreifen soll, muss das GSKit-Schlüsselverwaltungsprogramm auf dem Client installiert sein. Weitere Informationen zur Beschaffung und Installation der GSKit-Software enthält die README-Datei auf dem Installationsdatenträger.

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 Clientsicherheitszertifikaten 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 Clientzertifikat 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-Schlüsselverwaltungsprogramm.

## Remote API Client für Linux auf System z deinstallieren

---

Sie können Remote API Client für Linux auf System z mit den folgenden Befehlen deinstallieren (verwenden Sie unter Ubuntu Linux `dpkg -r`):

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

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 unter AIX installieren

Dieses Kapitel beschäftigt sich mit der Installation von IBM Remote API Client für 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/AIX-Servern (oder CS-Linux-Servern) herstellen.

Lesen Sie vor der Installation der Software die README-Datei zu IBM Remote API Client. Diese Datei ist im Verzeichnis `/ibm-commserver-clients/aix` auf der Installations-CD enthalten. Falls Sie ein Upgrade für eine ältere Version von CS/AIX und der Remote API Clients durchführen, sollten Sie das Upgrade für alle Server vor dem Upgrade der Remote API Clients durchführen. Weitere Details hierzu enthält der Abschnitt „[Vorversionen von CS/AIX migrieren](#)“ auf Seite 29.

## Hardware- und Softwarevoraussetzungen

### Hardwarevoraussetzungen

IBM Remote API Client erfordert ein Power System, das von einer der im Abschnitt „[Betriebssystemversion](#)“ auf Seite 51 aufgelisteten Versionen des Betriebssystems AIX unterstützt wird.

### Betriebssystemversion

Die aktuelle Version von IBM Remote API Client wurde mit folgenden Versionen des Betriebssystems getestet.

- AIX ab Version 7.2

Der Client kann in der globalen Umgebung oder auf System- bzw. Anwendungs-WPAR ausgeführt werden. Sie müssen sicherstellen, dass jede WPAR, auf der der Client ausgeführt wird, einen eindeutigen Hostnamen hat, der vom DNS aufgelöst werden kann.

### Java

Falls Sie die Java-API CPI-C verwenden, benötigen Sie Java-Software. Das neueste, unter <http://www.ibm.com/developerworks/java/jdk> verfügbare Java SDK erfüllt alle Voraussetzungen.

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

### GSKit

Wenn der Client mit HTTPS auf CS/AIX-Server zugreifen soll, benötigen Sie GSKit-Software, um den HTTPS-Zugriff auf die Server über einen WebSphere-Server zu aktivieren. Weitere Informationen zur Beschaffung und Installation der GSKit-Software enthält die README-Datei auf dem Installationsdatenträger.

### Umgebungsvariablen für CS/AIX definieren

Der Betrieb von CS/AIX wird mit einer Reihe von Umgebungsvariablen gesteuert, die Sie vor der Aktivierung der Software CS/AIX auf dem Client festlegen müssen. Am einfachsten ist es, die Variablen in einer Textdatei festzulegen, die CS/AIX beim Start liest.

Erstellen Sie eine Textdatei mit dem Namen `environment` im Konfigurationsverzeichnis `/etc/sna` von CS/AIX und legen Sie in jeder Zeile eine Umgebungsvariable fest. Beispiel:

```
export LANG=en_US
export PATH='$PATH:/usr/bin'
export LD_LIBRARY_PATH=/usr/lib:/usr/lib/sna
export LD_RUN_PATH=/usr/lib:/usr/lib/sna
```

## 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 für 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 für AIX deinstallieren](#)“ auf Seite 54 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.7.1.0.0.I 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.
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 README-Datei im Verzeichnis /ibm-commserver-clients/aix der Installations-CD.
4. Nach Abschluss der Installation können Sie die Datei sna.client.7.1.0.0.I aus dem Arbeitsverzeichnis löschen.
5. Erstellen Sie die Clientnetzdatendatei, um die CS/AIX-Server anzugeben, zu denen der Client eine Verbindung herstellen darf. Wenn Sie die erweiterte Unterstützung für die Verfolgung von LUs und die Zuordnung von Aliasnamen der lokalen LU aktivieren möchten, sind weitere Konfigurationsschritte erforderlich. Mit dieser Unterstützung können Clients dynamischer integriert und LU-Ressourcen in einer Serverdomäne verwaltet werden. Weitere Details hierzu können Sie im *Verwaltungshandbuch für IBM Communications Server for Data Center Deployment für AIX* im Abschnitt 'Remote API Clients verwalten' nachlesen.
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 53.

Außerdem müssen Sie die Clientnetzdatendatei aktualisieren und die CS/AIX-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 *Verwaltungshandbuch für IBM Communications Server for Data Center Deployment für AIX* 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 README-Datei im Verzeichnis /ibm-commserver-clients/aix der Installations-CD.

4. Hängen Sie die CD nach Abschluss des Installationsprozesses mit dem folgenden Befehl ab.

```
umount /mnt
```

5. Erstellen Sie die Clientnetzdatendatei, um die CS/AIX-Server anzugeben, zu denen der Client eine Verbindung herstellen darf. Weitere Details hierzu können Sie im *Verwaltungshandbuch für IBM Communications Server for Data Center Deployment für AIX* im Abschnitt 'Remote API Clients verwalten' nachlesen.

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](#)“ auf Seite 53.

Außerdem müssen Sie die Clientnetzdatendatei aktualisieren und die CS/AIX-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 *Verwaltungshandbuch für IBM Communications Server for Data Center Deployment für AIX* 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 si-

cherzustellen, 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 Clientsicherheitszertifikaten 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 Clientzertifikat 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-Schlüsselverwaltungsprogramm.

## Remote API Client für AIX deinstallieren

---

Sie können Remote API Client mit den folgenden Befehlen deinstallieren.

1. Falls die Clientsoftware 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 für Windows planen und ausführen

Dieses Kapitel beschäftigt sich mit der Installation von IBM Remote API Client für 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/AIX-Servern (oder CS-Linux-Servern) herstellen.

Falls Sie ein Upgrade für eine frühere Version von CS/AIX und der Remote API Clients durchführen, sollten Sie das Upgrade für alle Server vor dem Upgrade der Remote API Clients durchführen. Weitere Details hierzu enthält der Abschnitt „Vorversionen von CS/AIX migrieren“ auf Seite 29.

Der mit CS/AIX Version 7.1 ausgelieferte Client unterstützt nur 64-Bit-Windows-Betriebssysteme. Ältere CS/AIX-Clients können weiterhin unter 32-Bit-Windows-Betriebssystemen mit CS/AIX Version 7.1 verwendet werden.

Die vom IBM Remote API Client für Windows bereitgestellten Schnittstellen sind weitestgehend mit den von IBM Personal Communications und Microsoft Host Integration Server (der Windows Open Server Architektur) 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 für Windows muss der Computer die folgenden Voraussetzungen erfüllen:

- Der Computer muss eines der folgenden Betriebssysteme ausführen. Die neuesten Informationen zu den spezifischen Versionsnummern, die für jede Betriebssystemversion unterstützt werden, sowie zu weiteren Voraussetzungen für bestimmte Versionen finden Sie in der README-Datei auf der Installations-CD im Abschnitt zum Windows-Client.
  - Microsoft Windows 10 (64-Bit)
  - Microsoft Windows Server 2012
  - Microsoft Windows Server 2016
  - Microsoft Windows Server 2019

Der Computer muss mit einem der folgenden Mechanismen auf CS/AIX-Server zugreifen können:

- Serverzugriff über ein TCP/IP-Netz
- Zugriff auf einen WebSphere-Server, der den HTTPS-Zugriff auf CS/AIX-Server ermöglicht

**Anmerkung:** Je nach verwendeter Windows-Version und den verwendeten, speziellen Features des Remote API Client, müssen Sie unter Umständen zusätzliche Konfigurationsschritte ausführen, bevor Sie den Remote API Client unter Windows installieren und verwenden können. Weitere Details hierzu enthalten die Informationen zum Windows-Client in der README-Datei auf der Installations-CD. Wenn der Client mit HTTPS auf Server zugreifen soll, muss die Software GSKit installiert werden.

## Zugriff auf das Setup-Programm

Remote API Client, die SDK-Software und das Setup-Programm sind im Windows-Format auf der Installations-CD enthalten. Sie können die Software demzufolge direkt von der CD auf dem Windows-Computer

installieren. Sie müssen die Software Remote API Client 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.

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

- Es ist 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/AIX-CD installieren. Wenn Sie diese ausführbare Datei ausführen, wird das Installations-Image entpackt und automatisch das Setup-Programm ausgeführt. Falls Sie das Installations-Image 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 Programm-symbol verwenden.)

Nachdem Sie das Installations-Image 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 56](#)“ 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 über die Befehlszeile installieren“ auf Seite 59](#)“ beschrieben vor. Bei dieser Methode haben Sie keine Möglichkeit, das SDK zu installieren.

**Anmerkung:** IBM Remote API Client kann erst mit HTTPS Verbindungen zu Servern herstellen, nachdem Sie die Clientnetzdatendatei aktualisiert haben. Die Datei muss die CS/AIX-Server angeben, zu denen der Client eine Verbindung herstellen kann, sowie den Namen des WebSphere-Servers, der die HTTPS-Unterstützung bereitstellt. Weitere Details hierzu können Sie im *Verwaltungshandbuch für IBM Communications Server for Data Center Deployment für AIX* im Abschnitt 'Remote API Clients verwalten' nachlesen.

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

Sie können das Programm `setup` automatisch ausführen, indem Sie die selbst entpackende komprimierte Datei `i_w64cli.exe` ausführen, oder manuell über die 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 Softwarelizenzzvereinbarung 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 für 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 deinstallieren](#)“ auf Seite 64.)
- Brechen Sie die Installation der Clientsoftware 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 *Verwaltungshandbuch für IBM Communications Server for Data Center Deployment für AIX*. Falls Sie diese Standardwerte nicht verwenden möchten, können Sie sie wie nachfolgend beschrieben konfigurieren:

### Domäne

Geben Sie den Namen der CS/AIX-Client-Server-Domäne an.

Falls der Client IPV6-Adressen verwendet, müssen Sie die folgenden Einstellungen konfigurieren. Die Einstellungen sind optional, wenn der Client IPV4-Adressen verwendet.

### 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.

Geben Sie jeden Servernamen in einem der folgenden Formate an:

- Falls der Client für den Serverzugriff HTTPS verwendet, geben Sie den Namen des WebSphere-Servers, der die HTTPS-Unterstützung bereitstellt, und den Namen des CS/AIX-Servers im folgenden Format an:

*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.

- Falls der Client für den Serverzugriff kein HTTPS verwendet, geben Sie den Namen des Servers an, mit dem als Erstes eine Verbindung hergestellt werden soll. Die Parameter *Webservername* und *Port-Nummer* werden nicht verwendet und sollten nicht angegeben werden.
- Wenn Client und Server im selben privaten Netz sind, können Sie angeben, dass der Client einen Server mit CS/AIX suchen soll, indem er eine UDP-Broadcastnachricht an alle Computer in seinem TCP/IP-Teilnetz (bzw. in Teilnetze, auf die der Client zugreifen kann, wenn der Clientcomputer über mehr als eine LAN-Adapterkarte verfügt) sendet. Dazu geben Sie als ersten Servernamen einen Stern (\*) ein.

Diese Option ist nur verfügbar, wenn der Client IPV4-Adressen verwendet. UDP-Broadcasts werden für IPV6 nicht unterstützt.

Der Client wiederholt den Broadcast-Versuch alle 10 Sekunden, bis die vom Parameter *broadcast\_attempt\_count* angegebene Anzahl von Versuchen erreicht ist oder der Kontakt zu einem Server hergestellt wurde. Wird die von *broadcast\_attempt\_count* angegebene Begrenzung erreicht, bevor der Kontakt zu einem Server hergestellt werden kann, versucht der Client, direkte Nachrichten an benannte Server (die von den folgenden Zeilen der Datei angegeben werden) zu senden.

**Anmerkung:** Wenn Sie keine UDP-Broadcasts verwenden, müssen Sie die Namen aller Server angeben, zu denen der Client eine Verbindung herstellen soll. Der Client kann Ressourcen auf den in dieser Datei angegebenen Servern verwenden, jedoch keine Ressourcen auf anderen Servern.

