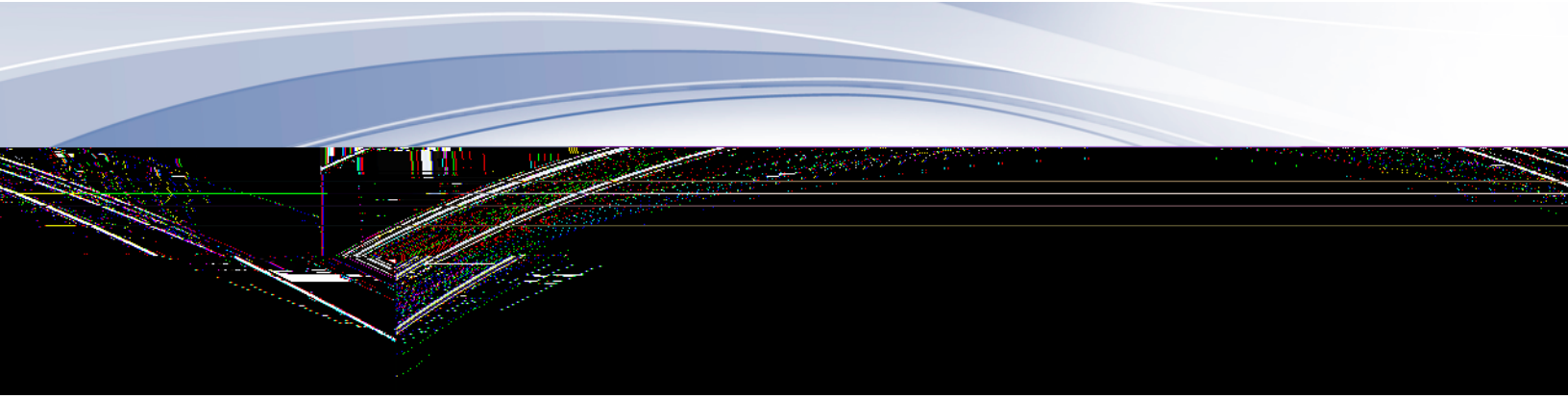
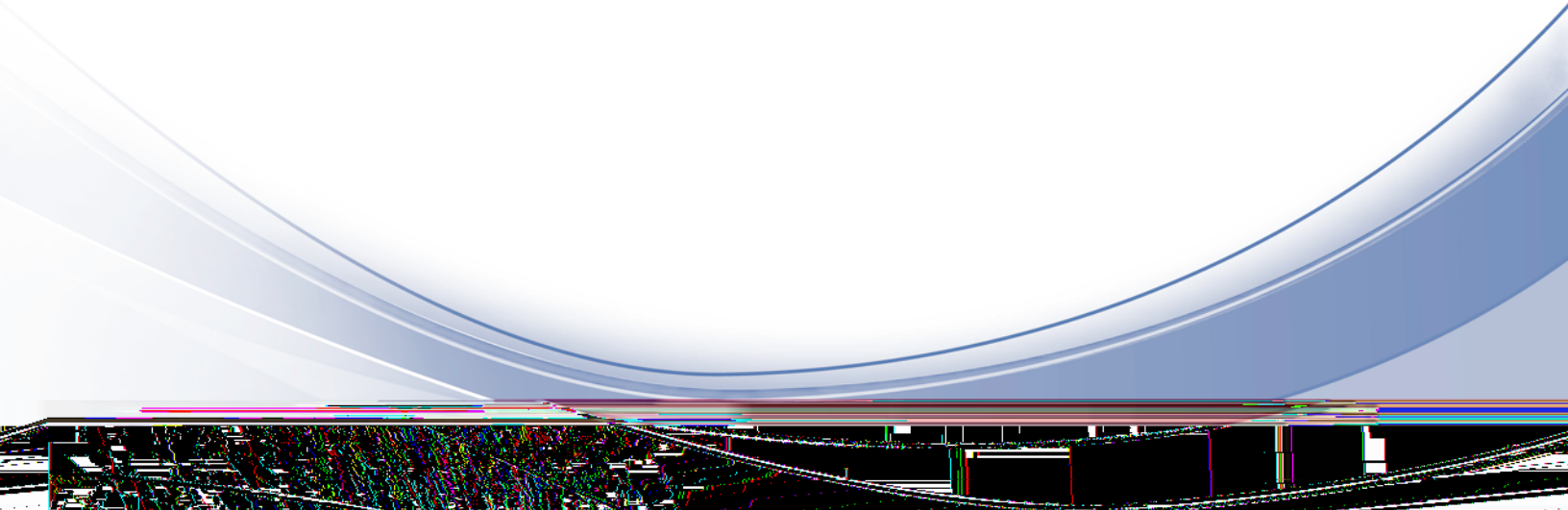


IBM Communications Server for Data Center Deployment für Linux auf System z 7.1

Einstieg



Note

Before using this information and the product it supports, be sure to read the general information under Appendix B, “Notices,” on page 101.

Siebente Ausgabe (Januar 2021)

Diese Ausgabe bezieht sich auf IBM Communications Server for Data Center Deployment für Linux 7.1, Programmnummer 5725-H32, und, sofern in neuen Ausgaben oder TNLs 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.

© Copyright International Business Machines Corporation 1998, 2021.

Inhaltsverzeichnis

Tabellen ..... **vii**

Abbildungsverzeichnis ..... **ix**

Willkommen bei IBM Communications Server for Data Center Deployment für Linux ..... **xi**
Benutzung des Handbuchs xi
Orientierungshilfe xi
Typografische Konventionen xii
Verwendete Abkürzungen xii
Neuerungen xiii
Neue Funktionen xiv
Gesperrte Funktionen xiv
Informationsquellen xiv

Kapitel 1. Über IBM Communications Server for Data Center Deployment für Linux **1**
IBM Communications Server for Data Center Deployment für Linux - Features und Programmpakete 1
IBM Communications Server for Data Center Deployment für Linux 1
Erweiterte Netzfeatures 6
Features und Vorteile 11
Vielseitige Bausteine 11
Client-Server-Betrieb 11
Problemlose Konfiguration 12
Zusätzliche Schnittstellenoptionen für Verwaltung 12
Verbesserte Leistung 13
Sicherheitsoptionen 13
Flexible Netzverwaltung 13
Zuverlässigkeit, Verfügbarkeit und Wartungsfreundlichkeit 14
Netzintegration, Wachstum und Veränderungen 14

Kapitel 2. Netz mit CS Linux auf System z planen **17**
Schritte bei der Netzplanung 17
Funktionsanforderungen für das Netz 17
Konfiguration von CS Linux planen 18
Ressourcenanforderungen für Installation und Betrieb 18
IPV4- und IPV6-Adressen 21
Firewall für den Datenverkehr von Enterprise Extender, Client/Server und TN3270 Server konfigurieren 22
Namenskonventionen 23

Kapitel 3. CS Linux auf Linux-Servern installieren **25**
Lizenzierung und Konfektionierung von CS Linux 25
Mechanismen der Lizenzierung für CS Linux 25
Angebotene CS-Linux-Lizenzprogrammpakete 25
Installation von CS Linux vorbereiten 26
Vorausgesetzte Software installieren 26
Details der Produktinstallation anzeigen 26

Sprachumgebungsvariable ändern....27
Vorversionen von CS Linux migrieren....27
Hinweise....27
Migrationsprozess....28
Lizenzprogramm CS Linux installieren....29
CS Linux installieren....29
Onlinedokumentation zu CS Linux....31
WebSphere Application Server konfigurieren....31
Sicherheitszertifikat für WebSphere Application Server konfigurieren....31
WebSphere Application Server konfigurieren....32
Serverkonfigurationsdatei installieren....32
Prozeduren für den Installationsabschluss....33
Client-Server-Betrieb....33
Bereinigung nach der Installation....33
PDF-Handbücher anzeigen....33
Aktuelle Releaseinformationen....33
SSL für die Verwendung mit TN Server oder TN Redirector konfigurieren....33
Konfigurationsdateien von CS Linux sichern....34
Sicherungskopie der Konfigurationsdateien von CS Linux zurückschreiben....34
Konfigurationsdateien reinitialisieren....35
CS Linux deinstallieren....36

Kapitel 4. IBM Remote API Clients unter Linux installieren....37
Hardware- und Softwarevoraussetzungen....37
Hardwarevoraussetzungen....37
Version des Betriebssystems Linux....37
Java....38
GSKit....38
Details der Produktinstallation anzeigen....38
Umgebungsvariablen für CS Linux definieren....38
Sprachumgebungsvariable setzen....38
Remote API Client für Linux installieren....39
HTTPS-Sicherheitszertifikate mit dem GSKit konfigurieren....40
Remote API Client für Linux deinstallieren....41

Kapitel 5. IBM Remote API Clients für Linux auf System z installieren....43
Hardware- und Softwarevoraussetzungen....43
Hardwarevoraussetzungen....43
Version des Betriebssystems Linux....43
Java....43
GSKit....43
Details der Produktinstallation anzeigen....43
Umgebungsvariablen für CS Linux definieren....44
Sprachumgebungsvariable setzen....44
Remote API Client für Linux auf System z installieren....44
HTTPS-Sicherheitszertifikate mit dem GSKit konfigurieren....46
Remote API Client für Linux auf System z deinstallieren....47

Kapitel 6. IBM Remote API Clients unter AIX installieren....49
Hardware- und Softwarevoraussetzungen....49
Hardwarevoraussetzungen....49
Betriebssystemversion....49
Java....49
GSKit....49
Umgebungsvariablen für CS Linux definieren....49
Sprachumgebungsvariable ändern....50
Remote API Client für AIX installieren....50

Dateien für die Installation von Remote API Client auf die AIX-Workstation kopieren..... 50
Remote API Client von der CD installieren..... 51
HTTPS-Sicherheitszertifikate mit dem GSKit konfigurieren..... 51
Remote API Client für AIX deinstallieren..... 52

Kapitel 7. Installation von Remote API Client für Windows planen und ausführen..... 53
Hardware- und Softwarevoraussetzungen..... 53
Zugriff auf das Setup-Programm..... 53
Remote API Client mit dem Setup-Programm unter Windows installieren..... 54
Erweiterte Optionen für die Konfiguration von Remote API Client..... 57
Remote API Client über die Befehlszeile installieren..... 57
HTTPS-Sicherheitszertifikate mit dem GSKit konfigurieren..... 60
Remote API Client nach der installation anpassen..... 61
Software Remote API Client erneut installieren..... 61
Remote API Client deinstallieren..... 62
Remote API Client über die Befehlszeile deinstallieren..... 62
Hilfe..... 63

Kapitel 8. CS Linux konfigurieren und verwenden..... 65
CS-Linux-Konfiguration planen..... 66
Planungsblätter..... 66
Aufgabenblätter..... 66
Umgebungsvariablen für CS Linux definieren..... 67
Motif-Verwaltungsprogramm verwenden..... 67
Pfad zu CS-Linux-Programmen angeben..... 67
CS Linux aktivieren..... 67
CS Linux mit dem Motif-Verwaltungsprogramm verwalten..... 68
Client-Server-Funktionen konfigurieren..... 72
Knoten konfigurieren..... 73
Konnektivität konfigurieren..... 73
SDLC-Verbindung für abhängigen Datenverkehr konfigurieren..... 74
Ethernet-Verbindung für die Unterstützung von abhängigem und unabhängigem Datenverkehr konfigurieren..... 75
Enterprise-Extender-Verbindung konfigurieren..... 76
LUs der Typen 0-3 konfigurieren..... 77
LUs der Typen 0-3 definieren..... 77
LU-Pool definieren..... 78
APPC-Kommunikation konfigurieren..... 78
Einfaches APPN-Netz konfigurieren..... 79
Abhängiges APPC konfigurieren..... 83
Konfiguration für CPI Communications..... 84
LUA konfigurieren..... 84
LU-Pool definieren..... 85
SNA Gateway konfigurieren..... 86
Implizite untergeordnete LUs unterstützen..... 87
Untergeordnete LUs definieren..... 87
DLUR konfigurieren..... 88
DLUR-Unterstützung auf dem lokalen Knoten konfigurieren..... 89
Durchgriff-DLUR-Unterstützung für untergeordnete Knoten konfigurieren..... 90
TN Server konfigurieren..... 90
3270-LUs definieren..... 91
LU-Pool definieren..... 92
TN3270 Server konfigurieren..... 92
TN Redirector konfigurieren..... 94
TN Redirector konfigurieren..... 94
CS Linux inaktivieren..... 95