Die folgenden Einstellungen sind optional:

### Erweitert

Sie können anstelle der vom Setup-Programm vorgegebenen Standardwerte zusätzliche Werte angeben. Klicken Sie dazu unten im Fenster auf die Schaltfläche 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 59.

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-Datei

### **Client starten**

Ausführung des CS/AIX-Clients 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 Clientverbindung 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 der Client UDP-Broadcasts verwendet. Dies wird mit dem Zeichen \* (Stern) anstelle des ersten Servernamens angezeigt.

### **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 59 zurück. Klicken Sie andernfalls im Konfigurationsdialog auf die Schaltfläche OK, um die Konfiguration abzuschließen.

## Remote API Client über die 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 56 erläutert. Sie können das SDK nicht von der Befehlszeile aus installieren.

Nachdem Sie das Installationsimage für den Remote API Client in einem temporären Verzeichnis entpackt haben, müssen Sie die Software Remote API Client 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 auszuführen, in dem die Bedingungen der Softwarelizenzzvereinbarung akzeptiert werden.

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

### **-accept -s**

Führt die Installation im Hintergrundmodus aus. Die Bedingungen der Softwarelizenzzvereinbarung werden akzeptiert. Sie finden diese Vereinbarung im Unterverzeichnis `license` des Windows-Installationsimage.

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.)

### **-kOrdner**

Geben Sie den Programmordner an.

### **-1Sprachencode**

Geben Sie die Sprache des Clients an, die Sie verwenden möchten. Wenn Sie keine Sprache angeben, wird standardmäßig Englisch installiert.

Verwenden Sie die folgenden Codes (mit dem vorangestellten `0x`) für die Sprachauswahl. Geben Sie beispielsweise `-10x000c` an, um den Client auf Französisch zu verwenden.

- Englisch (Standard): `0x0009`
- Chinesisch: `0x0804`
- Französisch: `0x000c`
- Deutsch: `0x0007`
- Japanisch: `0x0011`
- Koreanisch: `0x0012`
- Portugiesisch: `0x0016`
- Spanisch: `0x000a`
- Taiwanesisch: `0x0404`

### **-pVerzeichnis**

Geben Sie das Installationsverzeichnis an.

### **-iDomäne**

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

### **-wVerzeichnis**

Geben Sie das Quellenverzeichnis mit den Dateien der CS/AIX-Clientsoftware an, sofern sich die Quelle auf einer Platte oder CD befindet. Verwenden Sie andernfalls die Option `-v`.

**-vServer**

Geben Sie den Server an, von dem die Clientsoftwaredateien 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.

**-uServer**

Geben Sie im folgenden Format den Namen eines Servers an, der in die Liste der Server aufgenommen werden soll, auf die dieser Client zugreifen kann:

- Falls der Client für den Serverzugriff HTTPS verwendet, geben Sie den Namen des WebSphere-Servers, der die HTTPS-Unterstützung bereitstellt, und den Namen des CS/AIX-Servers im folgenden Format an:

*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.

- Falls der Client für den Serverzugriff kein HTTPS verwendet, geben Sie den Namen des Servers an, mit dem als Erstes eine Verbindung hergestellt werden soll.
- Wenn Client und Server im selben privaten Netz sind, können Sie angeben, dass der Client einen Server mit CS/AIX suchen soll, indem er eine UDP-Broadcastnachricht an alle Computer in seinem TCP/IP-Teilnetz (bzw. in Teilnetze, auf die der Client zugreifen kann, wenn der Clientcomputer über mehr als eine LAN-Adapterkarte verfügt) sendet. Dazu geben Sie als ersten Servernamen einen Stern (\*) ein.

Diese Option ist nur verfügbar, wenn der Client IPV4-Adressen verwendet. UDP-Broadcasts werden für IPV6 nicht unterstützt.

Der Client wiederholt den Broadcast-Versuch alle 10 Sekunden, bis die vom Parameter *broadcast\_attempt\_count* angegebene Anzahl von Versuchen erreicht ist oder der Kontakt zu einem Server hergestellt wurde. Wird die von *broadcast\_attempt\_count* angegebene Begrenzung erreicht, bevor der Kontakt zu einem Server hergestellt werden kann, versucht der Client, direkte Nachrichten an benannte Server (die von den folgenden Zeilen der Datei angegeben werden) zu senden.

**Anmerkung:** Wenn Sie keine UDP-Broadcasts verwenden, müssen Sie die Namen aller Server angeben, zu denen der Client eine Verbindung herstellen soll. Der Client kann Ressourcen auf den in dieser Datei angegebenen Servern verwenden, jedoch keine Ressourcen auf anderen Servern.

**-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.

**-aZeitlimit**

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

### **-bmaximale Broadcast-Versuche**

Dies Option wird nur verwendet, wenn der Client UDP-Broadcasts verwendet. Dies wird mit dem Zeichen \* (Stern) anstelle des ersten Servernamens angezeigt.

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.

### **-jZeitlimit 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.

Geben Sie den Befehl `setup -h -1Sprachencode` ein, um Hilfeinformationen zu den Optionen am Bildschirm anzuzeigen. `Sprachencode` entspricht dabei dem Code (siehe oben) für die Sprache, in der Sie die Informationen anzeigen wollen. Geben Sie beispielsweise den Befehl `setup -h -10x0009` ein, um die Hilfeinformationen auf Englisch anzuzeigen. Sie können `-h` durch `-?` ersetzen. Um die Hilfeinformationen auf Spanisch anzuzeigen, können Sie beispielsweise `setup -? -10x000a` eingeben.

Hier sehen Sie eine Beispielbefehlszeile für die Installation des Remote API Client:

```
setup -imy_domain -userver1.company.com -userver2.company.com -b0 -j30 -accept -s -f2C:\instrapi.log -y
```

Für dieses Beispiel gilt Folgendes:

- Der Client wird in der Domäne `my_domain` installiert.
- Der Client hat Zugriff auf zwei Server, die sich in demselben privaten Netz wie der Client befinden, und verwendet keine UDP-Broadcasts, um Kontakt zu anderen Servern aufzunehmen. Geht der Kontakt zu einem Server verloren, wartet der Client 30 Sekunden, bis er eine neue Verbindung herstellt.
- Die Installation wird im unbeaufsichtigten Modus durchgeführt, so dass die Informationen des Installationsprotokolls in die Datei `C:\instrapi.log` auf dem Client geschrieben werden.
- Vorhandene Kopien der .DLL-Dateien des Remote API Client werden in einem Unterverzeichnis gespeichert, bevor die neuen Dateien installiert werden.
- Wenn keine Sprachenoption angegeben ist, wird die Standardsprache (Englisch) verwendet.

## 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 `Installationsverzeichnis\snakeyman.exe` aus. `Installationsverzeichnis` steht hier für das Verzeichnis, in dem Sie die Clientsoftware installiert haben. Wenn Sie während der Clientinstallation kein anderes Verzeichnis angegeben haben, ist dies das Verzeichnis `C:\IBMCS\w32cli` (32-Bit-Client) oder `C:\IBMCS\w64cli` (64-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 Clientsicherheitszertifikaten 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 Clientzertifikat 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-Schlüsselverwaltungsprogramm.

## Remote API Client nach der Installation anpassen

---

Nach der Erstinstallation können Sie die angepassten Einstellungen der Software jederzeit mit dem Konfigurationsdienstprogramm ändern. Sie finden dieses Programm in der Programmgruppe "IBM Remote API". 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 56 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 und als Installationstyp **Developer** auswählen.

Für den Client gibt es weitere Optionen, die mit Variablen in der Windows-Registrierung konfiguriert werden. Diese Optionen sind im *Verwaltungshandbuch für IBM Communications Server for Data Center Deployment für AIX* beschrieben. Zu ihnen gehört ein Aufrufzeitgeber, mit dem der Client regelmäßig Aufrufe an den Server absetzen kann, um zu verhindern, dass Firewalls die TCP/IP-Verbindung zwischen Client und Server unterbrechen.

Wenn Sie die erweiterte Unterstützung für die Verfolgung von LUs und die Zuordnung von Aliasnamen der lokalen LU aktivieren möchten, sind weitere Konfigurationsschritte erforderlich. Mit dieser Unterstützung können Clients dynamischer integriert und LU-Ressourcen in einer Serverdomäne verwaltet werden. Weitere Details hierzu können Sie im *Verwaltungshandbuch für IBM Communications Server for Data Center Deployment für AIX* im Abschnitt 'Remote API Clients verwalten' nachlesen.

## Software Remote API Client erneut installieren

---

Sie können die Software Remote API Client 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 56 oder im Abschnitt „[Remote API Client über die Befehlszeile installieren](#)“ auf Seite 59 stützen. Das Setup-Programm zeigt das Verzeichnis an, von dem die Clientsoftwaredateien 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 Software Remote API Client im Hintergrundmodus ausführen (siehe Abschnitt „Remote API Client über die Befehlszeile installieren“ auf Seite 59), 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 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 die Schaltfläche Beenden klicken, kehrt das System zu Windows zurück.

## Remote API Client über die Befehlszeile deinstallieren

Anstatt die Software Remote API Client mit der Option `Programme ändern oder entfernen` in der Windows-Systemsteuerung zu deinstallieren, können Sie sie auch über die Befehlszeile deinstallieren. Verwenden Sie den folgenden Befehl:

`Installationsverzeichnis\sqxcluninst -y instdir installdir`

- `Installationsverzeichnis` steht hier für das Verzeichnis, in dem Sie die Clientsoftware installiert haben. Dies ist das Verzeichnis `C:\IBMCS\w64cli`, wenn Sie während der Clientinstallation keine andere Position angegeben haben.
- Die Option `-y` wird zur Bestätigung verwendet, um eine versehentliche Verwendung dieses Befehls auszuschließen.
- Die Option `instdir` sollte angegeben werden, wenn das Programm nicht im Verzeichnis `C:\IBMCS\w64cli` installiert wurde.

Das Deinstallationsprogramm wird ohne Eingabeaufforderungen und ohne weitere erforderliche Eingaben ausgeführt.

## **Hilfe**

---

Falls Sie Hilfe benötigen, können Sie jederzeit über die Taste F1 Hilfetexte aufrufen. Im Konfigurationsfenster und im Fenster "Erweiterte Optionen" gibt es außerdem eine Schaltfläche Hilfe.



# Kapitel 8. CS/AIX konfigurieren und verwenden

Der einfachste Weg, die CS/AIX-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 Verwaltungstools verwenden, z. B. das Webverwaltungsprogramm oder das Befehlszeilenverwaltungsprogramm. Wir empfehlen Ihnen jedoch, mit dem Motif-Programm zu arbeiten.

Das Motif-Verwaltungsprogramm stellt Hilfearbeiten mit übersichtlichen Informationen zu SNA und CS/AIX, Referenzinformationen zu CS/AIX-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 CS/AIX 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/AIX-System verwalten. Das Verwaltungsprogramm bietet Ihnen die Möglichkeit, die Konfiguration zu ändern, während CS/AIX aktiv ist. In diesem Programm können Sie auch auf komfortable Weise Statusinformationen zu den Knotenressourcen aufrufen.

Das Motif-Verwaltungsprogramm zeigt automatisch Statusinformationen zu CS/AIX-Ressourcen an. Die meisten dieser Informationen werden im Knotenfenster angezeigt (siehe Abschnitt „CS/AIX mit dem Motif-Verwaltungsprogramm verwalten“ auf Seite 70). Über die Schaltflächen 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 CS/AIX definieren oder ändern möchten, müssen Sie zur Anmeldegruppe system gehören.
2. Für die Verwendung des Motif-Verwaltungsprogramms brauchen Sie ein Low-Function Terminal (LFT) oder X-Terminal. Andernfalls können Sie SMIT (System Management Interface Tool) oder das Webverwaltungsprogramm verwenden. Beide stellen ähnliche Funktionen wie das Motif-Programm bereit. Weitere Informationen hierzu finden Sie im *Verwaltungshandbuch für IBM Communications Server for Data Center Deployment für AIX*.
3. Zusätzliche Informationen zur Benutzerschnittstelle des Motif-Verwaltungsprogramms, z. B. zu den in den Fenstern angezeigten Schaltflächen und Symbolen, können Sie den Hilfetextanzeigen des Programms und dem *Verwaltungshandbuch für IBM Communications Server für AIX* 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/AIX-Verwaltungstools (u. a. zur Webverwaltung, zum Befehlszeilenverwaltungsprogramm und zu NOF-Anwendungsprogrammen) finden Sie im *Verwaltungshandbuch für IBM Communications Server für AIX*, im *Verwaltungshandbuch für IBM Communications Server for Data Center Deployment für AIX* und im *IBM Communications Server for Data Center Deployment on AIX NOF Programmer's Guide*.

## CS/AIX-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/AIX-Client-Server-System mit mehreren Knoten konfigurieren, vergewissern Sie sich, dass alle CS/AIX-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 *Verwaltungshandbuch für IBM Communications Server for Data Center Deployment für AIX* können Sie feststellen, welche Konfigurationsdaten Sie für bestimmte CS/AIX-Funktionen erfassen müssen.

Im vorliegenden Kapitel finden Sie Anweisungen für das Konfigurieren der am häufigsten verwendeten Funktionen von CS/AIX. 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 CS/AIX eingeben müssen. Weitere Informationen zu den Feldern einzelner Dialoganzeigen finden Sie in den Texten der Onlinehilfe für das Motif-Verwaltungsprogramm oder SMIT.

## Planungsblätter

Bevor Sie mit dem Konfigurieren von Ressourcen für CS/AIX beginnen, müssen Sie alle Konfigurationsdaten für die neuen Ressourcen zusammenstellen. Verwenden Sie zum Erfassen der Daten für eine bestimmte, benötigte Funktion oder Anwendung die im *Verwaltungshandbuch für IBM Communications Server for Data Center Deployment für AIX* 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.

## Umgebungsvariablen für CS/AIX definieren

Der Betrieb von CS/AIX wird mit einer Reihe von Umgebungsvariablen gesteuert, die Sie vor der Aktivierung der Software CS/AIX auf dem Server festlegen müssen. Am einfachsten ist es, die Variablen in einer Textdatei festzulegen, die CS/AIX beim Start liest.

Erstellen Sie eine Textdatei mit dem Namen `environment` im Konfigurationsverzeichnis `/etc/sna` von CS/AIX und legen Sie in jeder Zeile eine Umgebungsvariable fest. Beispiel:

```
export LANG=en_US
export PATH='$PATH:/usr/bin'
export LD_LIBRARY_PATH=/usr/lib:/usr/lib/sna
export LD_RUN_PATH=/usr/lib:/usr/lib/sna
```

## 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/AIX-Programmen angeben](#)“ auf Seite 69). Darüber hinaus müssen Sie die Software CS/AIX aktivieren, bevor Sie das Verwaltungsprogramm verwenden können (siehe Abschnitt „[CS/AIX aktivieren](#)“ auf Seite 69).

Informationen zum Aufrufen des Motif-Verwaltungsprogramms und einen Überblick über die Verwendung des Programms finden Sie im Abschnitt „[CS/AIX mit dem Motif-Verwaltungsprogramm verwalten](#)“ auf Seite 70.

## Pfad zu CS/AIX-Programmen angeben

Voraussetzung für die Ausführung von CS/AIX-Programmen ist, dass Sie den Pfad zu dem Verzeichnis angeben, das die ausführbaren CS/AIX-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 `/usr/bin/X11` gespeichert. Die übrigen Programme befinden sich im Verzeichnis `/usr/bin`. Wenn Sie diese Verzeichnisse zur Definition der Umgebungsvariablen `PATH` in Ihrer Datei `.login` oder `.profile` hinzufügen, findet CS/AIX die Programme automatisch. Alternativ dazu können Sie wie in den folgenden Beispielen den Verzeichnisnamen angeben, wenn Sie das Programm ausführen:

```
/usr/bin/sna start
/usr/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.

## CS/AIX aktivieren

Sie können den lokalen Knoten erst konfigurieren oder verwalten, nachdem Sie CS/AIX 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.

Normalerweise wird CS/AIX nach der Installation automatisch aktiviert. Falls CS/AIX inaktiviert wurde, können Sie die Software reaktivieren, indem Sie an der AIX-Eingabeaufforderung den folgenden Befehl eingeben:

```
sna start
```

**Anmerkung:** Wenn Sie den Befehl `sna start` angeben, verwendet die Software CS/AIX das Verzeichnis, von dem aus Sie den Befehl abgesetzt haben, als aktuelles Arbeitsverzeichnis und verwaltet offene Dateideskriptoren in diesem Verzeichnis. Deshalb können Sie das Dateisystem mit diesem Verzeichnis nicht

abhangen, solange die Software CS/AIX aktiv ist. Um Probleme zu vermeiden, sollten Sie die Software CS/AIX von einem Verzeichnis in einem Dateisystem starten, das nicht abgehängt werden muss. Sie können Beispielsweise mit `cd /` das Stammverzeichnis aufrufen, bevor Sie den Befehl `sna start` absetzen.

Bei der Installation von CS/AIX aktualisiert das Installationsdienstprogramm automatisch die Startdatei `/etc/inittab` und fügt einen Eintrag für die Datei `/etc/rc.sna` hinzu, die den Befehl `sna start` enthält. Damit wird sichergestellt, dass CS/AIX beim Systemstart automatisch gestartet wird. Falls Sie nicht möchten, dass CS/AIX 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 CS/AIX ausführen.

CS/AIX schreibt Nachrichten auf die Standardfehlerausgabe (in der Regel der Bildschirm Ihres Terminals) und gibt so an, ob die Initialisierung erfolgreich verläuft.

## CS/AIX mit dem Motif-Verwaltungsprogramm verwalten

Stellen Sie vor Verwendung des Motif-Verwaltungsprogramms für CS/AIX sicher, dass CS/AIX wie im Abschnitt „CS/AIX aktivieren“ auf Seite 69 beschrieben initialisiert wurde. (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 &
```

CS/AIX zeigt daraufhin 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 [Abbildung 4 auf Seite 71](#) 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 74 beschrieben zu konfigurieren.

**Anmerkung:** Im vorliegenden Handbuch wird der Begriff Fenster für die Motif-Fenster verwendet, in denen Informationen zu CS/AIX-Ressourcen angezeigt werden. Ein Fenster kann ein oder mehrere Teilelfenster 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/AIX-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

[Abbildung 4 auf Seite 71](#) zeigt ein Beispiel für ein Knotenfenster. In der Titelleiste ist der Name des AIX-Systems angegeben.

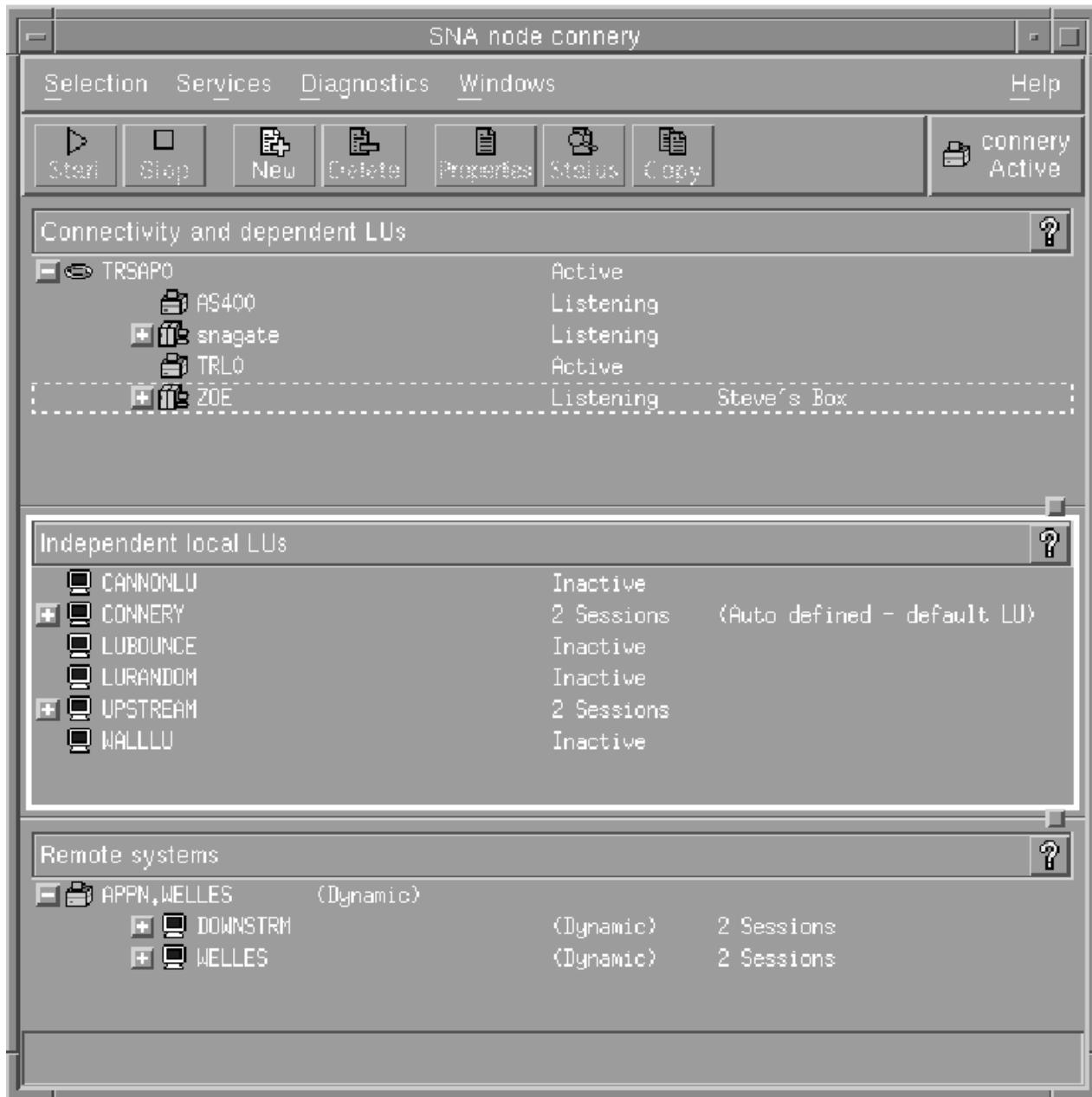


Abbildung 4. Knotenfenster

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

- Ports
- Verbindungsstationen
- LUs der Typen 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 Schaltflächen 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 die Schaltfläche Einblenden (+) klicken, werden die Ressourcen für diese Komponente angezeigt (sofern sie nicht schon vorher angezeigt wurden). Klicken Sie auf die Schaltfläche Ausblenden (-), wird die Anzeige der Ressourcen für diese Komponente verdeckt.

Im Knotenfenster können Sie die folgenden Verwaltungsaufgaben ausführen:

### **Ressource starten oder stoppen**

Wählen Sie die Ressource aus und klicken Sie auf die Schaltfläche 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 die Schaltfläche 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 die Schaltfläche Neu.

### **Ressource löschen**

Wählen Sie die Ressource aus und klicken Sie auf die Schaltfläche 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 die Schaltfläche Eigenschaften (oder wählen Sie im Menü Auswahl die Option Eigenschaften aus).

### **Statusinformationen für eine Ressource abrufen**

Wählen Sie die Ressource aus und klicken Sie auf die Schaltfläche 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 die Schaltfläche 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 untergeordnete Elemente 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.

## Symbolleistenschaltflächen

Ressourcenfenster enthalten eine Symbolleiste mit Schaltflächen, die das Ausführen allgemeiner Funktionen vereinfachen. Eine Symbolleiste für CS/AIX ist in Abbildung 5 auf Seite 73 dargestellt.



Abbildung 5. CS/AIX-Symbolleiste

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

### Starten

Aktiviert das ausgewählte Element

### Stoppen

Inaktiviert das ausgewählte Element

### Neu

Fügt einen neuen Ressourceneintrag hinzu

### Löschen

Löscht die ausgewählten Ressourcen

### Eigenschaften

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 diese Schaltfläche 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 die Schaltfläche Merkmale die zugehörige Dialoganzeige öffnen. Wenn Sie die Dialoganzeige wieder schließen wollen, klicken Sie auf die Schaltfläche Schließen.