Automatischer Start von CS Linux ... 95
CS Linux aktivieren ... 95
Initialisieren des SNA-Knotens ... 95
Ports und Verbindungsstationen aktivieren ... 96
CS Linux beim Warmstart starten ... 96

Kapitel 9. Informationsquellen für CS Linux und SNA ... 97
SNA-Bibliothek ... 97
Über das Netz zugängliche Informationen ... 97
Empfohlene Literatur ... 98

Anhang A. How to send your comments to IBM ... 99
Email feedback template ... 99
If you have a technical problem ... 99

Anhang B. Notices ... 101
Trademarks ... 102

Literaturverzeichnis ... 105
Veröffentlichungen zu CS Linux 7.1 ... 105
Veröffentlichungen zur Systemnetzwerkarchitektur (SNA) ... 106
Veröffentlichungen zur Hostkonfiguration ... 106
Veröffentlichungen zu z/OS Communications Server ... 107
Veröffentlichungen zu TCP/IP ... 107
Veröffentlichungen zu X.25 ... 107
Veröffentlichungen zu APPC ... 107
Veröffentlichungen zur Programmierung ... 107
Veröffentlichungen zu anderen IBM Produkten für den Netzbetrieb ... 107

Index ... 109

Tabellen

1. Orientierungshilfe für den Einstieg..... xi

2. Typografische Konventionen..... xii

Willkommen bei IBM Communications Server for Data Center Deployment für Linux

Das vorliegende Handbuch gibt eine Einführung in das Softwareprodukt IBM Communications Server for Data Center Deployment für Linux auf System z (CS Linux), Lizenzprogrammnummer 5725-H32, mit dessen Hilfe ein Linux-Computer Daten mit anderen Knoten in einem SNA-Netz (Systemnetzwerkarchitektur) austauschen kann.

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

CS Linux
CS Linux kann auf den folgenden Computern ausgeführt werden:

- 64-Bit-AMD64- bzw. -Intel-EM64T-Workstations mit Linux (x86_64)
- IBM Power-Computer mit Linux (ppc64le)

CS Linux für System z
CS Linux für System z kann auf System-z-Großrechnern mit Linux für System z (s390x) betrieben werden.

Das Handbuch *Einstieg in IBM Communications Server for Data Center Deployment für Linux* gibt es in zwei verschiedenen Versionen, jeweils eine für jede der beiden Installationsvarianten. Vergewissern Sie sich, dass Ihnen die richtige Version dieses Handbuchs für Ihre Installation von CS Linux vorliegt. Das vorliegende Handbuch gilt für CS Linux auf System z.

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

Benutzung des Handbuchs

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

Orientierungshilfe

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

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

Tabelle 1. Orientierungshilfe für den Einstieg

Sie möchten ...	Lesen Sie ...
sich über CS Linux informieren	Kapitel 1, „Über IBM Communications Server for Data Center Deployment für Linux", auf Seite 1
die Verwendung von CS Linux in Ihrem Netz planen	Kapitel 2, „Netz mit CS Linux auf System z planen", auf Seite 17
CS Linux auf Linux-Servern installieren	Kapitel 3, „CS Linux auf Linux-Servern installieren", auf Seite 25

© Copyright IBM Corp. 1998, 2021

Tabelle 1. Orientierungshilfe für den Einstieg (Forts.)

Sie möchten ...	Lesen Sie ...
Remote API Clients für Linux (Intel (32 Bit), Intel/AMD (64 Bit) oder pSeries) installieren	Kapitel 4, „IBM Remote API Clients unter Linux installieren", auf Seite 37
Remote API Clients für Linux auf System z installieren	Kapitel 5, „IBM Remote API Clients für Linux auf System z installieren", auf Seite 43
Remote API Clients unter AIX installieren	Kapitel 6, „IBM Remote API Clients unter AIX installieren", auf Seite 49
Remote API Clients unter Windows installieren	Kapitel 7, „Installation von Remote API Client für Windows planen und ausführen", auf Seite 53
CS Linux konfigurieren	Kapitel 8, „CS Linux konfigurieren und verwenden", auf Seite 65
Hinweise zur Dokumentation für CS Linux und zu anderen Publikationen, einschließlich Onlineinformationen, erhalten	Kapitel 9, „Informationsquellen für CS Linux und SNA", auf Seite 97
die Bemerkungen und Informationen zu Marken lesen	Anhang B, „Notices", auf Seite 101

Typografische Konventionen

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

Tabelle 2. Typografische Konventionen

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

Verwendete Abkürzungen

Im vorliegenden Handbuch werden die folgenden Abkürzungen verwendet:

AIX	Advanced Interactive Executive
API	Application Programming Interface (Anwendungsprogrammierschnittstelle)
APPC	Advanced Program-to-Program Communication
APPN	Advanced Peer-to-Peer Networking
ZNK	Zweignetzknoten
COS	Class of Service (Serviceklasse)
CPI-C	Common Programming Interface for Communications

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

Neuerungen

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

Neue Funktionen

In diesem Release wurde CS Linux um folgende Funktionen erweitert:

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

  Das Überwachungsprogramm für Windows-Clients `sxclappl.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.
- Möglickeit 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.
- Unterstützung für die Ubuntu-Versionen von Linux.

  Das Produkt kann jetzt neben Red Hat Enterprise Linux und SUSE Linux Enterprise Server auch mit Ubuntu Linux verwendet werden. Informationen zur aktuellen Betriebssystemunterstützung finden Sie in der README-Datei.

Gesperrte Funktionen

In diesem Release wurden keine Funktionen gesperrt.

Informationsquellen

Im Literaturverzeichnis sind weitere Bücher aus der Bibliothek zu CS Linux sowie Bücher mit Zusatzinformationen zu SNA und anderen zugehörigen Produkten angegeben.

Kapitel 1. Über IBM Communications Server for Data Center Deployment für Linux

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

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

CS Linux ist eine DFV-Software, die unter dem Betriebssystem Linux ausgeführt wird. Zum Lieferumfang der Software gehören die in den Abschnitten „IBM Communications Server for Data Center Deployment für Linux" auf Seite 1 und „Erweiterte Netzfeatures" auf Seite 6 beschriebenen Features.

CS Linux auf System z ist eine Lösung zur Konsolidierung Ihrer Server und Vereinfachung Ihrer Netze.

- Server können mit der System-z-Technologie, die Vorzüge wie die gemeinsame Benutzung von Prozessoren und Speicher durch virtuelle Server bietet, auf einer Plattform konsolidiert werden.
- Duale SNA- und IP-Netze können auf reine IP-Netze zurückgeführt werden, sodass der SNA-Datenverkehr über ein IP-Netz zu CS Linux auf System z transportiert, dort zurück in SNA konvertiert und über eine Schnittstelle mit hoher Zuverlässigkeit und Sicherheit an CS für z/OS gesendet werden kann. Ein weiterer Vorteil dieser Netzvereinfachung besteht darin, dass das Know-how zu SNA nur an einer zentralen Stelle erforderlich ist.

IBM Communications Server for Data Center Deployment für Linux

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

Die Kommunikation von CS Linux mit einem SNA-Host kann auf die unterschiedlichsten Arten erfolgen. Abbildung 1 auf Seite 2 zeigt zwei Beispiele für die Implementierung von CS Linux:

- Im ersten Beispiel ist CS Linux auf einem separaten z800-System installiert, um das z/OS-Hauptsystem zu entlasten. Die beiden Systeme sind über eine Enterprise-Extender-Verbindung mit IP oder eine LLC2-Verbindung miteinander verbunden.
- Im zweiten Beispiel ist CS Linux auf VMs oder LPARs des z/OS-Hauptsystems installiert. Obwohl CS Linux und Communications Server für z/OS auf demselben Großrechner installiert sind, stellen beide Produkte gesonderte SNA-Knoten dar. Deshalb ist auch hier eine Enterprise-Extender-Verbindung mit HyperSockets IP oder eine LLC2-Verbindung zwischen beiden Knoten erforderlich.

© Copyright IBM Corp. 1998, 2021

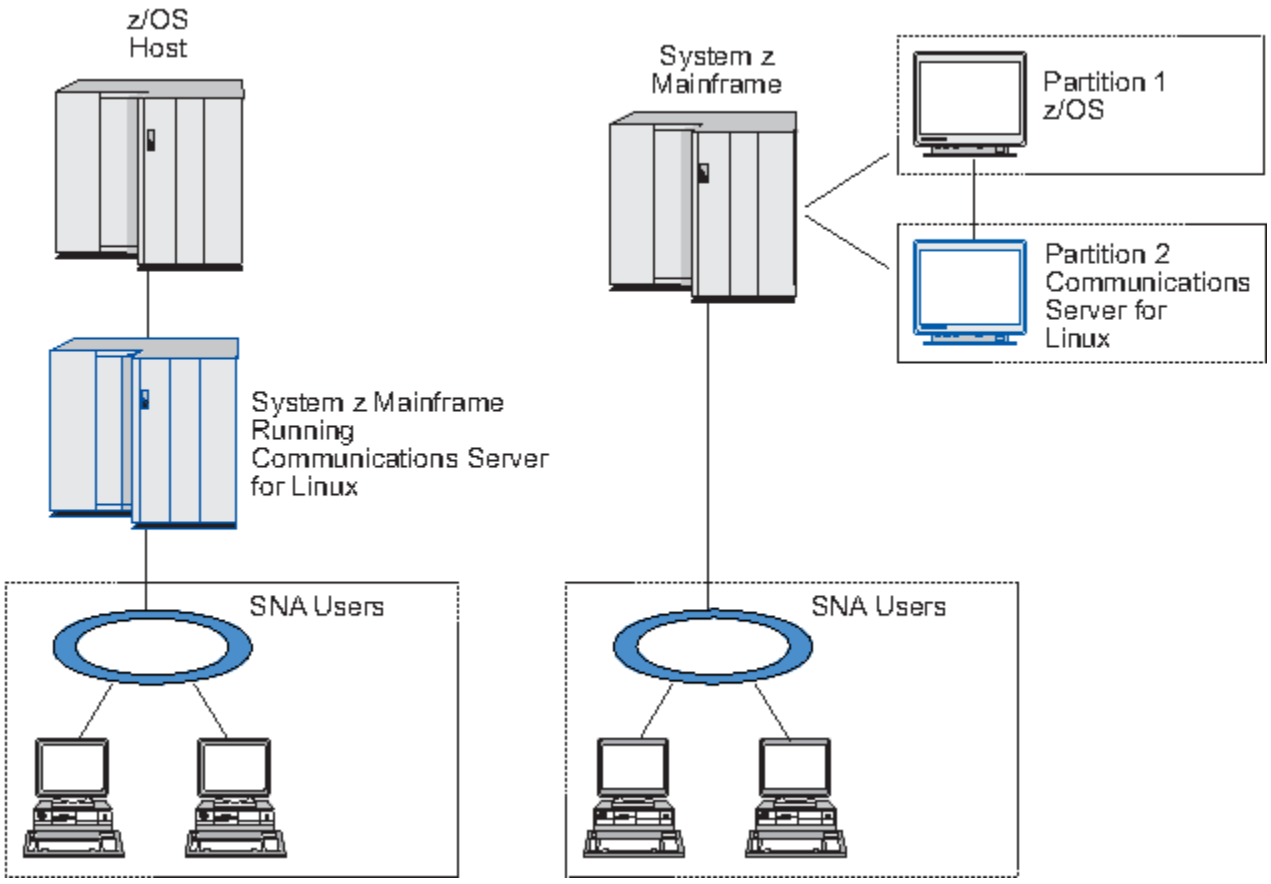


Abbildung 1. Hostkommunikation von CS Linux auf System z

Die beiden dargestellten Konfigurationen sind konzeptionell identisch; für beide ist die gleiche CS-Linux-Konfigurationen erforderlich (einschließlich der Kommunikationsverbindung zwischen CS Linux und dem SNA-Host). Aus Gründen der Anschaulichkeit zeigen die Abbildungen in diesem Handbuch die erste Konfiguration, bei der sich CS Linux und der SNA-Host auf verschiedenen Computern befinden.