## Client-Server-Funktionen konfigurieren

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

In einer Client-Server-Umgebung kann ein Server als Konfigurationsserver markiert werden. CS/AIX verwaltet eine Liste dieser Konfigurationsserver. Der erste aufgelistete Server ist der Controller-Server. Alle weiteren Server in der Liste sind Ausweichserver. Die Server werden der Reihe nach aufgelistet, so dass der zweite aufgelistete Server (der erste Ausweichserver) die Aufgaben des Controller-Servers übernimmt, wenn dieser nicht verfügbar ist. Der dritte Server in der Liste (der zweite Ausweichserver) übernimmt diese Aufgaben, falls weder der Controller 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 CS/AIX, zu dem eine Verbindung hergestellt werden kann) zum Controller-Server. Falls der aktuelle Controller 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 Controller.

CS/AIX kann ohne einen Controller 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 Controller-Servers übernehmen soll. Der Controller-Server 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 Controller-Server, 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 CS/AIX ausgeführt wird, weil in diesem Fall kein Server mehr verfügbar wäre, der die Aufgaben des Controller-Servers übernehmen könnte. In einer Client-Server-Konfiguration ist mindestens ein aktiver Controller-Server erforderlich.

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

## Knoten konfigurieren

Der erste Schritt der CS/AIX-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.

Abbildung 6 auf Seite 75 zeigt einen CS/AIX-Knoten, der direkt mit einem Host kommuniziert.

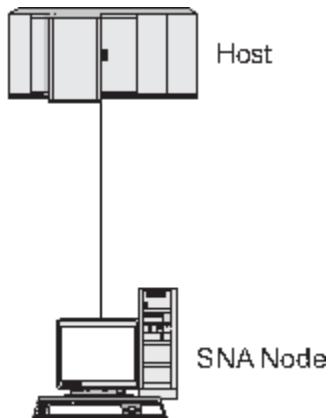


Abbildung 6. CS/AIX-Knoten, der direkt mit einem Host kommuniziert

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

Abbildung 7 auf Seite 75 zeigt mehrere CS/AIX-Knoten in einem APPN-Netz.

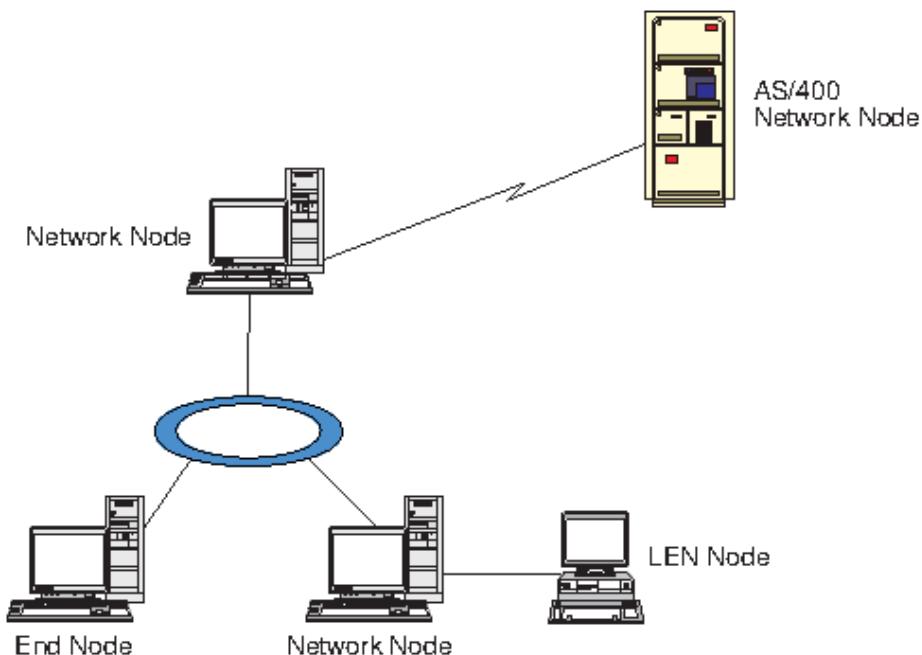


Abbildung 7. CS/AIX-Knoten in einem APPN-Netz

## Konnektivität konfigurieren

Wenn der lokale Knoten Teil eines APPN-Netzes ist und APPN-Routingdienste für andere Knoten bereitstellen soll, konfigurieren Sie ihn als APPN-Netzknoten. Werden die Routingdienste 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. CS/AIX zeigt daraufhin den Parameterdialog für Knoten 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 CS/AIX 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 die Schaltfläche Abbrechen.

## Konnektivität konfigurieren

Ein CS/AIX-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 CS/AIX unterstützten Verbindungsprotokolle finden Sie im Abschnitt „Installationsvoraussetzungen“ auf Seite 17.

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 *Verwaltungshandbuch für IBM Communications Server for Data Center Deployment für AIX* 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 Wähleleitung oder Standleitung)
- Funktion der Verbindungsstation ('Primär', 'Sekundär', 'Aushandelbar', 'Primär für Mehrpunktverbindungen' oder 'Sekundär, mehrere PUs')
- Aufrufadresse (nur für eine ankommende Wähleleitung an einem nicht primären Port). Bei anderen Port-Typen wird die Aufrufadresse auf der Verbindungsstation konfiguriert.

Für ankommende Wähleitungen und Standleitungen benötigen Sie außerdem die Verschlüsselung (NRZ oder NRZI) und die Duplexeinstellung (Halb- oder Voll duplex). Bei anderen Port-Typen werden die Verschlüsselung und die Duplexeinstellung auf der Verbindungsstation konfiguriert.

- Art der physischen Verbindung (zur Bezeichnung des Modemtyps)
- Wählfolge (nur für ankommende Wähleitungen). Bei einer abgehenden Wähleitung wird die Wählfolge für die 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 die Schaltfläche 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 CS/AIX 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 die Schaltfläche Neu).
- c. Klicken Sie auf OK.

CS/AIX zeigt daraufhin 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 die Unterstützung von abhängigem und unabhängigem Datenverkehr 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, Servicezugriffspunkt) angeben (in der Regel 04).
- 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 die Schaltfläche **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 CS/AIX 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 die Schaltfläche **Neu**).
- c. Klicken Sie auf **OK**.

CS/AIX zeigt daraufhin 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 die Schaltfläche 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 CS/AIX 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 die Schaltfläche Neu).
- c. Klicken Sie auf OK.

CS/AIX zeigt daraufhin 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 der Typen 0-3 konfigurieren

Zur Unterstützung von Benutzeranwendungen, die LUs der Typen 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 74 beschrieben.

## LUs der Typen 0-3 konfigurieren

- Konfigurieren Sie eine Verbindung für abhängigen LU-Datenverkehr. Lesen Sie dazu die Beschreibung im Abschnitt „Konnektivität konfigurieren“ auf Seite 76.

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 87 und „DLUR konfigurieren“ auf Seite 90.

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 der Typen 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 der Typen 0-3 für eine bereits definierte Verbindungsstation zu konfigurieren:

1. Wählen Sie im Konnektivitätsteilfenster die Verbindungsstation zum Host aus.
2. Klicken Sie auf 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 CS/AIX den Dialog für LUs der Typen 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 der Typen 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/AIX-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

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.

CS/AIX zeigt daraufhin das Fenster für LU-Pools an.

2. Klicken Sie auf Neu.

CS/AIX 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 die Schaltfläche 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 die Schaltfläche 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 Peercomputer 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 74 beschrieben.
2. Konfigurieren Sie die Konnektivität wie im Abschnitt „Konnektivität konfigurieren“ auf Seite 76 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/AIX-Knoten ein Endknoten oder Netz-knoten 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 86). 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 Peercomputer zu kommunizieren. Für eine CPI-C-Anwendung müssen Sie die gleichen Ressourcen wie für eine APPC-Anwendung definieren. Wenn das Transaktionsprogramm auf dem CS/AIX-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 86 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“ auf Seite 82) 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 86 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 *Verwaltungshandbuch für IBM Communications Server for Data Center Deployment für AIX*.

## 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 Sitzungsrouting 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 74 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 76 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/AIX-Knotens können Sie wie folgt abrufen:

1. Wählen Sie im Knotenfenster den Port aus.
2. Klicken Sie auf **Start**, um den Knoten zu definieren.
3. Klicken Sie auf die Schaltfläche **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 74 beschrieben. Wählen Sie für das Feld *APPN-Unterstützung* den Wert Endknoten aus.
2. Konfigurieren Sie die Konnektivität wie im Abschnitt „Konnektivität konfigurieren“ auf Seite 76 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 Netzknöten ein (siehe Abschnitt „Netzknöten konfigurieren“ auf Seite 82).
  - Geben Sie im Teilfenster 'Verbindungsinformationen' des Konfigurationsdialogs für die Verbindungsstation die MAC-Adresse und die SAP-Nummer des Ports auf dem Netzknöten ein.

In einem APPN-Netz ist es möglich, über nur eine Verbindungsstation zu einem benachbarten Netzknöten 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 Netzknöten gemäß der Beschreibung im Abschnitt „Netzknöten konfigurieren“ auf Seite 82 und einen Endknoten gemäß der Beschreibung im Abschnitt „Endknoten konfigurieren“ auf Seite 83 konfiguriert haben. Auf dem Endknoten können Sie die folgenden Schritte ausführen:

1. Wählen Sie im Knotenfenster die Verbindungsstation zum benachbarten Netzknöten aus.
2. Klicken Sie auf **Starten**, um die Verbindungsstation zu starten.

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 die Schaltfläche **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 die Schaltfläche **Neu**).
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 Netzknoten-server 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“ auf Seite 85), eine Definition für eine Partner-LU auf einem bestimmten fernen Knoten hinzufügen (siehe Abschnitt „Partner-LU auf einem fernen Knoten definieren“ auf Seite 85) oder mehrere Partner-LUs unter Verwendung von Platzhaltern definieren (siehe Abschnitt „Mehrere Partner-LUs mit Platzhaltern definieren“ auf Seite 85).

## Fernen Knoten definieren

Bevor Sie einen fernen Knoten konfigurieren, benötigen Sie die folgende Information:

- 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 die Schaltfläche Neu und wählen Sie die Option Fernen Knoten definieren aus).

CS/AIX zeigt daraufhin 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 CS/AIX 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 die Schaltfläche Neu und wählen Sie die Option Aliasnamen für Partner-LU definieren aus).

CS/AIX 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 fernen Knoten aus (oder klicken Sie in der Symbolleiste auf die Schaltfläche Neu und wählen Sie die Option Partner-LU auf fernen Knoten definieren aus).

CS/AIX 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 mit 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 die Schaltfläche Neu und wählen Sie die Option Generische Partner-LU auf **fernem Knoten** definieren aus).  
CS/AIX zeigt daraufhin den Konfigurationsdialog für generische Partner-LUs 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 die Schaltfläche Neu und wählen Sie die Option Neue abhängige lokale LU aus).  
CS/AIX zeigt daraufhin 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.  
CS/AIX zeigt daraufhin das Fenster für CPI-C-Bestimmungsorte an.
2. Klicken Sie auf Neu.  
CS/AIX zeigt daraufhin 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 der Typen 0-3 mit einem Host kommunizieren. (Ausführliche Informationen zur API LUA finden Sie im *IBM Communications Server for Data Center Deployment on AIX or 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 74 beschrieben.
2. Konfigurieren Sie Konnektivität für abhängigen Verkehr wie im Abschnitt „[Konnektivität konfigurieren](#)“ auf Seite 76 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 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 80 beschrieben.

## SNA Gateway konfigurieren

---

CS/AIX 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/AIX-Knoten auf einen Host zugreifen, so dass keine gesonderte Verbindung vom Host zu jedem einzelnen Computer erforderlich ist.

Das Feature SNA Gateway ist in [Abbildung 8 auf Seite 88](#) veranschaulicht.

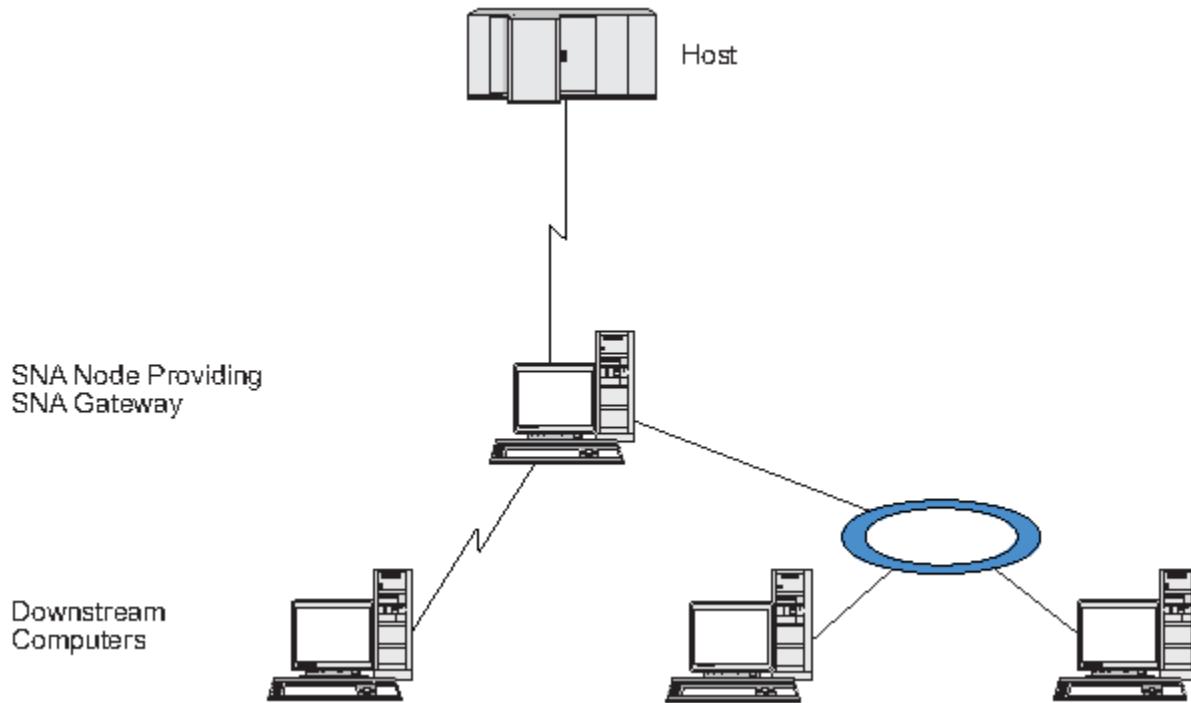


Abbildung 8. SNA Gateway

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/AIX-Computer oder ein PC sein, auf dem Communications Server für Windows ausgeführt wird.

Wenn der lokale CS/AIX-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/AIX-Computer oder mit anderen untergeordneten Computern nutzen. Sie können z. B. mehrere untergeordnete Computer installieren, die über ein lokales Token-Ring-Netz mit dem CS/AIX-Computer verbunden sind. In diesem Fall greifen alle Computer auf dieselbe Standfernleitung des CS/AIX-Computers zum Host zu.

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/AIX-Computer und dessen Hostübertragungsleitung umfassen. Die LUs auf den untergeordneten Computern werden zusammen mit den Ressourcen des CS/AIX-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 74 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 76 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](#)“ auf Seite 89).
- Definieren Sie die LUs auf dem lokalen Knoten, die für die Kommunikation mit dem Host verwendet werden (übergeordnete LUs). Definieren Sie die übergeordneten LUs der Typen 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 80 beschrieben.

## Implizite untergeordnete LUs unterstützen

Zur Unterstützung untergeordneter LUs, die noch nicht für CS/AIX 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 76 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 Knotenfens-ters doppelt auf die Port-Definition. CS/AIX zeigt daraufhin 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 Neu.
- c. Wählen Sie in der daraufhin erscheinenden Dialoganzeige die Option zum Definieren eines Ports und den Verbindungsprotokolltyp aus.

CS/AIX zeigt daraufhin den Konfigurationsdialog für Ports an.

- d. Geben Sie gemäß der Beschreibung im Abschnitt „Konnektivität konfigurieren“ auf Seite 76 die wichtigsten Port-Parameter ein.

2. Klicken Sie unten in der Dialoganzeige auf die Schaltfläche **Erweitert**.

CS/AIX zeigt daraufhin den Parameterdialog für Ports 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.

CS/AIX 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 Knotenfens-ters die Verbindungsstation zum untergeordneten Knoten aus.

2. Klicken Sie auf Neu.

3. Wählen Sie die Option **Neue untergeordnete LU** aus und klicken Sie auf OK.

CS/AIX zeigt daraufhin den Dialog für untergeordnete LU an.

## DLUR konfigurieren

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

---

CS/AIX 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/AIX-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/AIX-DLUR-Knoten ein Netzknoten oder ein Zweignetzknoten ist, kann er auch Durchgriff-DLUR-Funktionen für abhängige LUs auf untergeordneten Computern, die mit dem CS/AIX-Knoten verbunden sind, bereitstellen. Diese LUs können ebenso wie knoteninterne LUs DLUR auf dem CS/AIX-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.

[Abbildung 9 auf Seite 91](#) zeigt einen als APPN-Netzknoten konfigurierten CS/AIX-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 (untergeordneten Knoten).

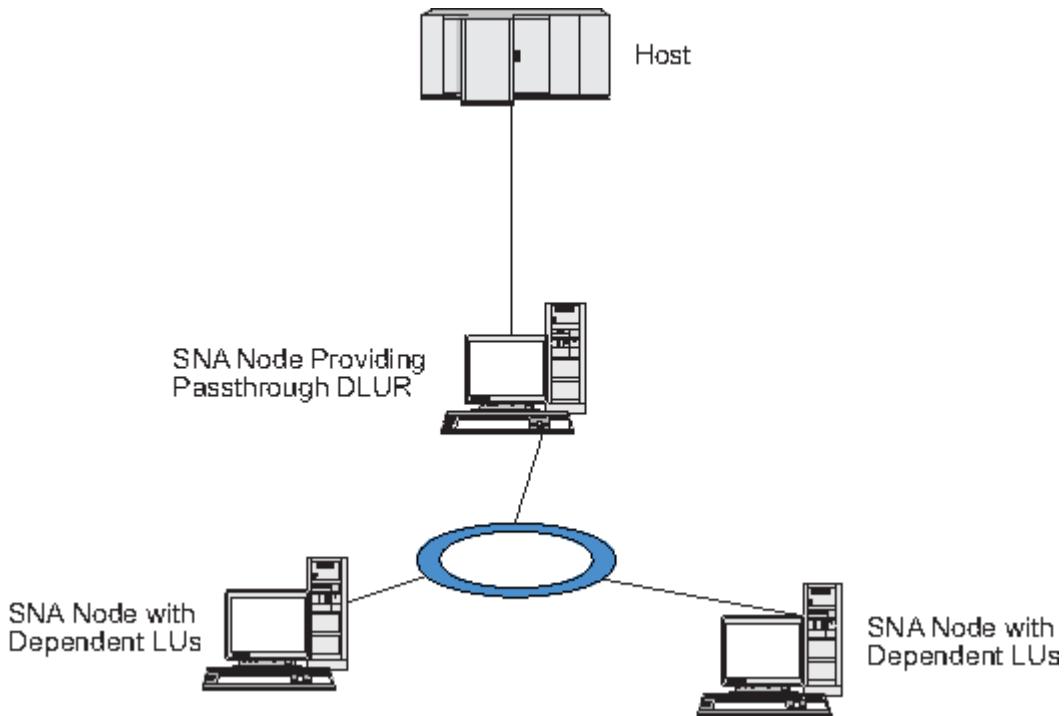


Abbildung 9. CS/AIX-Knoten, der DLUR bereitstellt

**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 74 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 76.

## TN Server konfigurieren

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 die Schaltfläche Neu und wählen Sie die Option DLUR-PU aus).

Wenn Sie auf OK klicken, zeigt CS/AIX 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 87 beschrieben für die Unterstützung von LUA konfiguriert werden. In Abhängigkeit von den Anforderungen der von den LUs unterstützten Benutzeranwendungen können weitere Konfigurations-schritte 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 74).
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 76 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/AIX-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.

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

Abbildung 10 auf Seite 93 zeigt einen CS/AIX-Knoten mit TN-Server-Unterstützung für TN3270-Clients. Der TN-Server-Knoten kommuniziert über das TCP/IP-Netz mit den Clients.

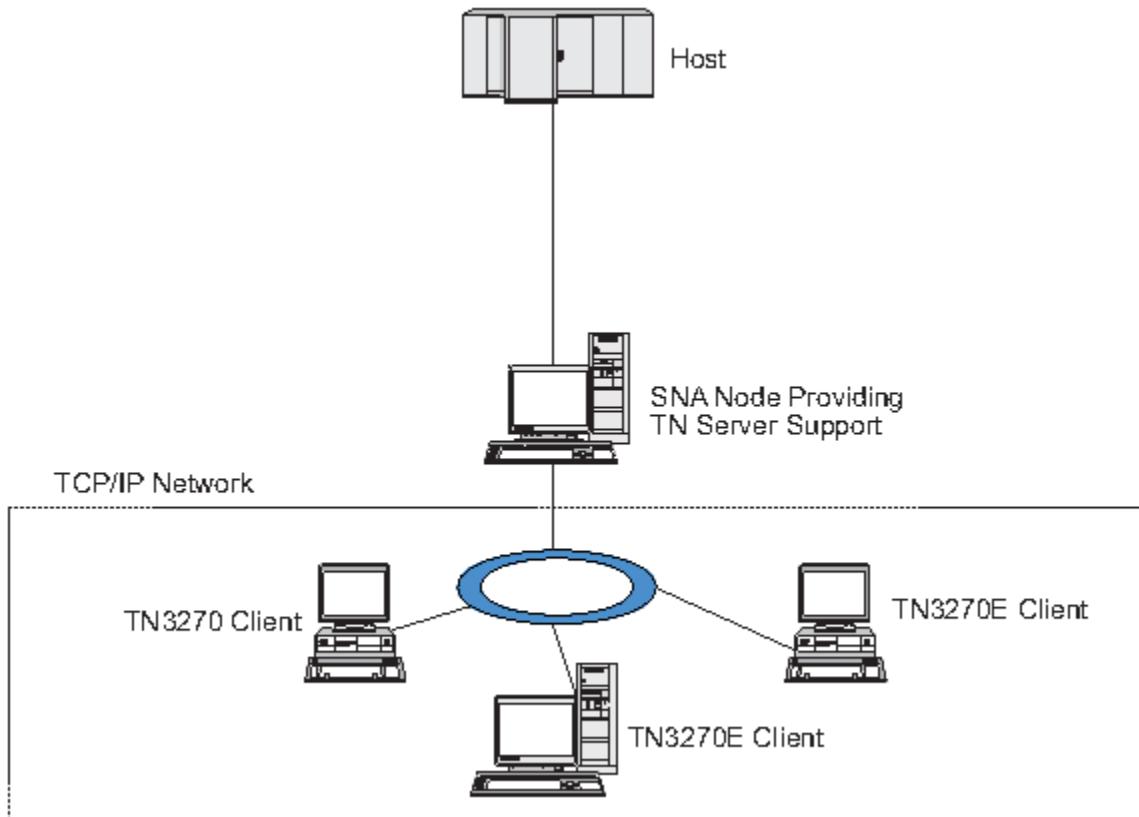


Abbildung 10. Für TN Server konfigurierter CS/AIX-Knoten

Das Feature TN Server von CS/AIX ermöglicht die Zuordnung eines TN3270-Benutzers zu einer 3270-LU unter CS/AIX. 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.

CS/AIX TN Server 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 CS/AIX das Programm über die TCP/IP-Adresse des Computers, auf dem das TN3270-Programm ausgeführt wird. CS/AIX kann zwei TN3270-Programme, die von zwei verschiedenen Benutzern auf demselben Computer ausgeführt werden, nicht unterscheiden. In den CS/AIX-Handbüchern bezieht sich die Bezeichnung 'Benutzer von TN Server' auf den Computer, auf dem ein TN3270-Programm ausgeführt wird, nicht auf einen individuellen Programm Benutzer.

Wie in Abbildung 11 auf Seite 94 gezeigt, stellt sich die Konfiguration aus Sicht des Hosts und des TN-Server-Benutzers unterschiedlich dar.