CS Linux stellt die folgenden Dienste bereit:

Netzunterstützung

CS Linux unterstützt Unterbereichsnetze und Peer-zu-Peer-Netze:

SNA-Unterbereichsnetze

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

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

Peer-zu-Peer-Netze

In verteilten Verarbeitungsumgebungenunterstützt CS Linux APPN-Netze. In diesen Peer-zu-Peer-Netzen nehmen Linux-Computer ihre Verarbeitungsfunktion wahr und kommunizieren direkt als Peers miteinander.

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:

dem Host konfiguriert werden. (Abhängige LUs auf dem CS-Linux-Knoten müssen dennoch definiert werden.) Auf diese Weise wird der Aufwand für die Erstkonfiguration auf dem Host verringert und eine spätere Erweiterung vereinfacht.

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

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

  Die DLUR-Funktion von CS Linux gestattet darüber hinaus den Transport des Datenverkehrs von abhängigen LUs über ein APPN-Netz.
- Mit der Primary-RUI-Unterstützung kann eine CS-Linux-Anwendung untergeordnete abhängige LU-Einheiten, die 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 Linux kann Tausende von Sitzungen unterstützen. CS Linux 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 Linux-Computer befinden. Dadurch können Sie ein Paar aus Quellen- und Zieltransaktionsprogranörm P •PP ehomund N3 tels de dene werbindung vt3-1 sdimäer erden. um die adforderlichenllnd bentenzu ü er• M ur UHUsass D8yönnen Sie ei CS Linux gv

teme 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 Linux auch eine CPI-C-Anwendungsprogrammierschnittstelle für Java 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 Handbüchern zu CS Linux auch auf CPI-C für Java.

Weitere CS-Linux-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 Linux sind außerdem die folgenden proprietären Programmierschnittstellen enthalten:

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

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

Client-Server-Unterstützung

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

Computer mit CS Linux können in einer Client-Server-Konfiguration die folgenden Aufgabenbereiche übernehmen:

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

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

In einer Domäne mit mehreren CS-Linux-Servern befindet sich auf einem Server die Controllerkopie der Konfigurationsdatei für die CS-Linux-Domäne. Dieser Server ist der Controller-Server. Andere Server in der Domäne können als Ausweichserver definiert werden oder Peer-Server bleiben. Die Domänenkonfigurationsdatei wird auf die Ausweichserver kopiert, wenn diese gestartet werden oder wenn sich die 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 Linux kooperieren die auf Remote API Clients ausgeführten Anwendungen für die Ausführung einer Task mit Konnektivitätsressourcen auf Servern. Anwendungen, die auf anderen Computern (ohne CS Linux) ausgeführt werden, können für die verteilte Verarbeitung ebenfalls mit Anwendungen auf CS-Linux-Computern kooperieren.

CS Linux unterstützt verteilte Anwendungen mittels APPC (auch bekannt als LU 6.2).

Erweiterte Netzfeatures

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

- SNA Gateway verbindet LANs mit SNA-Unterbereichsnetzen.
- Durch die Unterstützung für primäre LUs können untergeordnete abhängige LU-Einheiten wie von einer Großrechneranwendung (Hostanwendung) gesteuert werden.
- Branch Extender vereinfacht große APPN-Netze durch Auslagerung von Ressourcen an verschiedene Standorte (z. B. an unterschiedliche Zweigstellen einer großen Organisation). Dadurch wird die Anzahl der zu speichernden Topologiedaten reduziert, die Möglichkeit der effizienten Lokalisierung von Ressourcen jedoch nicht eingeschränkt.
- APPC Application Suite stellt ausgewählte Anwendungen für APPN-Netze bereit.
- Enterprise Extender (EE, auch bekannt als HPR/IP) ermöglicht den Transport von SNA-Datenverkehr in unveränderter Form über IP-Netze.
- TN Server bietet über SNA Hostzugriff auf TN3270- und TN3270E-Clients, die unter der Bezeichnung TN3270-Clients zusammengefasst werden.
- TN Redirector 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 Netzadaptern und Betriebssystemen konzentrieren sich auf IP-Netz-Funktionen. CS Linux 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 Netzkonnektivität 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-Linux-Computer als Gateway fungieren, das mehrere untergeordnete Computer in einem SNA-Netz mit einer oder mehreren Host-PUs verbindet (siehe Abbildung 2 auf Seite 7). 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 2. Verbindung mehrerer untergeordneter Linux-Computer mit einem Host über SNA Gateway

Unterstützung für primäre LU

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

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

Für die Verwendung von 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 3 auf Seite 8 dargestellte APPN-Feature Branch Extender bietet eine Lösung für diese Probleme an.

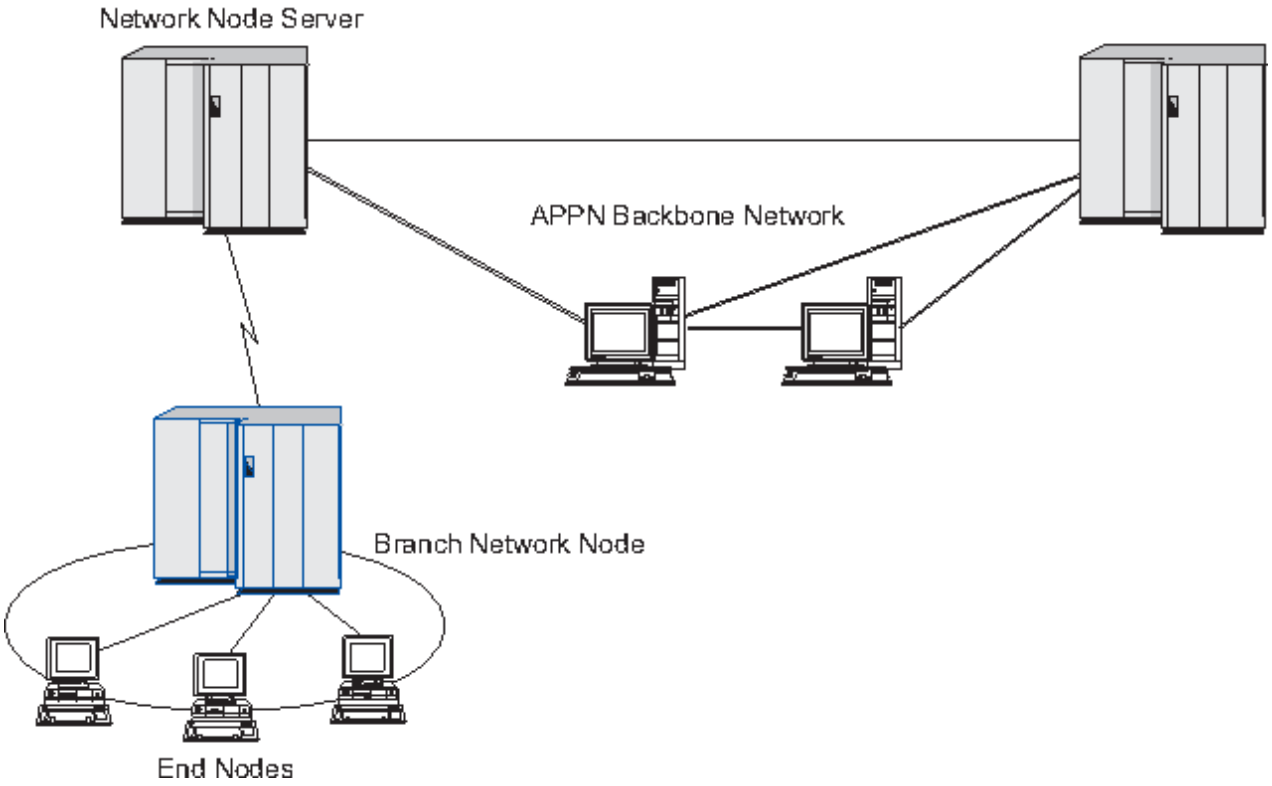


Abbildung 3. Branch Extender

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

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

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

APPC Application Suite

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

Zur APPC Application Suite gehören die folgenden Anwendungen:

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

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

Enterprise Extender

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

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

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

TN Server

3270-Emulationsprogramme, die über TCP/IP 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.

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

Die Funktion TN Server von CS Linux ist in Abbildung 4 auf Seite 10 veranschaulicht.

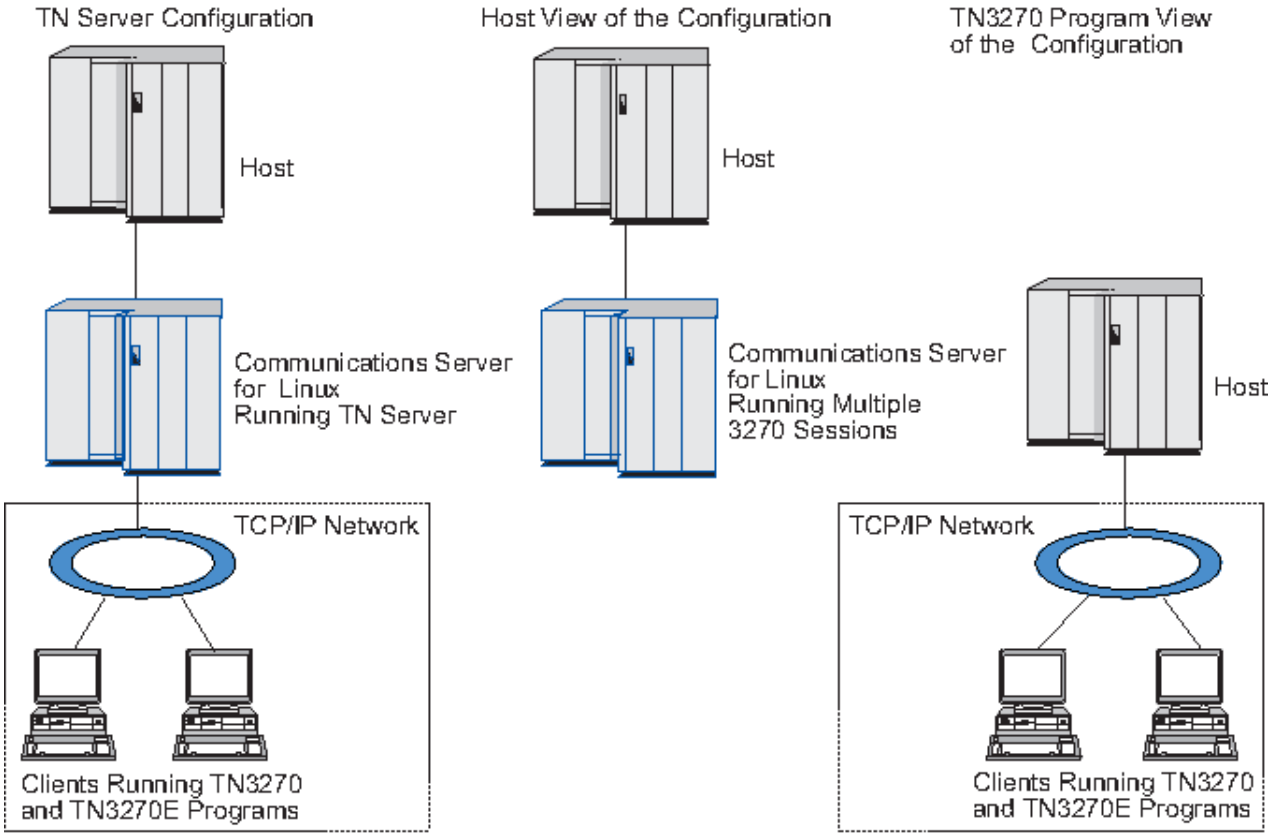


Abbildung 4. TN Server

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

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

Sicherheitsfeatures

TN Server von CS Linux unterstützt mit der SSL-Software (Secure Sockets Layer) die Datenverschlüsselung, die Server- und Clientauthentifizierung 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.