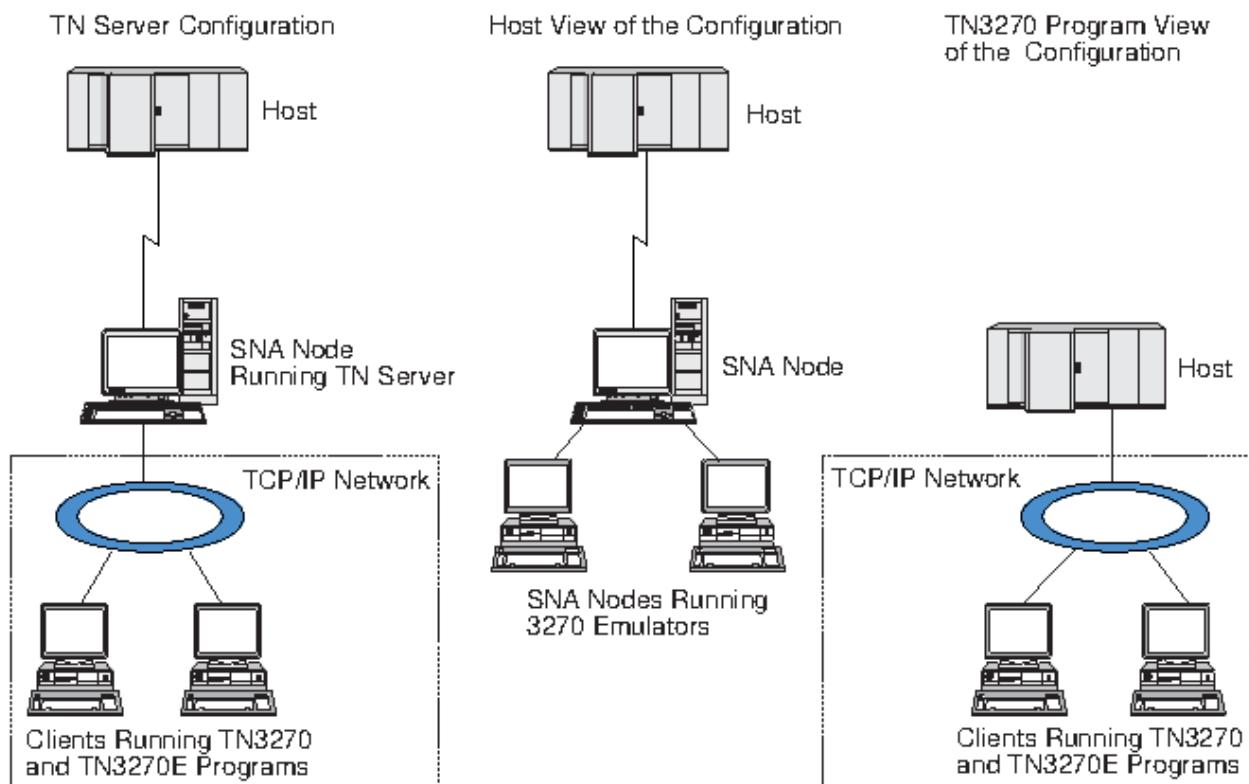


Abbildung 11. TN Server

Für jeden Benutzer von TN Server, der mit dem Feature TN3270 Server eine Verbindung zu CS/AIX 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 74 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 76 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“ auf Seite 94.
- Wenn Sie LU-Pools verwenden wollen, definieren Sie diese wie im Abschnitt „LU-Pool definieren“ auf Seite 95 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 der Typen 0-3 für eine bereits definierte Verbindungsstation zu konfigurieren:

1. Wählen Sie im Konnektivitätsteilfenster die Verbindungsstation zum Host aus.
2. Klicken Sie auf 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 CS/AIX den Dialog für LUs der Typen 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 Clientsitzung 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/AIX-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.

CS/AIX zeigt daraufhin das Fenster für LU-Pools an.

2. Klicken Sie auf Neu.

CS/AIX 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 die Schaltfläche 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 die Schaltfläche Entfernen.

4. Klicken Sie auf OK, um den LU-Pool zu definieren.

## TN Server konfigurieren

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, Clientauthentifizierung und Serverauthentifizierung erforderlich sind (Diese Option ist nur verfügbar, wenn Sie die zusätzliche, zur Unterstützung dieser Option erforderliche Software installiert haben.)
- Angabe, ob der TN3270-Server in einem SLP-Netz verwendet wird

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-Clientsitzungen 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.

CS/AIX 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 die Schaltfläche Neu.

CS/AIX ruft daraufhin den Dialog für TN-Server-Zugriff auf.

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 die Schaltfläche Neu.

CS/AIX ruft daraufhin den Dialog für TN-Server-Zuordnungseinträge auf.

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 Supportwebseiten zu IBM Communications Server unter der Adresse <https://www.ibm.com/mysupport/s/topic/0TO0z0000006v3OGAQ/communication-server>.

## TN Redirector konfigurieren

---

Das CS/AIX-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 CS/AIX und CS/AIX kommuniziert dann 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 CS/AIX 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 CS/AIX und dem Host verwenden. Auf diese Weise wird die Sicherheit für alle Clients überprüft. Die einzelnen Clients müssen keine Sicherheitsangaben machen.
- Wenn CS/AIX an demselben Standort wie der Host installiert ist, die Clients die Verbindung jedoch von externen Standorten aus aufzubauen, können Sie SSL für die Clientverbindungen zu CS/AIX 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 74 beschrieben definieren. Außerdem benötigen Sie die folgenden Informationen:

- den TCP/IP-Namen oder die TCP/IP-Adresse des Clients, wenn nur bestimmte Clients zulässig sind
- 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, Clientauthentifizierung 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.

CS/AIX 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 die Schaltfläche Neu.

CS/AIX ruft daraufhin den Dialog für TN-Redirector-Zugriff auf.

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.

## **CS/AIX inaktivieren**

---

Durch Inaktivierung der Software CS/AIX werden automatisch der CS/AIX-Knoten und die zugehörigen Konnektivitätskomponenten gestoppt. Nach Inaktivierung von CS/AIX können alle Prozesse (z. B. 3270-Emulationsprogramme) auf diesem Server keine CS/AIX-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/AIX-Aktivität vorliegt.

Wenn Sie CS/AIX inaktivieren müssen, warnen Sie die Benutzer, dass Sie CS/AIX stoppen wollen, und geben Sie ihnen Zeit, die gerade laufenden Aktivitäten vor Inaktivierung der Software zu beenden.

Benutzt ein 3270-Emulationsprogramm LUs auf dem Knoten, wenn Sie die Software CS/AIX inaktivieren, werden alle 3270-Emulationssituationen, die diese LUs benutzen, beendet. Das Programm wird weiter ausgeführt, doch der Benutzer kann die Sitzungen erst wieder verwenden, wenn die Software reaktiviert wurde. Anwendungen, die die API APPC, CSV, LUA, NOF oder MS benutzen, werden durch einen Rückkehrcode COMM\_SUBSYSTEM\_ABENDED und CPI-C-Anwendungen durch einen Rückkehrcode CM\_PRODUCT\_SPECIFIC\_ERROR benachrichtigt.

Geben Sie zum Inaktivieren der Software CS/AIX an der AIX-Eingabeaufforderung den folgenden Befehl ein:

```
sna stop
```

Wenn CS/AIX 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 CS/AIX nicht inaktiviert wurde. Weitere Informationen zu den Werten von Exit-Codes finden Sie im *IBM Communications Server for Data Center Deployment on AIX Diagnostics Guide*.

# Kapitel 9. Informationsquellen für CS/AIX 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.

Eine Liste der wichtigsten Veröffentlichungen zu CS/AIX finden Sie im Literaturverzeichnis am Ende dieses Handbuchs.

Informationen zu zusätzlichen Veröffentlichungen erhalten Sie beim zuständigen IBM Ansprechpartner.

## Über das Netz zugängliche Informationen

Zur Förderung des Informationsaustausches sponsert IBM elektronische Foren und Bulletin Boards. IBM unterhält Homepages im Internet und stellt Onlinedokumentationen zur Verfügung, auf die mit CompuServe und 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 CS/AIX, zugreifen. Gezielte Informationen zu CS/AIX finden Sie unter <https://www.ibm.com/products/communications-server-for-data-center>.

Weitere ausführliche Hinweise zur Unterstützung für CS/AIX bietet die Seite <https://www.ibm.com/mysupport/s/topic/0TO0z0000006v3OGAQ/communication-server>.

### Informationen zum Herunterladen

Benutzer können Redbook-Veröffentlichungen aus dem World Wide Web (<http://www.redbooks.ibm.com>) herunterladen.

## Empfohlene Literatur

Im CompuServe-Netz haben Sie über 'APPC Online' Zugriff auf ein breites Spektrum nützlicher Informationen (unter anderem auch auf Programmcode). Verwenden Sie GO APPC.

Informationen zu IBM Software können Sie unter <http://www.ibm.com/software> abrufen. Von dieser Seite aus sind Links zu Seiten für CS/AIX und alle weiteren IBM Softwareserver verfügbar.

### Testsoftware

In einigen Ländern bietet IBM Testsoftware an, die 90 Tage kostenlos genutzt werden kann. Ein solches Angebot gibt es auch für die neueste Version von CS/AIX. Details zur Beschaffung von Testversionen erhalten Sie bei Ihrem IBM Ansprechpartner, oder nutzen Sie die CS/AIX-Seite im World Wide Web (<https://www.ibm.com/products/communications-server-for-data-center>).

## 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 CS/AIX. 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)
- *Verwaltungshandbuch für IBM Communications Server for Data Center Deployment für AIX* (IBM Form SC12-2556)
- *IBM Communications Server for AIX Version 6* (IBM Form SG24-5947)
- *IBM CS/AIX Understanding and Migrating to Version 5: Part 1 - Configuration and New Features* (IBM Form SG24-5215)
- *IBM CS/AIX Understanding and Migrating to Version 5: Part 2 - Performance* (IBM Form SG24-2136)
- Schulungsmaterial für Communications Server for Data Center Deployment unter <https://www.ibm.com/support/pages/node/594013>

Falls Sie weitere Fragen zu spezifischen Fachgebieten haben, überprüfen Sie, ob das Literaturverzeichnis weitere Referenzveröffentlichungen enthält, oder wenden Sie sich an den zuständigen IBM Ansprechpartner.

---

# Appendix A. How to send your comments to IBM

We appreciate your input on our publications. Feel free to comment on the clarity, accuracy, and completeness of the information or provide any other feedback that you have.

Use one of the following methods to send your comments:

1. Use the feedback link at the bottom of Knowledge Center.
2. Use the feedback template below and send us an email at "[mhvrcfs@us.ibm.com](mailto:mhvrcfs@us.ibm.com)"
3. Mail the comments to the following address:

IBM Corporation  
Attention: MHVRCFS Reader's Comments  
Department H6MA, Building 707  
2455 South Road  
Poughkeepsie, NY 12601-5400  
US

## Email feedback template

---

Please cut and paste the template below into your email. Then fill in the required information.

- My name:
- My Company, University or Institution:
- The URL of the topic or web page you are commenting on:
- The text of your comment

If you are willing to talk to us about your comment, please feel free to include a phone number and the best time to reach you.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute the comments in any way appropriate without incurring any obligation to you.

IBM or any other organizations use the personal information that you supply to contact you only about the issues that you submit.

## If you have a technical problem

---

Do not use the feedback methods that are listed for sending reader's comments. Instead, take one of the following actions:

- Contact your IBM service representative
- Call IBM technical support
- Visit the IBM support portal at <https://www.ibm.com/support/home/>.



---

## Appendix B. Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

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

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

- IBM World Trade Asia Corporation
- Licensing
- 2-31 Roppongi 3-chome, Minato-ku
- Tokyo 106, Japan

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:** INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

- IBM Corporation
- P.O. Box 12195
- 3039 Cornwallis Road
- Research Triangle Park, NC 27709-2195
- U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

**COPYRIGHT LICENSE:** This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows: © (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. 2000, 2005, 2006, 2007, 2008, 2021. All rights reserved.

## Trademarks

---

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

- ACF/VTAM
- Advanced Peer-to-Peer Networking
- AIX
- Application System/400
- APPN
- AS/400
- CICS
- DATABASE 2
- DB2
- Enterprise System/3090
- Enterprise System/4381
- Enterprise System/9000
- ES/3090
- ES/9000
- eServer
- IBM
- IBMLink
- IMS
- MVS
- MVS/ESA
- Operating System/2
- Operating System/400
- OS/2
- OS/400
- PowerPC
- PowerPC Architecture
- S/390
- System/390
- System p5
- System z
- System z9
- VSE/ESA
- VTAM
- WebSphere

The following terms are trademarks or registered trademarks of other companies:

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc., in the United States, other countries, or both.

UNIX is a registered trademark in the United States and other countries licensed exclusively through The Open Group.

Intel and EM64T are trademarks of Intel Corporation.

AMD64 is a trademark of Advanced Micro Devices, Inc.

Linux is a trademark of Linus Torvalds.

RedHat and RPM are trademarks of Red Hat, Inc.

SuSE Linux is a trademark of Novell.

Ubuntu is a trademark of Canonical Limited.

Microsoft, Windows, Windows 10, Windows Server 2012, Windows Server 2016, Windows Server 2019 and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.



# Literaturverzeichnis

---

Die folgenden Veröffentlichungen von IBM® enthalten zusätzliche Informationen zu den in diesem Handbuch behandelten Themen. Die Veröffentlichungen sind in folgende Themenbereiche unterteilt:

- CS/AIX Version 7.1
- Redbooks
- Betriebssystem AIX
- 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/AIX-Bibliothek sind Kurzbeschreibungen vorhanden. Für andere Bücher sind hier nur die Titel und Bestellnummern angegeben.

## CS/AIX-Veröffentlichungen

---

Die Bibliothek zu CS/AIX enthält die nachstehend genannten Handbücher. Softcopys dieser Dokumentationen sind auf CD-ROM verfügbar. Informationen zum Aufrufen der Softcopydateien von CD-ROM finden Sie in der Veröffentlichung *Einstieg in IBM Communications Server for Data Center Deployment für AIX*. Für die Installation dieser Softcopyhandbücher benötigen Sie (in Abhängigkeit von den installierten Landessprachen) 9-15 MB Festplattenspeicherplatz.

- *IBM Communications Server for Data Center Deployment on AIX Migration Guide* (IBM Form SC31-8585)

Dieses Handbuch erläutert die Migration von Communications Server for AIX Version 4 Release 2 oder noch älteren Versionen auf CS/AIX Version 6.

- *Einstieg in IBM Communications Server for Data Center Deployment für AIX* (IBM Form GC12-2555)

Dieses Handbuch enthält eine allgemeine Einführung in CS/AIX und Informationen zu unterstützten Netzen und zu Installation, Konfiguration und Betrieb.

- *Verwaltungshandbuch für IBM Communications Server for Data Center Deployment für AIX* (IBM Form SC12-2556)

Dieses Handbuch gibt einen Überblick über SNA und CS/AIX und enthält Informationen zu Konfiguration und Betrieb von CS/AIX.

- *IBM Communications Server for Data Center Deployment on AIX Administration Command Reference* (IBM Form SC31-8587)

Dieses Handbuch enthält Informationen zu SNA- und CS/AIX-Befehlen.

- *IBM Communications Server for Data Center Deployment on AIX or Linux CPI-C Programmer's Guide* (IBM Form SC23-8591)

Dieses Handbuch enthält Informationen für erfahrene C'- oder Java-Programmierer zum Schreiben von SNA-Transaktionsprogrammen mit der CS/AIX-API CPI Communications.

- *IBM Communications Server for Data Center Deployment on AIX or Linux APPC Programmer's Guide* (IBM Form SC23-8592)

Dieses Handbuch enthält die für das Schreiben von Anwendungsprogrammen mit APPC (Advanced Program-to-Program Communication) erforderlichen Informationen.

- *IBM Communications Server for Data Center Deployment on AIX or Linux LUA Programmer's Guide* (IBM Form SC23-8590)

Dieses Handbuch enthält die für das Schreiben von Anwendungen mit der herkömmlichen Anwendungsprogrammierschnittstelle für LU-Anwendungen LUA erforderlichen Informationen.

- *IBM Communications Server for Data Center Deployment on AIX or Linux CSV Programmer's Guide* (IBM Form SC23-8589)

Dieses Handbuch enthält die für das Schreiben von Anwendungsprogrammen mit der API (Anwendungsprogrammierschnittstelle) Common Service Verbs (CSV) erforderlichen Informationen.

- *IBM Communications Server for Data Center Deployment on AIX or Linux MS Programmer's Guide* (IBM Form SC23-8596)

Dieses Handbuch enthält die für das Schreiben von Anwendungen mit der API Management Services (MS) erforderlichen Informationen.

- *IBM Communications Server for Data Center Deployment on AIX NOF Programmer's Guide* (IBM Form SC31-8595)

Dieses Handbuch enthält die für das Schreiben von Anwendungen mit der API Node Operator Facility (NOF) erforderlichen Informationen.

- *IBM Communications Server for Data Center Deployment on AIX Diagnostics Guide* (IBM Form SC31-8588)

Dieses Handbuch enthält Informationen zur Behebung von SNA-Netzfehlern.

- *IBM Communications Server for Data Center Deployment on AIX or Linux APPC Application Suite User's Guide* (IBM Form SC23-8595)

Dieses Handbuch enthält Informationen zu APPC-Anwendungen, die zusammen mit CS/AIX eingesetzt werden können.

- *IBM Communications Server for Data Center Deployment on AIX Glossary* (IBM Form GC31-8589)

Dieses Handbuch enthält eine umfangreiche Liste von Begriffen und Definitionen, die in allen Veröffentlichungen der Bibliothek zu CS/AIX verwendet werden.

## IBM Redbooks

---

IBM unterhält ein internationales Zentrum für technische Unterstützung (International Technical Support Center), dessen Veröffentlichungen als Redbooks bezeichnet werden. Redbooks beschäftigen sich ähnlich wie die Produktdokumentation mit theoretischen und praktischen Aspekten der SNA-Technologie. Sie enthalten jedoch nicht die Informationen, die dem Kunden beim Kauf von Produkten für den Netzbetrieb bereitgestellt werden.

Folgende Bücher enthalten Informationen, die für CS/AIX hilfreich sein können:

- *IBM Communications Server for AIX Version 6* (IBM Form SG24-5947)
- *IBM CS/AIX Understanding and Migrating to Version 5: Part 2 - Performance* (IBM Form SG24-2136)
- *Load Balancing for Communications Servers* (IBM Form SG24-5305)

Benutzer können Redbook-Veröffentlichungen aus dem World Wide Web (<http://www.redbooks.ibm.com>) herunterladen.

## Veröffentlichungen zum Betriebssystem AIX

---

Die aktuelle Dokumentation zu AIX finden Sie im [AIX Knowledge Center](https://www.ibm.com/support/knowledgecenter/ssw_aix) (unter [https://www.ibm.com/support/knowledgecenter/ssw\\_aix](https://www.ibm.com/support/knowledgecenter/ssw_aix)).

## 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)
- *ESCON Director Planning* (IBM Form GA23-0364)

## 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:

- *AIXLink/X.25 for AIX: Guide and Reference* (IBM Form SC23-2520)

- *RS/6000 AIXLink/X.25 Cookbook* (IBM Form SG24-4475)
- *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 CS/AIX:

- *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

3270-LU  
definieren 94  
für TN Server 9, 93

## A

Abfragebefehle 14  
Abhängige LU 6.2 86  
Advanced Interactive Executive (AIX) 1  
Advanced Program-to-Program Communication (APPC) 5  
AIX  
Ausführung von CS/AIX 1  
Hardwarevoraussetzungen für CS/AIX 17  
Man-Pages 27  
Aktivieren einer Ressource 72  
Aktivieren von CS/AIX  
auf dem lokalen System 69  
Alerts 14  
Aliasnamen für Partner-LU definieren 85  
Ändern der Konfiguration 72  
Anforderungen  
Personal und Qualifikation 16  
Angepasste Nachrichtendosierung auf Sitzungsebene 12  
Antwortzeit 21  
Anwendungsprogrammierschnittstelle (API) 3  
Anzeigen der Konfiguration 72  
API  
Arten für CS/AIX 4  
für CS/AIX-Verwaltung 12  
Unterstützung 3  
APPC  
abhängige LU 6.2 86  
Application Suite 5, 8  
Konfiguration 81  
online 99  
unabhängige LU 6.2 83  
Unterstützung für verteilte Anwendungen 5  
APPC Application Suite 8  
APPN  
Anwendungen 5, 8  
DLUR-Unterstützung 2  
dynamische Konfiguration 12  
Endknoten 1  
Hostunterstützung für APPN 1, 2  
Knotentypen 1  
Konfiguration 82, 83  
Netzknoten 1  
Routing 12  
Segmentierung von Netzen 22  
unabhängige LU-Unterstützung 3  
Unterbereichsfunktionen 2  
Verbindungsnetz 12  
verteilter Verwaltungsservice 13  
Arbeitsblätter für Planung 68  
Arbeitsspeicher (RAM) 20

Aufgabenblätter 68  
Aufrufe 3  
Ausweichserver 5, 74

## B

Basisbetriebssystem 18  
Befehlszeilenverwaltungsprogramm 12  
Branch Extender 7

## C

CDE 31  
CICS (Customer Information Control System) 5  
Client 4  
Client-Server-Installation 35  
Client-Server-Unterstützung 4  
Client/Server  
Konfiguration 74  
Clientsoftware  
anpassen 63  
deinstallieren 64  
erneut installieren 63  
Upgrade 63  
comments on publication  
sending feedback 101  
Common Desktop Environment (CDE) 31  
Common Programming Interface for Communications (CPI-C) 4  
Controller-Server 4  
CPI Communications (CPI-C) 4  
CPI-C  
API 4  
Interoperabilität 14  
Konfiguration 86  
Customer Information Control System (CICS) 5

## D

DATABASE 2 (DB2) 5  
Datenstrom 3  
Datenübertragungssteuerung (DLC) 25  
DB2 (DATABASE 2) 5  
DDLU (Dynamic Definition of Dependent LUs) 3  
Deinstallation von Remote API Client für AIX 54  
Deinstallation von Remote API Client für Linux 43  
Deinstallation von Remote API Client für Linux auf System z 49  
Dependent Logical Unit Server (DLUS) 90  
Dependent LU Requester (DLUR) 2  
DFV-Adapter 18  
Dialoganzeige 70  
Diskussionsgruppen, online 99  
DLC  
in einer Port-Konfiguration 76  
Installation 28

DLC (Forts.)  
Konfiguration 78, 79  
Zweck 25  
DLUR  
auf dem lokalen Knoten 91  
Beschreibung 2  
Konfiguration 90  
PU konfigurieren 92  
Unterstützung für untergeordnete Knoten 92  
DLUS 90  
Dokumentation, online 99  
Domäne 4  
Domäne (Parameter) 58  
Dynamische Konfiguration 12  
Dynamisches Definieren abhängiger LUs (DDDLU) 3

## E

Einfache Installation  
mit CDE 31  
mit SMIT 30  
Eingangspunkt 13  
Empfohlene Literatur 100  
Enterprise Extender  
Dialog für Ports 79  
Überblick 8  
Verbindungskonfiguration 79  
Erweiterte Konfigurationen, Speicher- und Hauptspeicherbedarf 19  
Ethernet  
SAP-Dialoganzeige 78  
Verbindungskonfiguration 78

## F

Features 27  
feedback  
email template 101  
sending reader comments 101  
Fehler  
Daten 14  
Diagnosetools 14  
Fehlerbehebungstools 14  
Fenster 70  
Ferner Knoten  
Konfiguration 84  
Partner-LU konfigurieren 85  
Festplattenspeicher 19  
Foren, online 99  
Funktionen 3  
Funktionsanforderungen 15

## G

Gateway  
Definition 6  
SNA Gateway 6  
GSKit  
Remote API Client für AIX 51, 53  
Remote API Client für Linux 40, 42  
Remote API Client für Linux auf System z 45, 48  
Remote API Client für Windows 62

## H

Hardware  
Verbindung 17  
Voraussetzungen 17  
Hardwarevoraussetzungen  
Remote API Client für AIX 51  
Remote API Client für Linux 39  
Remote API Client für Linux auf System z 45  
Remote API Client für Windows 55  
Hauptspeicher 20  
Hilfe  
Motif-Verwaltungsprogramm 11  
Webverwaltungsprogramm 11  
Hinzufügen einer Ressource 72  
Host  
im APPN-Netz 2  
im Unterbereichsnetz 1  
LU-Unterstützung 2  
HPR  
im Vergleich zu ISR 12  
HPR/IP 8  
HTTPS  
konfigurieren 33  
Remote API Client für AIX 53  
Remote API Client für Linux 42  
Remote API Client für Linux auf System z 48  
Remote API Client für Windows 62  
Voraussetzungen 19