TN Redirector

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

TN Redirector von CS Linux 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 Linux eine Verbindung über ein TCP/IP-LAN ohne erforderliche Überprüfung herstellen, jedoch eine Verbindung zu einem fernen Host herstellen, der SSL erfordert, können Sie SSL für die TCP/IP-Verbindung zwischen CS Linux und dem Host verwenden. Auf diese Weise wird die Sicherheit für alle Clients überprüft. Die einzelnen Clients müssen keine Sicherheitsangaben machen.
- Wenn CS Linux 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 Linux verwenden und müssen die SSL-Software nicht auf dem Host installieren.

Features und Vorteile

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

Vielseitige Bausteine

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

- hostabhängiger Knoten
- 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 Linux” auf Seite 1)
- Partner (Quelle oder Ziel) in verteilten Anwendungen
- Gateway-Knoten zur Verbindung von SNA-Netzen

Durch APIs für Netzverwaltung kann der Linux-Computer als MS-Eingangspunkt konfiguriert werden und bietet dann Unterstützung für die verteilte Netzverwaltung. Auf Verbindungsebene kann der Linux-Computer mit einer der unterstützten Verbindungsarten mit verschiedenen LANs und WANs verbunden werden. (Eine Beschreibung der Verbindungsarten finden Sie in den Abschnitten „IBM Communications Server for Data Center Deployment für Linux” auf Seite 1 und „Installationsvoraussetzungen” auf Seite 19.)

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 mehrere Pfade zu einer SNA-Ressource macht eine Lastverteilung auf verschiedene Server möglich und bietet eine sofortige Ausweichlösung, falls ein bestimmter Server oder eine bestimmte Verbindung ausfällt.
- Werden mehrere Server übergreifende LU-Pools verwendet, kann der Administrator auf einfache Weise Server und Benutzer konfigurieren und hinzufügen.
- Durch die verringerte Anzahl von Verbindungen und PUs für die Hostkonnektivität reduziert sich die Größe der Host-VTAM-Definition.

- Mit den Verwaltungsdienstprogrammen können Knotenressourcen (für jeden Computer in der Domäne) und gemeinsam genutzte Ressourcen konfiguriert und verwaltet werden. Die Client-Server-Unterstützung der Verwaltungstools von CS Linux 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 Linux wurde mit Konfigurationsoptionen und Funktionen entwickelt, die die für die Konfiguration erforderliche Zeit und die Komplexität des Netzes reduzieren. Beispiele:

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

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

Webverwaltungsprogramm
Zu CS Linux gehört auch ein Webverwaltungsprogramm, das ähnliche Funktionen wie das Motif-Verwaltungsprogramm bereitstellt. Das Webverwaltungspaket ist ein Tool, das heruntergeladen werden kann und für die Verwaltung und Konfiguration von CS Linux bereitgestellt wird. Das können es von der Webseite https://www.ibm.com/support/pages/web-administration-package herunterladen.

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

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

Zusätzliche Schnittstellenoptionen für Verwaltung

Das Motif-Verwaltungsprogramm wird als Schnittstelle für die Konfiguration und Verwaltung von CS Linux empfohlen. Für CS Linux stehen Ihnen zusätzliche Schnittstellen zur el

API NOF

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

Verbesserte Leistung

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

- In APPN-Netzen unterstützt CS Linux sowohl HPR (High-Performance Routing) als auch ISR (Intermediate Session Routing) und stellt Verbindungsnetzoptionen bereit. ISR bietet Effizienz für kleine Netze, kann bei größeren Netzen jedoch die Leistung verschlechtern.
- In größeren Netzen mit LAN-Konnektivitätsoptionen (wie Token-Ring oder Ethernet) bzw. bei Verwendung von Enterprise Extender kann mit der Verbindungsnetzoption die Effizienz der Übertragung erhöht werden. Die Verbindungsnetzoption erstellt einen direkten Kommunikationspfad zwischen den Knoten, so dass der Datenverkehr Zwischennetzknoten umgehen kann.
- Ein weiterer Mechanismus zur Steuerung des Datenverkehrs, die angepasste Nachrichtendosierung auf Sitzungsebene, 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 Linux können Sie Ihre Daten durch die Definition verschiedener Sicherheitsstufen in der Konfiguration und durch Implementieren bestimmter Verbindungstypen schützen. Beispiele:

- In einem Client-Server-System können Sie einen WebSphere-Server konfigurieren, der Remote API Clients den HTTPS-Zugriff auf die Server ermöglicht. Bei dieser Art des Zugriffs werden Clientverbindungen mit Sicherheitszertifikaten authentifiziert. (Dieses Feature erfordert neben dem Standardprodukt CS Linux zusätzliche Software. Weitere Informationen hierzu finden Sie im Abschnitt „Installationsvoraussetzungen” auf Seite 19)
- LU-6.2-Benutzer können bis zu drei Sicherheitsstufen definieren: Sitzungssicherheit, Ressourcenschutz und Dialogsicherheit. So stellt der Benutzer sicher, dass die richtigen LUs an einer Sitzung beteiligt sind und dass der Zugriff auf alle einer bestimmten LU zugeordneten Anwendungen bzw. auf eine spezifische Anwendung eingeschränkt wird. Zusätzliche Sicherheit ist durch Datenverschlüsselungsroutinen möglich.
- TN Server und TN Redirector von CS Linux unterstützen mit der SSL-Software (Secure Sockets Layer) die Datenverschlüsselung sowie die Server- und die Clientauthentifizierung zwischen dem CS-Linux-Server und TN3270- oder Telnet-Clients. (Dieses Feature erfordert neben dem Standardprodukt CS Linux zusätzliche Software. Weitere Informationen hierzu finden Sie im Abschnitt „Installationsvoraussetzungen” auf Seite 19)

Flexible Netzverwaltung

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

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

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

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

Zuverlässigkeit, Verfügbarkeit und Wartungsfreundlichkeit

Zur Aufrechterhaltung eines zuverlässigen Systembetriebs stellt CS Linux 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
- Das WebAdmin-Paket ist ein Tool, das separat heruntergeladen werden kann und eine Web-Browser-Schnittstelle zum Verwalten, Konfigurieren und Abfragen von Statusinformationen bereitstellt. Dieses Tool ermöglicht einen sicheren Zugriff, sodass der Administrator Schreib-/Lesezugriff oder nur Lesezugriff auf SNA-Informationen haben kann.
- Abfrage- und Statusbefehle rufen Informationen zu folgenden Bereichen ab:
  - LU-LU-Sitzungen
  - APPN-Zwischensitzungen
  - aktive Verbindungen
  - APPN-Technologiedatenbanken, in denen Verbindungsinformationen gespeichert sind
- Tools für Fehlerdiagnose unterstützen die verschiedenen Phasen der Konfiguration und des Betriebs. Zu diesen Tools gehören unter anderem:
  - Tool zum Erfassen von Diagnoseinformationen (`snagetpd`), das Ihnen die Erfassung von Serviceinformationen erleichtert
  - Status- und Fehlernachrichten, die Sie bei der Fehlerbehebung für Konfigurationsroutinen und für den Systembetrieb unterstützen
  - Protokolle, in denen Informationen zu Netzfehlern, Störungen und Prüfungen erfasst werden
  - Trace-Funktionen für die Zusammenstellung und Formatierung ausführlicher Fehlerdaten

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

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

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

Netzintegration, Wachstum und Veränderungen

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

Enterprise Extender 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 CS Linux auf System z planen

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

Schritte bei der Netzplanung

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

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

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

Funktionsanforderungen für das Netz

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

- Soll das Netz ein APPN-Netz sein?
- Müssen die SNA-Anwendungen in Containern ausgeführt werden? Wenn ja, ist ein Client-Q

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

Konfiguration von CS Linux planen

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

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

Sie können CS Linux für die Unterstützung von zahlreichen Funktionen wie den 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)
- 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 Linux 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 Linux für die Ausführung von TN Server und die Unterstützung einer gemeinsam verwendeten Datenbank sowie einer unabhängigen LU-6.2-Verbindung zu MQSeries auf dem Host konfigurieren.

Ressourcenanforderungen für Installation und Betrieb

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

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

Die Beantwortung dieser Fragen hilft Ihnen bei der Festlegung der Ressourcenarten, die Linux verwendet, wenn das Produkt für die Unterstützung einer oder mehrerer der im Abschnitt „Funktionsanforderungen für das Netz” auf Seite 17 beschriebenen Funktionen konfiguriert wird. Die Beantwortung der Fragen hilft Ihnen darüber hinaus, das Verhältnis zwischen CS-Linux-Funktionen, Linux-Ressourcen und Netzressourcen besser zu verstehen.

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

Personalanforderungen

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

- Netzadministratoren, die das Netz planen, neue Einheiten hinzufügen und die Gesamtnetzleistung gewährleisten und verbessern
- Systemadministratoren, die CS Linux und die zugrunde liegende Hardware installieren bzw. warten und Systeme für die Netzverbindung konfigurieren

- Programmierer, die angepasste Anwendungen wie Transaktionsprogramme und Netzverwaltungsroutinen entwickeln

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

- Motif-Schnittstelle
- `rpm` (Installationstool für Red Hat Enterprise Linux und SuSE Linux Enterprise Server) oder `dpkg` (für Ubuntu Linux)
- 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-Linux-System Remote API Clients gehören, die HTTPS für die Verbindung zu Servern verwenden
- Web-Server, wenn das WebAdmin-Paket für die Verwaltung von CS Linux verwendet werden soll

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 Linux verfügbar sind, vertraut sein.

Übertragungsmedien

CS Linux 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 Linux kann die Token-Ring- und Ethernet-Adapter zusammen mit anderen Protokollen wie TCP/IP verwenden. Es ist möglicherweise erforderlich, eindeutige SAP-Adressen für jedes verwendete Protokoll anzugeben.

Installationsvoraussetzungen

Die Funktionen, die Sie CS Linux (aus dem Abschnitt „Funktionsanforderungen für das Netz” auf Seite 17) zuordnen, bestimmen gleichzeitig die Installationsvoraussetzungen. Dieser Abschnitt bietet einen Überblick über die für die Installation von CS Linux erforderlichen Computerressourcen. Weitere Informationen hierzu finden Sie in der zu den einzelnen Produkten gelieferten Dokumentation. (Das Literaturverzeichnis enthält hierzu eine Liste mit Büchern.)

Hardware

CS Linux erfordert einen zSeries-Computer (64-Bit), ein System z13 oder ein aktuelleres System.

Überprüfen Sie mit dem Befehl `uname -m` Ihren Zielcomputer. In der folgenden Tabelle ist die entsprechende Hardware und die Antwort von `uname -m` für diese Hardware angegeben.

Servertyp	Hardware	uname-Antwort
System z	64-Bit-zSeries oder System z13	`s390x`

Betriebssystem Linux

CS Linux unterstützt die folgenden Linux-Distributionen. Die neuesten Informationen zu den spezifischen Versionsnummern und Kernel-Builds, die für jede Distribution unterstützt werden, sowie zu weiteren Voraussetzungen für bestimmte Versionen finden Sie in der README-Datei aus dem CS-Linux-Installationsimage.

- Red Hat Enterprise Linux Server 7 und 8
- SUSE Linux Enterprise Server 12 und 15

- Ubuntu Linux LTS 18.04 und 20.04

Mit dem Feature SE Linux (Security Enhanced Linux) können Linux-Distributionen den Zugriff auf bestimmte Codebibliotheken und Funktionen überwachen und steuern. Für die Aktivierung von CS Linux und Linux Streams muss, je nach Version der installierten Linux-Distribution, die Konfiguration bearbeitet werden. Nähere Informationen zu diesen Schritten enthält die README-Datei.

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

CS Linux kann mit Enterprise Extender über TCP/IP-Schnittstellen verwendet werden, mit dem MPC-Einheitentreiber (MultiPath Channel) von Linux für System z über eine virtuelle MPC-Schnittstelle (nur Linux auf System z), mit dem Linux-Einheitentreiber `qeth` mit layer2/VSwitch-Unterstützung über 802.2-Ethernet-OSA-Verbindungen oder mit dem Linux-Einheitentreiber `lcs` über 802.2-Ethernet- bzw. Token-Ring-OSA-Verbindungen (wofür im OSE-Modus `chpid` ein OSA2 erforderlich ist).

Zusätzliche Software: Linux
CS Linux erfordert die folgende zusätzliche Software. In der README-Datei aus dem CS-Linux-Installationsimage finden Sie ausführliche Informationen zu den Voraussetzungen für bestimmte Versionen (je nach verwendeter Linux-Distribution) sowie Anweisungen zur Installation der entsprechenden Softwarepakete.