## I

Implizite untergeordnete LU konfigurieren 89  
Inaktivieren einer Ressource 72  
Inaktivieren von CS/AIX 98  
Informationsquellen 99  
Installation  
Einzelangaben zu vorhandenen Paketen 28  
manuell 31, 32  
mit Easy Install 30  
Remote API Client für AIX 52, 53  
Remote API Client für Linux 41  
Remote API Client für Linux auf System z 46  
Verwaltung nach der Installation 34  
vorbereiten 28  
Installation von Remote API Client für AIX 52, 53  
Installation von Remote API Client für Linux 41  
Installation von Remote API Client für Linux auf System z 46  
Installationsabschluss, Prozeduren 34  
Installationsvoraussetzungen 17  
Installationsvorbereitungen 28  
Intermediate Session Routing (ISR) 12  
International Organization for Standards (ISO) 22  
IP-Adressformate 21  
IP-Port, Dialog 79  
IPv4-Adresse 21  
IPv6-Adresse 21  
ISO (International Organization for Standards) 22  
ISR (Intermediate Session Routing) 12

## J

Java

## Java (Forts.)

- Remote API Client für AIX 51
- Remote API Client für Linux 40
- Remote API Client für Linux auf System z 45

## K

### Knoten

- fern 84
- Hostkommunikation 75
- in einer APPN-Konfiguration 75
- Konfiguration 74
- lokal 91
- übergeordnet 90
- untergeordnet 92

### Knoten für Low-Entry Networking (LEN-Knoten) 78

### Knotenfenster 70

### Kompatibilitätsplanung 22

### Komponentenverwaltung 70

### Komprimierung von LU-Sitzungsdaten 3

### Konfiguration

- ändern 72
- anzeigen 72
- APPC-Kommunikation 81
- Beispiele 74, 75, 90, 92
- CPI-C-Nebeninformationen 86
- Dateien 36, 37
- DLUR 90
- ferner Knoten 84
- implizite untergeordnete LU 89
- Knoten 74
- Konnektivität 76
- LU 6.2 83, 86
- LU-Typen 0-3 79
- Partner-LUs für einen LEN-Knoten 84
- Planung 68
- Port 77
- sichern 36

### Standardeinstellungen für TN Redirector 97

### TN-Server-Standardeinstellungen 96

### TN-Server-Zuordnungseinträge 96

### untergeordnete LUs für SNA Gateway 87

### Konfigurationsfenster für Remote API Client für Windows

#### erweiterte Parameter 59

#### Parameter 57

### Konfigurationsserver

- entfernen 74
- hinzufügen 74

### Konnektivität

- Konfiguration 76
- Optionen 2

## L

### LAN (Local Area Network) 2

### LEN-Knoten

- Beschreibung 1
- fernen Knoten identifizieren 78
- Partner-LU konfigurieren 84

### Lizenzierungsmechanismen 25

### Lizenzprogramm

- Remote API Client für AIX 52
- Remote API Client für Linux 41

### Lizenzprogramm (Forts.)

#### Remote API Client für Linux auf System z 46

#### Lizenzprogrammpaket (LPP) 26

#### Logische Einheit (LU) 2, 89

#### Lokale LU definieren 83

#### Lokales Netz (LAN) 2

#### Löschen einer Ressource 72

#### LPP (Lizenzprogrammpaket) 26

#### LU

##### Konfiguration 83, 86, 94

##### Namenskonventionen 23

##### Partner-LU definieren 84

##### Pool 94, 95

##### untergeordnet 88, 89

##### Unterstützung 2

#### LU-Pool

##### anzeigen 81

##### definieren 80

##### Konfiguration 80

#### LU-Typen 0-3 79, 80

## M

### MAC (Medium Access Control) 78

### Man-Pages 27

### Manageranwendung 13

### Manuelle Installation 31

### Maximale Broadcast-Versuche (Parameter) 59

### mbufs (Speicherpuffer) 20

### MDS-NMVT (Multiple Domain Support - Network Management Vector Transport) 13

### Medium Access Control (MAC) 78

### Mehrere Server in einer Domäne 4

### Migration für frühere Versionen von CS/AIX 29

### Motif-Verwaltungsprogramm

#### Beschreibung 11

#### Hilfe 11

#### Verwaltungsfähigkeit 14

#### verwenden 67

### MPQP (Multiprotocol Quad Port) 17

### Multiple Domain Support - Network Management Vector

### Transport (MDS-NMVT) 13

### Multiprotocol Quad Port (MPQP) 17

## N

### Nachrichtendosierung auf Sitzungsebene 12

### Namenskonventionen 22

### Network Installation Management 32

### Netz

#### Alerts 14

#### Namenskonventionen 22

#### Peer-zu-Peer 1

#### Planung 15, 16, 22

#### über das Netz verfügbare Informationen 99

#### Unterbereichsnetz 1

#### Unterstützung 1

#### Verwaltung 13

### NIM (Network Installation Management) 32

### Node-Lock-Lizenzen 25

### NOF (API) 12

## O

### Online

- APPC 99
- Diskussionsgruppen 99
- Dokumentation 99
- Foren 99
- Hilfe 11

- Open Systems Interconnection (OSI) 22
- Optionen für Datenübertragungssteuerung 2
- OSI (Open Systems Interconnection) 22

## P

### Partner-LU

- Aliasname 85
- auf fernem Knoten 85
- Konfiguration 84
- mit Platzhaltern definieren 85

### Partneranwendungen

- 5
- PDF, Handbücher anzeigen 35

### Peer

- Netz 1
- Peerserver 5
- Personalanforderungen 16
- Pfad für ausführbare CS/AIX-Programme 69
- Physische Einheit (PU) 6
- Planungsblätter 68
- Plattenspeicher 20
- Platzhalter 85
- Port-Konfiguration 77–79
- Primärer Speicher 20
- Primary RUI 3
- Prozeduren
  - Remote API Client für Windows installieren 56, 59
- PTFs (Program Temporary Fixes) 28
- PU (Physical Unit) 6
- PU-Konzentration 87
- PU-Konzentrator 6

## Q

### Qualifikationsanforderungen

- 16
- methods of sending feedback 101

### Releaseinformationen

- 35
- Remote API Client
  - AIX-Hardwarevoraussetzungen 51
  - Hardwarevoraussetzungen für Linux auf System z 45
  - Linux-Hardwarevoraussetzungen 39
  - Softwarevoraussetzungen für AIX 51
  - Softwarevoraussetzungen für Linux 39
  - Softwarevoraussetzungen für Linux auf System z 45

- Remote API Client für Linux
  - Einzelangaben zu vorhandenen Paketen 40
- Remote API Client für Linux auf System z
  - Einzelangaben zu vorhandenen Paketen 45
- Remote API Client für Windows

### Remote API Client für Windows (Forts.)

- installieren 55
- mit dem Setup-Programm installieren 56
- von der Befehlszeile aus installieren 59

### Ressource

- aktivieren 72
- Anforderungen 16
- definieren 72
- Einträge 73
- inaktivieren 72
- Informationen 99
- löschen 72
- Verwaltung 70

### RS/6000-Workstations

## S

### SAA (Systemanwendungsarchitektur)

- 4
- Sammelpunkt 13
- SAP (Service Access Point) 17, 78
- Schaltflächen in Ressourcenfenstern 73
- Schnittstellenauswahl 12

### SDK-Software

- Remote API Client für Windows 55

### SDLC

- für abhängigen Datenverkehr 77
- Konfiguration 77

### Secure Sockets Layer (SSL)

- Clientauthentifizierung 96, 97
- Datenverschlüsselung 35, 96, 97
- Serverauthentifizierung 35, 96, 97

### Seitenwechselspeicher

### Server

- entfernen 74
- hinzufügen 74

### Server, Telnet

### Servername

### Service Access Point (SAP)

### Servicezugriffspunkt

### Sicherheitsoptionen

### Sichern

- Konfigurationsdateien 36

### Sicherung

- zurückschreiben 37

### Simple Network Management Protocol-Management Information Base (SNMP-MIB)

### Sitzung

- Nachrichtendosierung 12
- Routing 12
- U-förmig 3
- Unterstützung 3

### SMIT

- DLC-Konfiguration 25
- einfache Installation 30
- manuelle Installation 31

### SMIT (System Management Interface Tool)

### SNA

- Bibliothek 99

### SNA Gateway

- Konfiguration 87

- Überblick 6

### snaadmin (Programm)

### SNMP-Agent

SNMP-MIB (Simple Network Management Protocol-Management Information Base) [13](#)

Softwarefeatures [5](#)

Softwarevoraussetzungen

  Remote API Client für AIX [51](#)

  Remote API Client für Linux [39](#)

  Remote API Client für Linux auf System z [45](#)

  Remote API Client für Windows [55](#)

Speicherbedarf

  erweiterte Konfigurationen [19](#)

  Speicherarten [20](#)

Speicherpuffer (mbufs) [20](#)

Sprachumgebungvariable

  Remote API Client für Linux [40](#)

  Remote API Client für Linux auf System z [46](#)

start (Befehl) [69](#)

Starten von CS/AIX

  automatisch beim Systemstart [70](#)

Statusbefehle [14](#)

Steuerung für synchrone Datenübertragung (SDLC) [77](#)

stop (Befehl) [98](#)

Symbolleistungsschaltflächen [73](#)

System Management Interface Tool (SMIT) [12, 17, 25](#)

Systemanwendungsarchitektur (SAA) [4](#)

## T

technical problems

  methods of resolving [101](#)

TN Redirector

  Konfiguration [97](#)

  Standardeinstellungen konfigurieren [97](#)

  Überblick [10](#)

  Zugriffseintrag konfigurieren [97](#)

TN Server

  Benutzer [93](#)

  Konfiguration [92](#)

  Standardeinstellungen konfigurieren [96](#)

  Überblick [8](#)

  Unterstützung für mehrere Sitzungen [94](#)

  Zugriffseintrag konfigurieren [96](#)

  Zuordnungseinträge konfigurieren [96](#)

TN3270

  Programme [8](#)

  Server [8](#)

TN3270-Benutzer [9, 93](#)

TN3270-Programme [92](#)

TP (transaction program) [3](#)

Transaktionsprogramm [3](#)

Transparenz zwischen lokalem und fernem Sitzungspartner [3](#)

## U

U-förmige Sitzungen [3](#)

Übergeordneter Knoten [90](#)

Übertragungsmedien [17](#)

Unabhängige LU 6.2 konfigurieren [83](#)

Untergeordnete LU

  für SNA Gateway [87](#)

  Hardwarebeispiele [88](#)

  Konfiguration [89](#)

Untergeordneter Computer [88](#)

Unterroutinen [3](#)

Utergeordneter Knoten [90](#)

## V

Verben [3](#)

Verbindungshardware [17](#)

Verbindungsnetz [12](#)

Verbindungsnetz, Konfiguration [78](#)

Verbindungsstation

  für Port definieren [77](#)

Version der IP-Adresse [21](#)

Verteilte Verarbeitung

  Anwendungsunterstützung [5](#)

  Umgebung [1](#)

Verwaltungsprogramm

  API NOF [12](#)

  Befehlszeile [12](#)

  Motif [11, 14](#)

  SMIT [12](#)

  Web [11](#)

Verzeichnis für ausführbare CS/AIX-Programme [69](#)

Voraussetzungen

  Hardware [17](#)

  Hauptspeicher und Speicher [19](#)

  HTTPS [19](#)

  Installation [17](#)

  Software [18](#)

  WebSphere Application Server [19](#)

Vorläufige Programmkorrekturen (PTFs) [28](#)

## W

WAN (Wide Area Network) [2](#)

WebSphere Application Server

  konfigurieren [33](#)

  Voraussetzungen [19](#)

Webverwaltungsprogramm

  Beschreibung [11](#)

  Hilfe [11](#)

Weitverkehrsnetz (WAN) [2](#)

Workstation

  Voraussetzungen [17](#)

## X

xsnaadmin (Programm) [11, 67](#)

## Z

Zeitlimit für LAN-Zugriff (Parameter) [59](#)

Zeitlimit für Verbindungswiederherstellung (Parameter) [59](#)

Zweignetzknoten [7](#)





IBM.®

GC12-3653-06