- Linux Streams (LiS).
- OpenMotif (nur auf einem Server, aber nicht auf einem Client erforderlich). Diese Software wird für die Verwendung des Motif-Verwaltungsprogramms benötigt. Dieses Verwaltungsprogramm wird zum Konfigurieren und Verwalten von CS Linux empfohlen.
- Java (ist erforderlich, wenn Sie Java CPI-C verwenden möchten). Sie benötigen die Java Runtime Environment (JRE). Wenn Sie neue Java-Klassen für die Verwendung mit einer Java-CPI-C-Anwendung kompilieren müssen, brauchen Sie außerdem das Java SDK.
- GSKit. Das Global Security Kit ist auf einem Server erforderlich, wenn Sie die SSL-Funktion von TN Server oder TN Redirector verwenden möchten. Auf einem Client ist es erforderlich, wenn dieser via HTTPS eine Verbindung zu CS-Linux-Servern herstellt.
  - Für einen Server ist die Software GSKit auf dem Installationsdatenträger enthalten und wird automatisch mit CS Linux installiert. Bei Bedarf können Sie den z90Crypto-Adapter mit CS Linux auf System z verwenden, um SSL-Sicherheit bereitzustellen. Weitere Informationen zur Konfiguration von CS Linux für die Verwendung des Adapters finden Sie in der Datei `CSLinux_Crypto_settings.pdf` auf dem Installationsdatenträger.
  - Wenn Sie die Software GSKit für einen Client verwenden möchte, lesen Sie die README-Datei auf dem Installationsdatenträger, um nähere Informationen über den Bezug und die Installation zu erhalten.
- MPC-Einheitentreiber von Linux für System z (Nur CS Linux auf System z und nur auf einem Server, nicht aber auf einem Client erforderlich. Diese Komponente wird benötigt, wenn Sie für die Verbindung zu VM/VTAM-Systemen MPC-Verbindungen verwenden.)

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

CS Linux 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 Linux-Computer wie CS Linux installiert werden.) Weitere Informationen zur Installation von WebSphere Application Server finden Sie in der zugehörigen Dokumentation. Um WebSphere zusammen mit CS Linux verwenden zu können, müssen Sie ein zusätzliches CS-Linux-Plug-in auf diesem Computer installieren. Dieser Schritt ist im Abschnitt „WebSphere Application Server konfigurieren” auf Seite 31 beschrieben.

Speicher und Hauptspeicher

Wenn CS Linux das gesamte Spektrum der Konfigurationen und Dienste unterstützen soll, muss zusätzlich zu dem für die Linux-Distribution erforderlichen Mindestspeicher ein Hauptspeicher von 64 MB und ein Plattenspeicherplatz von 200 MB verfügbar sein. Während der Installation sind zusätzlich 250 MB temporärer Speicher erforderlich.

Falls Sie die Dokumentation zu CS Linux als Softcopy (PDF) installieren wollen, benötigen Sie zusätzlichen Festplattenspeicherplatz. Für die Installation aller Softcopyhandbücher benötigen Sie 80 MB Plattenspeicherplatz.

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

IPV4- und IPV6-Adressen

Computer, auf denen CS Linux 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 Linux IPV4 verwendet, müssen TN-Clients, die eine Verbindung zum TN-Server herstellen, ebenfalls IPV4 verwenden. Wenn CS Linux 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 Linux und von Linux zum Host) IPV4 verwenden müssen, wenn CS Linux IPV4 verwendet.

  Verwendet CS Linux IPV6, gelten für die TCP/IP-Verbindung vom Client zu CS Linux dieselben Regeln wie für TN Server. Für die Verbindung von CS Linux zum Host kann IPV6 oder IPV4 verwendet werden. Es ist nicht erforderlich, dass die beiden Verbindungen dasselbe Adressformat verwenden.
- Für Enterprise Extender (HPR/IP) gilt, dass die Ports an beiden Enden der Verbindung dasselbe Adressformat verwenden müssen (IPV4 oder IPV6).
  - Wenn CS Linux IPV4 verwendet, kann die Software nur Verbindungen zu fernen Systemen herstellen, die für die Unterstützung von IPV4 konfiguriert sind.
  - Verwendet CS Linux 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. Gleichermaßen 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-Linux-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 System mit CS Linux wie im Abschnitt „Vorversionen von CS Linux migrieren” auf Seite 27 beschrieben ein Upgrade durchführen und dabei gleichzeitig zu IPV6-Adressen wech-

seln 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 Linux 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 Linux 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.)

Firewall für den Datenverkehr von Enterprise Extender, Client/Server und TN3270 Server konfigurieren

Die Standardfilter für die Firewalleinstellungen von Linux-Server in `/etc/sysconfig/iptables` verhindern, dass an Enterprise-Extender-, Client-Server- und TN3270-Server-Ports eingehender Datenverkehr empfangen wird. Falls Sie die Konnektivität über diese Ports bei aktivierter Firewall ermöglichen möchten, aktualisieren Sie die Datei `/etc/sysconfig/iptables` folgendermaßen.

Suchen Sie in der Datei den Abschnitt, in dem die INPUT-Anweisungen aufgelistet sind. Fügen Sie dem Abschnitt alle unten stehenden Anweisungen hinzu.

Wenn Sie Enterprise-Extender-Pakete erhalten möchten, fügen Sie die folgenden Anweisungen mit den Portnummern hinzu, die Enterprise Extender verwendet:

```
-A INPUT -p udp --dport 12000 -j ACCEPT
-A INPUT -p udp --dport 12001 -j ACCEPT
-A INPUT -p udp --dport 12002 -j ACCEPT
-A INPUT -p udp --dport 12003 -j ACCEPT
-A INPUT -p udp --dport 12004 -j ACCEPT
```

Wenn Sie möchten, dass Remote API Clients sich mit dem Server verbinden, fügen Sie die folgende Anweisung mit der entsprechenden Client/Server-Portnummer hinzu:

```
-A INPUT -p tcp --dport 1553 -j ACCEPT
```

Wenn Sie Datenverkehr von TN3270 Server und TN Redirector empfangen möchten, fügen Sie eine Anweisung ähnlich der folgenden für jede Portnummer, die TN Server oder TN Redirector verwendet, hinzu. Die Portnummern werden mit `define_tn3270_access` oder `define_tn_redirect` angegeben. Das folgende Beispiel gilt für die Portnummer 6023.

```
-A INPUT -p tcp --dport 6023 -j ACCEPT
```

Nachdem Sie die Datei aktualisiert haben, müssen Sie den Service iptables erneut starten, um den Firewallfilter mit den neuen Einstellungen zu aktivieren. Verwenden Sie den folgenden Befehl:

```
service iptables restart
```

Die Firewall lässt jetzt zu, dass CS Linux Enterprise-Extender-, Client-Server- und TN3270-Server-Pakete empfängt, um die Konnektivität zu Partnerservern und -clients zu etablieren.

Namenskonventionen

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

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

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

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

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

Kapitel 3. CS Linux auf Linux-Servern installieren

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

- genaue Paketnamen und/oder Versionsnummern für die benötigten zusätzlichen Softwarepakete
- ausführliche Informationen zur Installation und zu den Konfigurationsbefehlen

Lizenzierung und Konfektionierung von CS Linux

In diesem Abschnitt ist erläutert, wie das Produkt CS Linux lizenziert und bereitgestellt wird.

Mechanismen der Lizenzierung für CS Linux

Dieser Abschnitt soll dem Leser einen besseren Einblick in die Lizenzierungsmechanismen vermitteln. Das Dokument *License Information* für CS Linux enthält die vollständigen Vertragsbedingungen. Darüber hinaus stehen Beispielszenarien zur weiteren Erläuterung der Lizenzierung für viele verschiedene Arten der Konnektivität und Funktionalität von CS Linux zur Verfügung. Sie finden diese Informationen unter https://www.ibm.com/products/communications-server-for-data-center.

Für jede Maschine oder jeden SP-Knoten, auf dem einige oder alle Komponenten installiert sind, ist eine separate Programmlizenz für CS Linux erforderlich.

Die Lizenzierung für CS Linux umfasst die Programmlizenz (Server) und Benutzerlizenzen.

- Ein Benutzer wird als eine Person definiert. Sie müssen eine Benutzerberechtigung für jeden gleichzeitig angemeldeten Benutzer erwerben, der direkt oder indirekt auf CS Linux zugreift und das Produkt verwendet. 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 Linux herstellt, über die mehreren gleichzeitig angemeldete Benutzer Zugriff haben. In dem Fall ist für jeden der gleichzeitig angemeldeten Benutzer eine Benutzerlizenz erforderlich.
- Bei Anwendungsprogrammen, die keinen Benutzern zugeordnet sind, ist zusätzlich eine Benutzerberechtigung für jede aktive vor- oder nachgeordnete Verbindung, die auf dem CS-Linux-Knoten eingerichtet wird, erforderlich. In einer APPN-Umgebung wird eine aktive Verbindung zu einem Nachbarknoten als eine Verbindung gewertet.

Verwendung von CS-Linux-Ressourcen überwachen

Es gibt zwei Möglichkeiten der Lizenzierung für Communications Server for Data Center Deployment, einschließlich CS Linux: Prozessor-Value-Unit (PVU) oder Lizenzen 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 Linux ausführen. Daher ist es notwendig, die PVU-Nuztung mit IBM Tivoli License Manager (ITLM) zu überwachen. Bei der Lizenzierung für gleichzeitig angemeldete Benutzer protokolliert der CS-Linux-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/opt/ibm/sna/ad8a7aebefee4d8e9554c14f5f734b7b.slmtag` protokoliert.

Angebotene CS-Linux-Lizenzprogrammpakete

Das Lizenzprogramm CS Linux wird auf drei CDs mit folgendem Inhalt geliefert:

© Copyright IBM Corp. 1998, 2021

CD 1: Schnelleinstieg
Diese CD enthält die vollständige PDF-Dokumentation zu CS Linux (im Verzeichnis `/DOCS`).

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

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

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

- Linux-Client für AMD64/Intel EM64T x86_64 (64-Bit)
- Linux-Client für Power (ppc64le)
- Linux-Client für System z s390x
- AIX-Client
- x64-Windows-Client

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

Anmerkung: Informationen zum Speicherbedarf finden Sie im Abschnitt „Installationsvoraussetzungen” auf Seite 19.

Installation von CS Linux vorbereiten

Vorausgesetzte Software installieren

Vor der Installation von CS Linux müssen Sie die vorausgesetzte Software installieren, die im Abschnitt „Installationsvoraussetzungen” auf Seite 19 aufgelistet ist:

- LiS Streams
- OpenMotif
- Java
- MPC-Einheitentreiber von Linux für System z (nur CS Linux auf System z und nur erforderlich, wenn MPC-Verbindungen zu VM/VTAM-Systemen hergestellt werden sollen)

Umfassende Informationen zu den erforderlichen Softwarepaketen sowie eine schrittweise Anleitung für die Installation finden Sie in der Datei README aus dem CS-Linux-Installationsimage.

Details der Produktinstallation anzeigen

Sie können Informationen zu CS Linux 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`.

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

Sprachumgebungsvariable ändern

Wenn Sie CS Linux verwenden, vergewissern Sie sich, dass die Variable LANG auf die von Ihnen gewünschte Sprache gesetzt ist.

Mit dem folgenden Befehl können Sie die Variable LANG ändern:

```
export LANG=Sprache
```

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

Kennung	Sprache
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)

Vorversionen von CS Linux migrieren

Hinweise

Wenn Sie für eine frühere Version von CS Linux ein Upgrade auf CS Linux Version 7.1 durchführen, müssen Sie die folgenden Hinweise beachten.

1. Wenn Sie CS Linux 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 Linux Version 7.1.
   - Insbesondere ältere Clients unter Betriebssystemen, für die mit CS Linux Version 7.1 keine Clients ausgeliefert werden (z. B. 32-Bit-Windows-Betriebssysteme), funktionieren weiter mit CS Linux 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 Linux 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_REDIRECTION_INDICATION

3. Falls Sie die neue Funktionalität der IPV6-Adressen von Version 7.1 nutzen möchten, müssen Sie sicherstellen, dass die Server mit CS Linux für die Verwendung von IPV6-Adressen konfiguriert sind. Weitere Details hierzu enthält der Abschnitt „IPV4- und IPV6-Adressen" auf Seite 21.

Migrationsprozess

Falls Sie bereits eine frühere Version von CS Linux installiert haben und jetzt auf Version 7.1 migrieren möchten, müssen Sie die folgenden Schritte ausführen:

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

- `/etc/opt/ibm/sna/sna_node.cfg`
- `/etc/opt/ibm/sna/sna_domn.cfg`
- `/etc/opt/ibm/sna/sna.net`
- `/etc/opt/ibm/sna/sna_tps`
- `/etc/opt/ibm/sna/environment`
- `/etc/opt/ibm/sna/logfilter.txt`
- `/etc/opt/ibm/sna/ibmcs.kdb`
- `/etc/opt/ibm/sna/ibmcs.sth`
- `/etc/opt/ibm/sna/ibmcs.rdb`
- `/etc/opt/ibm/sna/ibmcs.crl`

Falls Sie die Startdatei `/etc/rc.d/init.d/snastart` wie im Abschnitt „CS Linux aktivieren" auf Seite 67 beschrieben angepasst und den Befehl `sna start` entfernt haben, damit CS Linux beim Systemstart nicht automatisch gestartet wird, müssen Sie die Änderungen notieren, die Sie an dieser Datei vorgenommen haben.

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

```
sna stop
rpm -e ibm-conmserver-ptf
rpm -e ibm-commserver-docs
rpm -e ibm-commserver-ecl
rpm -e ibm-commserver
rpm -e gskssl32
rpm -e gskcrypt32
rpm -e gskssl64
rpm -e gskcrypt64
```

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

```
PATH=$PATH:/sbin
unset LD_PRELOAD
cd /usr/src/LiS
```

```
make uninstall
make very-clean
cd /usr/src
rm -rf LiS*
```

Ändern von PATH und anderen Umgebungsvariablen
Falls Sie die folgenden Umgebungsvariablen für die frühere Version von CS Linux modifiziert haben, sollten Sie die Änderungen rückgängig machen, weil die Pfade für das Lizenzprogramm CS Linux Version 7.1 andere sein können.

- PATH
- LD_LIBRARY_PATH
- LD_RUN_PATH
- LD_PRELOAD
- CLASSPATH

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

```
env | grep sna
```

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

Abschließende Bereinigung
Mit den folgenden Befehlen werden alle verbliebenen Einträge der alten Produktversion entfernt.

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

Installieren des Lizenzprogramms CS Linux Version 7.1
Führen Sie für die Installation des Produkts die Anweisungen in diesem Handbuch und in der Datei README aus.

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

```
/opt/ibm/sna/bin/sna stop
```

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

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

Falls Sie Änderungen an der Startdatei /etc/rc.d/init.d/snastart gespeichert haben, müssen Sie dieselben Änderungen an der neuen Kopie der Datei vornehmen, um sicherzustellen, dass CS Linux nicht automatisch beim Systemstart gestartet wird. Gehen Sie dazu wie im Abschnitt „CS Linux aktivieren" auf Seite 67 beschrieben vor.

Starten Sie die Software CS Linux mit folgendem Befehl erneut:

```
/opt/ibm/sna/bin/sna start
```

Lizenzprogramm CS Linux installieren

CS Linux installieren

Wenn bereits eine frühere Version von CS Linux installiert ist, führen Sie die Schritte im Abschnitt „Vorversionen von CS Linux migrieren" auf Seite 27 aus, um die alte Version zu entfernen, bevor Sie diese neue Version installieren.

Führen Sie für die Installation von CS Linux die folgenden Schritte aus:

1. Kopieren Sie die Datei `ibm-commserver-7.1.0.0-s390x.tgz` von 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

   zcat ibm-commserver-7.1.0.0-s390x.tgz | tar - xf -
   ```
4. Führen Sie wie folgt das Shell-Script `installibmcs` aus:

   ```
   ./installibmcs
   ```

   Dieses Shell-Script testet, ob bestimmte Vorbedingungen erfüllt sind, und setzt Warnungen ab, falls sie nicht erfüllt sind. Es fordert Sie außerdem zu den folgenden Eingaben auf. Nach Eingabe der vom Shell-Script angeforderten Informationen installiert das Script die `rpm`/`deb`-Pakete.

   - Bestätigung, dass Sie die Lizenzbedingungen für CS Linux gelesen haben.

   Sie können diese Eingabeaufforderungen außer Kraft setzen, indem Sie den Befehl `installibmcs` wie nachfolgend beschrieben mit zusätzlichen Parametern angeben.

   Stellt das Shell-Script einen Fehler fest, der die Installation von CS Linux unmöglich macht, schreibt es eine Fehlernachricht in die Standardausgabe (dies ist in der Regel der Bildschirm). Hilfe bei der Behebung derartiger Fehler finden Sie in der README-Datei des CS-Linux-Installationsimage.

   Bei Systemen mit begrenzter Speicherkapazität müssen Sie nach der Installation von CS Linux unter Umständen einen Warmstart durchführen, bevor der SNA-Knoten gestartet werden kann. Für größere Systeme ist dies vielleicht nicht erforderlich. Wenn der CS-Linux-Knoten nicht gestartet wird, überprüfen Sie, ob die Datei `/var/log/messages` einen Eintrag wie den folgenden enthält:

   ```
   kernel: SNA Trace Driver can only get X blocks of memory - please reboot
   ```

   Wird diese Nachricht auch nach dem Warmstart noch angezeigt, benötigen Sie mehr Speicherkapazität.
5. Fügen Sie die Binärverzeichnisse von CS Linux 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:/opt/ibm/sna/bin/X11'

   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 CS Linux. Nach der Installation geschieht dies automatisch, wenn die Maschine neu gebootet wird.

   ```
   cd /

   sna start
   ```
7. Führen Sie das Motif-Verwaltungsprogramm von CS Linux aus. Wir empfehlen Ihnen dringend, dieses Programm zu verwenden, bis Sie besser mit der Funktionsweise von CS Linux vertraut sind.

Sie müssen einen fernen X-Window-Server verwenden, weil das System z mit Linux nur die Funktionalität eines X-Window-Clients bereitstellt. Verwenden Sie auf dem X-Window-Server den folgenden Befehl:

```
xhost +XXXX
```

XXXX steht hier für den TCP/IP-Namen oder die Adresse des Systems z mit Linux.

Teilen Sie jetzt dem xsnaadmin-Client mit, wo sich der Server befindet, und starten Sie ihn:

```
export DISPLAY= YYYY:Z
```

```
xsnaadmin &
```

YYYY steht hier für den TCP/IP-Namen oder die Adresse des X-Window-Servers und *Z* für die Nummer der virtuellen Anzeige (in der Regel `0`).

Wenn Sie eine nicht überwachte Installation ausführen müssen, können Sie den Befehl `installibmcs` mit zusätzlichen Parametern angeben, um die Lizenzbedingungen für Linux zu akzeptieren und den Namen des Controller-Servers anzugeben. In diesem Fall wird das Shell-Script ausgeführt, ohne den Benutzer zur Eingabe weiterer Informationen aufzufordern. Verwenden Sie den folgenden Befehl:

```
./installibmcs license_accepted
```

Onlinedokumentation zu CS Linux

Führen Sie die im Abschnitt „CS Linux installieren” auf Seite 29 beschriebenen Schritte aus, um die `tgz`-Datei zu entpacken. Führen Sie dann wie folgt das Shell-Script `installibmcsdocs` aus:

```
./installibmcsdocs
```

WebSphere Application Server konfigurieren

Wenn Sie mit einem Client-Server-System arbeiten, in dem Remote API Clients über HTTPS eine Verbindung zu CS-Linux-Servern erstellen, 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 19.

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

- Konfigurieren eines sicheren Zertifikats auf dem WebSphere-Server, das den Clients vorgelegt wird
- Konfigurieren von WebSphere Application Server für die Verwendung mit CS Linux
- 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 Verwendung mit CS Linux zu konfigurieren. Weitere Informationen hierzu finden Sie in der Dokumentation zu WebSphere Application Server.

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

   Wenn die Administrationskonsole unter Windows ausgeführt wird, müssen Sie die Dateien nicht kopieren, weil Sie direkt auf die CD mit den Dateien zugreifen können. Sie müssen nur die Installations-CD mit Remote API Client in das CD-Laufwerk des Windows-Computers einlegen.
2. Starten Sie die WebSphere-Administrationskonsole.
3. Erstellen Sie gemäß den Anweisungen in der WebSphere-Dokumentation einen virtuellen Host, auf den nur über eine sichere SSL-Verbindung zugegriffen werden kann. Dieser virtuelle Host wird für das Java-Plug-in verwendet, das SNA-HTTPS-Verbindungen verwaltet.
4. Wählen Sie in der Menüleiste 'Anwendungen' -> 'Neue Anwendung installieren' aus.
5. Geben Sie die Position der Datei `snahttpsrv.ear` an. Klicken Sie auf 'Weiter'.
6. Wenn Sie in den beiden ersten Anzeigen aufgefordert werden, einen virtuellen Hostnamen anzugeben, geben Sie den Namen des virtuellen Hosts ein, den Sie für HTTPS konfiguriert haben. Für alle übrigen Parameter können Sie die Standardeinstellungen übernehmen, sofern Sie keine spezifische WebSphere-Konfiguration erstellen möchten. Klicken Sie in den folgenden Dialoganzeigen jeweils auf 'Weiter', bis nur noch 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 Linux benötigt WebSphere Application Server eine Liste der CS-Linux-Server, auf die mit HTTPS zugegriffen werden soll. Führen Sie zum Erstellen und Installieren der Liste die folgenden Schritte aus.

1. Wählen Sie in der Menüleiste der WebSphere-Administrationskonsole 'Umgebung' -> 'WebSphere-Variablen verwalten' aus.
2. Suchen Sie in der Liste nach der Variablen `USER_INSTALL_ROOT` und notieren Sie den Wert der Variablen. (Dies ist der Pfad eines Verzeichnisses auf dem WebSphere-Server.) Die Liste der Umgebungsvariablen kann zwei oder mehr Seiten umfassen, so dass Sie unter Umständen die Taste zum Vorblättern verwenden müssen, um die gesamte Liste durchzublättern.
3. Kopieren Sie die Datei `snahttpsrv.cfg` von der Position, an der Sie sie beim Durcharbeiten des Abschnitts „WebSphere Application Server konfigurieren” auf Seite 32 gespeichert haben, (oder von der Installations-CD) in das von der Variablen `USER_INSTALL_ROOT` angegebene Verzeichnis. Bearbeiten Sie diese Datei dann mit einem Texteditor. Nehmen Sie die CS-Linux-Server auf, auf die Remote API Clients mit HTTPS zugreifen können. Jeder Server muss in einer gesonderten Zeile der Datei und im folgenden Format angegeben werden:

   `server=`*servername.domänenname.com*

Prozeduren für den Installationsabschluss

In den folgenden Abschnitten ist die Ausführung von Verwaltungstasks beschrieben, die nach der Installation von CS Linux erforderlich sein können.

Client-Server-Betrieb

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

Bereinigung nach der Installation

Nach Abschluss der Installation können Sie die während der Installation erstellte `tgz`-Datei sowie das temporäre Verzeichnis löschen.

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 `/opt/ibm/sna/docs` installiert. Die Handbücher sind außerdem im Verzeichnis `/DOCS` des Installationsdatenträgers mit CS Linux und in der `tgz`-Datei 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 Informationsdatei README zum Produkt befindet sich im Verzeichnis `/opt/ibm/sna` und enthält Informationen zu allen Produktänderungen, die nach Veröffentlichung der Bibliothek zu CS Linux vorgenommen wurden. Sie finden diese Datei auch im Stammverzeichnis des Installationsdatenträgers mit CS Linux und in der `tgz`-Datei. Immer, wenn Sie Produktupdates erhalten, sollten Sie nach zugehörigen Informationen in der README-Datei suchen.

SSL für die Verwendung mit TN Server oder TN Redirector konfigurieren

Falls Sie TN Server oder TN Redirector mit dem Feature SSL verwenden möchten, müssen Sie die SSL-Software nach der Installation von CS Linux konfigurieren.

Die SSL-Software erfordert zwei Komponenten:

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

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

Für die Verwaltung der Schlüsselringdatenbank muss OpenMotif installiert werden. Die README-Datei im CS-Linux-Installationsimage enthält Anweisungen für die Installation von OpenMotif.

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

```
snakeyman
```

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

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

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

```
snaadmin term_node
snaadmin init_node
```

Konfigurationsdateien von CS Linux sichern

CS Linux erstellt automatisch Sicherungskopien der Knoten-, Domänen- und TN3270-Einheitendaten (`tn3270dev.dat`) sowie der TP-Konfigurationsdatei, wenn Sie (mit einem der CS-Linux-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 Linux eine Sicherungsdatei mit dem Namen `sna_node.bk`*n*, wobei die Zahl *n* entweder 1 oder 2 ist.

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

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

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

- vor Installation einer neuen Version des Betriebssystems Linux
- vor Installation eines neuen Release von CS Linux
- nach Erstellung einer neuen Konfiguration

Führen Sie zum Sichern von Konfigurationsdateien die folgenden Befehle aus:

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

Sicherungskopie der Konfigurationsdateien von CS Linux zurückschreiben

Gehen Sie wie folgt vor, um die Konfigurationsdateien von CS Linux zurückzuschreiben, die Sie wie im Abschnitt „Konfigurationsdateien von CS Linux sichern” auf Seite 34 beschrieben gesichert haben:

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

   ```
   snaadmin status_node
   ```

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

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

```
sna stop
```

2. Geben Sie den folgenden Befehl ein:

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

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

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

Konfigurationsdateien reinitialisieren

Werden Konfigurationsdateien von CS Linux unabsichtlich geändert, so dass die darin enthaltenen Daten nicht mehr verwendet werden können, müssen Sie die Dateien möglicherweise neu initialisieren. Auf diese Weise können Sie CS Linux 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/opt/ibm/sna/` kopieren und für die Initialisierung des Knotens mit dem Befehl `sna start` verwenden.

Sie können die folgenden Konfigurationsdateien neu initialisieren:

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

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

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

```
sna stop
```

2. Sichern Sie die vorhandenen Konfigurationsdateien, indem Sie alle Dateien, die Sie neu initialisieren, in ein anderes Verzeichnis kopieren.
3. Löschen Sie die neu zu initialisierenden Dateien.
4. Falls Sie die Domänenkonfigurationsdatei gelöscht haben, setzen Sie zum erneuten Erstellen dieser Datei den folgenden Befehl ab (der die zu CS Linux gelieferte leere Domänenkonfigurationsdatei kopiert):

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

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

5. Falls Sie die SSL-Schlüsselringdatenbankdatei gelöscht haben, setzen Sie zum erneuten Erstellen dieser Datei den folgenden Befehl ab (der die zu CS Linux gelieferte Beispieldatei kopiert):

```
cp -p /opt/ibm/sna/samples/ibmcs.* /etc/opt/ibm/sna
```

6. Geben Sie den folgenden Befehl ein, um CS Linux neu zu starten:

```
sna start
```

7. Starten Sie wie folgt das Motif-Verwaltungsprogramm:

```
xsnaadmin &
```

Wenn die Datei `sna_node.cfg` nicht vorhanden ist, fordert das Verwaltungsprogramm Sie auf, den Knoten zu konfigurieren. Sie können nun den Knoten und die übrigen Ressourcen konfigurieren. Lesen Sie dazu die Informationen in Kapitel 8, „CS Linux konfigurieren und verwenden", auf Seite 65 oder im *Verwaltungshandbuch für IBM Communications Server for Data Center Deployment für Linux*.

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

CS Linux deinstallieren

Sie können das Produkt CS Linux jederzeit deinstallieren. Gehen Sie dazu wie folgt vor:

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

   ```
   snaadmin status_node
   ```

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

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

   ```
   sna stop
   ```
3. Entfernen Sie das CS-Linux-Paket und die zugeordneten Softwarepakete mit den folgenden Anweisungen (verwenden Sie unter Ubuntu Linux `dpkg -r`):

   ```
   rpm -e ibm-commserver-docs
   ```

   ```
   rpm -e ibm-commserver
   ```

   ```
   /sbin/shutdown -r now
   ```

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 für Linux kann über ein TCP/IP-Netz eine Verbindung zu CS-Linux-Servern herstellen (oder zu CS/AIX-Servern, jedoch nicht zu beiden gleichzeitig). (CS-Linux-Server können nicht in derselben Domäne wie CS/AIX-Server ausgeführt werden.)

Dieses Kapitel bezieht sich auf IBM Remote API Clients, die auf 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 43.

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 Linux 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 Linux migrieren" auf Seite 27.

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

© Copyright IBM Corp. 1998, 2021

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-AI 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 eine Verbindung zu CS-Linux-Servern herstellen soll, benötigen Sie die Software GSKit, um den HTTPS-Zugriff auf die Server über einen WebSphere-Server zu ermöglichen. 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 Linux definieren

CS Linux steuert die Operationen mit einer Reihe von Umgebungsvariablen, die Sie vor der Aktivierung der Software CS Linux auf dem Client festlegen müssen. Am einfachsten ist es, die Variablen in einer Textdatei festzulegen, die CS Linux beim Start liest.

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

```
export LANG=en_US
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
```

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 41 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
   ./installibmcscli
   ```

   Das Shell-Script testet, ob bestimmte Vorbedingungen erfüllt sind, und setzt Warnungen ab, falls sie nicht erfüllt sind. Sie werden aufgefordert, die Lizenzvereinbarung zu lesen und zu akzeptieren. Erst dann installiert das Script die rpm/deb-Pakete.
4. Erstellen Sie die Clientnetzdatendatei, um die CS-Linux-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 Linux* 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 40.

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 Linux* im Abschnitt 'Remote API Clients verwalten' nachlesen.

HTTPS-Sicherheitszertifikate mit dem GSKit konfigurieren

Wenn der Client mit HTTPS eine Verbindung zu CS-Linux-Servern herstellen 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-Schlüsselverwaltungsprogram.

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`):

```
/opt/ibm/sna/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 für Linux auf System z kann über ein TCP/IP-Netz eine Verbindung zu CS-Linux-Servern (oder zu CS/AIX-Servern) herstellen.

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

Falls Sie ein Upgrade für eine frühere Version von CS Linux 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 Linux migrieren” auf Seite 27.

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 43 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-AI 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 eine Verbindung zu CS-Linux-Servern herstellen soll, benötigen Sie die Software GSKit, um den HTTPS-Zugriff auf die Server über einen WebSphere-Server zu ermöglichen. 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:

© Copyright IBM Corp. 1998, 2021

```
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 Linux definieren

CS Linux steuert die Operationen mit einer Reihe von Umgebungsvariablen, die Sie vor der Aktivierung der Software CS Linux auf dem Client festlegen müssen. Am einfachsten ist es, die Variablen in einer Textdatei festzulegen, die CS Linux beim Start liest.

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

```
export LANG=en_US
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
```

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 47 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 Linux zu bestätigen. Sie können diese Eingabeaufforderung außer Kraft setzen, indem Sie den Befehl `instal-libmcscli` 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-Linux-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 Linux* 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 46.

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 Linux* im Abschnitt 'Remote API Clients verwalten' nachlesen.

HTTPS-Sicherheitszertifikate mit dem GSKit konfigurieren

Wenn der Client mit HTTPS eine Verbindung zu CS-Linux-Servern herstellen 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-Schlüsselverwaltungsprogram.

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 für AIX kann über ein TCP/IP-Netz eine Verbindung zu CS-Linux-Servern (oder CS/AIX-Servern) herstellen.

Lesen Sie vor der Installation der Software die README-Datei zu IBM Remote API Client. Diese Datei ist im Verzeichnis `/ibm-commserver-clients/aix` auf der Installations-CD enthalten. Falls Sie ein Upgrade für eine frühere Version von CS Linux 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 Linux migrieren” auf Seite 27.

Hardware- und Softwarevoraussetzungen

Hardwarevoraussetzungen

IBM Remote API Client erfordert ein Power System, das von einer der im Abschnitt „Betriebssystemversion” auf Seite 49 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 eine Verbindung zu CS-Linux-Servern herstellen soll, benötigen Sie die Software GSKit, um den HTTPS-Zugriff auf die Server über einen WebSphere-Server zu ermöglichen. Weitere Informationen zur Beschaffung und Installation der GSKit-Software enthält die README-Datei auf dem Installationsdatenträger.

Umgebungsvariablen für CS Linux definieren

CS Linux steuert die Operationen mit einer Reihe von Umgebungsvariablen, die Sie vor der Aktivierung der Software CS Linux auf dem Client festlegen müssen. Am einfachsten ist es, die Variablen in einer Textdatei festzulegen, die CS Linux beim Start liest.

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

© Copyright IBM Corp. 1998, 2021

```
export LANG=en_US
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
```

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 52 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-Linux-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 Linux* 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 51.

Außerdem müssen Sie die Clientnetzdatendatei aktualisieren und die CS-Linux-Server angeben, zu denen der Client eine Verbindung herstellen darf, sowie den WebSphere-Server, der die HTTPS-Unterstützung bereitstellt. Weitere Details hierzu können Sie im *Verwaltungshandbuch für IBM Communications Server for Data Center Deployment für Linux* 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.

   ```
   unmount /mnt
   ```

5. Erstellen Sie die Clientnetzdatendatei, um die CS-Linux-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 Linux* 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 51.

Außerdem müssen Sie die Clientnetzdatendatei aktualisieren und die CS-Linux-Server angeben, zu denen der Client eine Verbindung herstellen darf, sowie den WebSphere-Server, der die HTTPS-Unterstützung bereitstellt. Weitere Details hierzu können Sie im *Verwaltungshandbuch für IBM Communications Server for Data Center Deployment für Linux* 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-Schlüsselverwaltungsprogram.

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 für Windows kann über ein TCP/IP-Netz eine Verbindung zu CS-Linux-Servern (oder CS/AIX-Servern) herstellen.

Falls Sie ein Upgrade für eine frühere Version von CS Linux 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 Linux migrieren” auf Seite 27.

Der mit CS Linux Version 7.1 ausgelieferte Client unterstützt nur 64-Bit-Windows-Betriebssysteme. Ältere CS-Linux-Clients können weiterhin unter 32-Bit-Windows-Betriebssystemen mit CS Linux 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-Linux-Server zugreifen können:
  - Serverzugriff über ein TCP/IP-Netz
  - Zugriff auf einen WebSphere-Server, der den HTTPS-Zugriff auf CS-Linux-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

© Copyright IBM Corp. 1998, 2021

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 auf andere Windows-PC im Netz kopieren und dann ohne direkten Zugang zur CS-Linux-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 Programmsymbol 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 54 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 57 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-Linux-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 Linux* 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 Softwarelizenzvereinbarung an, die Sie aufmerksam lesen sollten.
3. Wenn Sie den Lizenzbedingungen zustimmen können, wählen Sie `Akzeptieren` aus, um fortzufahren.

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

Das Programm fragt Sie nach der gewünschten Art der Installation:

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

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

Anmerkung: Wenn Sie das SDK installieren möchten, müssen Sie `Developer` auswählen.

5. Wählen Sie die Installationsart aus.

   Das Programm fordert Sie auf, den Namen des Programmordners anzugeben, in dem die Symbole für Remote API Client unter Windows angezeigt werden sollen.

6. Geben Sie den Ordnernamen ein.
7. Falls das Systemverzeichnis `.DLL`-Dateien enthält, deren Namen mit denen der von diesem `Setup`-Programm verwendeten Dateien übereinstimmen, jedoch keine Remote-API-Client-Dateien sind (z. B. Dateien einer anderen SNA-Software), fordert das Programm Sie zur Ausführung eines der folgenden Schritte auf:

   - Kopieren Sie die `.DLL`-Dateien von Remote API Client über die vorhandenen `.DLL`-Dateien.
   - Kopieren Sie die vorhandenen `.DLL`-Dateien in ein Verzeichnis `OTHERSNA`, das ein Unterverzeichnis des Installationsverzeichnisses sein muss. Installieren Sie dann die `.DLL`-Dateien von Remote API Client. Diese Option gibt Ihnen die Möglichkeit, die ursprüngliche Konfiguration vor der Installation von Remote API Client wiederherzustellen, falls Sie die Dateien später deinstallieren. (Lesen Sie dazu den Abschnitt „Remote API Client deinstallieren” auf Seite 62.)
   - 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 Linux*. Falls Sie diese Standardwerte nicht verwenden möchten, können Sie sie wie nachfolgend beschrieben konfigurieren:

Domäne
Geben Sie den Namen der Client-Server-Domäne für CS Linux 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-Linux-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 31.
- 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 Linux suchen soll, indem er eine UDP-Broadcastnachricht an alle Computer in seinem TCP/IP-Teilnetz (bzw. in allen 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 57.

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 An-

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 Softwarelizenzvereinbarung akzeptiert werden.

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

`-accept -s`
Führt die Installation im Hintergrundmodus aus. Die Bedingungen der Softwarelizenzvereinbarung 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.)

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

`-l`*Sprachencode*
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 `-l0x000c` 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`

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

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

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

-v*Server*
Geben Sie den Server an, von dem die 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`.

-u*Server*
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-Linux-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 31.
- 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 Linux suchen soll, indem er eine UDP-Broadcastnachricht an alle Computer in seinem TCP/IP-Teilnetz (bzw. in allen 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.

-a*Zeitlimit*
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.

-b*maximale 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.

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

Geben Sie den Befehl `setup -h -l`*Sprachencode* 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 -l0x0009` ein, um die Hilfeinformationen auf Englisch anzuzeigen. Sie können `-h` durch `-?` ersetzen. Um die Hilfeinformationen auf Spanisch anzuzeigen, können Sie beispielsweise `setup -? -l0x000a` 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-Schlüsselverwaltungsprogram.

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 54 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 Linux* 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 Linux* 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 54 oder im Abschnitt „Remote API Client über die Befehlszeile installieren” auf Seite 57 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 57), 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\sxcluninst -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 Linux konfigurieren und verwenden

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

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

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

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

Das Motif-Verwaltungsprogramm zeigt automatisch Statusinformationen zu CS-Linux-Ressourcen an. Die meisten dieser Informationen werden im Knotenfenster angezeigt (siehe Abschnitt „CS Linux mit dem Motif-Verwaltungsprogramm verwalten" auf Seite 68). 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 Linux definieren oder ändern möchten, müssen Sie zur Anmeldegruppe `sna` gehören.
2. Für die Verwendung des Motif-Verwaltungsprogramms brauchen Sie ein X-Terminal.
3. Zusätzliche Informationen zur Benutzerschnittstelle des Motif-Verwaltungsprogramms, z. B. zu den in den Fenstern angezeigten Schaltflächen und Symbolen, können Sie den Hilfetextanzeigen des Programms und dem *Verwaltungshandbuch für IBM Communications Server für Linux* 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.

Das WebAdmin-Paket ist ein Tool, das separat heruntergeladen werden kann und eine Web-Browser-Schnittstelle zum Verwalten, Konfigurieren und Abfragen von Statusinformationen bereitstellt. Dieses Tool ermöglicht einen sicheren Zugriff, sodass der Administrator Schreib-/Lesezugriff oder nur Lesezugriff auf SNA-Informationen haben kann.

Informationen zu weiteren CS-Linux-Verwaltungstools (u. a. zum Befehlszeilenverwaltungsprogramm und zu NOF-Anwendungsprogrammen) finden Sie im *Verwaltungshandbuch für IBM Communications Server für Linux*, im *Verwaltungshandbuch für IBM Communications Server for Data Center Deployment für Linux* und im *IBM Communications Server for Data Center Deployment on Linux NOF Programmer's Guide*.

© Copyright IBM Corp. 1998, 2021

CS-Linux-Konfiguration planen

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

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

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

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

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

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

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

Planungsblätter

Bevor Sie mit dem Konfigurieren von Ressourcen für CS Linux 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 Linux* 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 Linux definieren

CS Linux steuert Operationen mit einer Reihe von Umgebungsvariablen, die Sie vor der Aktivierung der Software CS Linux auf dem Server festlegen müssen. Am einfachsten ist es, die Variablen in einer Textdatei festzulegen, die CS Linux beim Start liest.

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

```
export LANG=en_US
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
```

Motif-Verwaltungsprogramm verwenden

Bevor Sie das Motif-Verwaltungsprogramm verwenden, sollten Sie zu Ihrer Datei `.login` oder `.profile` Pfadangaben hinzufügen, damit das System ausführbare Programme finden kann (siehe Abschnitt „Pfad zu CS-Linux-Programmen angeben" auf Seite 67). Darüber hinaus müssen Sie die Software CS Linux aktivieren, bevor Sie das Verwaltungsprogramm verwenden können (siehe Abschnitt „CS Linux aktivieren" auf Seite 67).

Informationen zum Aufrufen des Motif-Verwaltungsprogramms und einen Überblick über die Verwendung des Programms finden Sie im Abschnitt „CS Linux mit dem Motif-Verwaltungsprogramm verwalten" auf Seite 68.

Pfad zu CS-Linux-Programmen angeben

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

Das Motif-Verwaltungsprogramm ist im Verzeichnis `/opt/ibm/sna/bin/X11` gespeichert. Die übrigen Programme befinden sich im Verzeichnis `/opt/ibm/sna/bin`. Wenn Sie diese Verzeichnisse zur Definition der Umgebungsvariablen PATH in Ihrer Datei `.login` oder `.profile` hinzufügen, findet CS Linux die Programme automatisch. Alternativ dazu können Sie wie in den folgenden Beispielen den Verzeichnisnamen angeben, wenn Sie das Programm ausführen:

```
/opt/ibm/sna/bin/sna start
```

```
/opt/ibm/sna/bin/X11/xsnaadmin
```

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

CS Linux aktivieren

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

Geben Sie zum Aktivieren von CS Linux an der Linux-Eingabeaufforderung den folgenden Befehl ein:

```
sna start
```

Anmerkung: Wenn Sie den Befehl `sna start` angeben, verwendet die Software CS Linux 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 abhängen, solange die Software CS Linux aktiv ist. Um Probleme zu vermeiden, sollten Sie die Software CS Linux von einem Verzeichnis in einem Dateisystem starten, das nicht abgehängt werden muss.

Sie könnten beispielsweise mit `cd /` das Stammverzeichnis aufrufen, bevor Sie den Befehl `sna start` absetzen.

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

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

CS Linux mit dem Motif-Verwaltungsprogramm verwalten

Stellen Sie vor Verwendung des Motif-Verwaltungsprogramms für CS Linux sicher, dass CS Linux wie im Abschnitt „CS Linux aktivieren" auf Seite 67 beschrieben initialisiert ist. (Gegebenenfalls müssen Sie die Umgebungsvariable `DISPLAY` definieren, um einen geeigneten X-Server anzugeben.)

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

```
xsnaadmin &
```

CS Linux zeigt das Domänenfenster an. Dieses Fenster zeigt alle definierten Knoten an und stellt Optionen für das Aktivieren und Inaktivieren von Knoten bereit. Durch doppeltes Klicken auf einen Knoten wird das in Abbildung 5 auf Seite 69 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 73 beschrieben zu konfigurieren.

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

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

Wenn Sie ein Client-Server-System mit CS Linux 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 5 auf Seite 69 zeigt ein Beispiel für ein Knotenfenster. In der Titelleiste ist der Name des Linux-Systems angegeben.

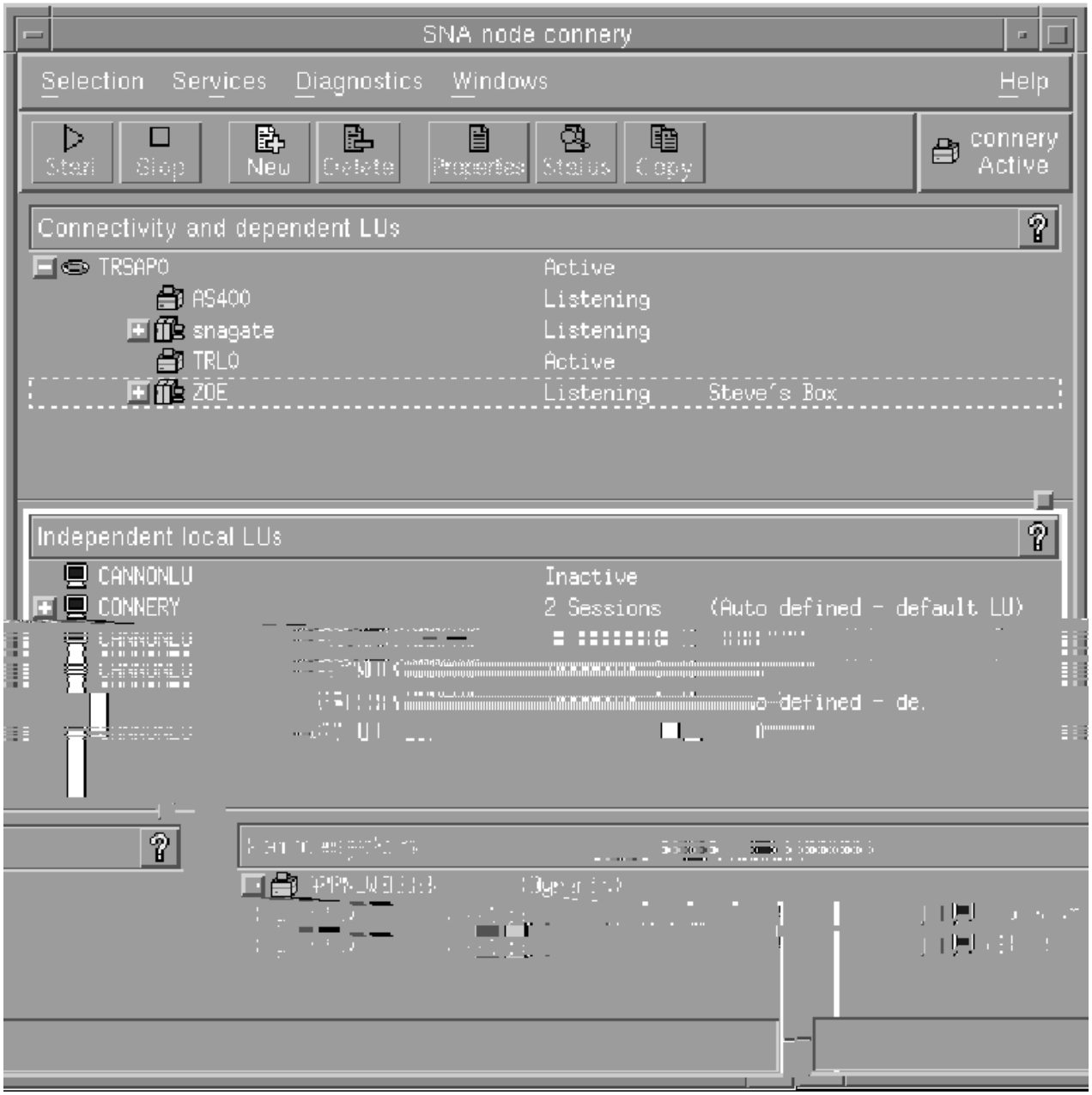


Abbildung 5. Knotenfenster

Im Knotenfenster können Sie alle Ressourcen und Komponenten des CS-Linux-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 aktivieren oder inaktivieren
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`.

Löschen einer Ressource
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. Abbildung 6 auf Seite 71 zeigt eine CS-Linux-Symbolleiste.

Abbildung 6. CS-Linux-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 Linux für die Ausführung in einer Client-Server-Umgebung (mit mehreren CS Linux-Knoten in einem Netz) installiert haben.

In einer Client-Server-Umgebung kann ein Server als Konfigurationsserver markiert werden. CS Linux 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 Linux, 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 Linux 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 Conroller-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 Linux 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 aktivierter Controller-Server erforderlich.

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

Knoten konfigurieren

Der erste Schritt beim Konfigurieren von CS Linux 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.

Sie können den CS-Linux-Knoten als APPN-Netzknoten oder APPN-Endknoten konfigurieren. (Wenn CS Linux für die Kommunikation mit dem Host ausschließlich SNA verwendet, werden Sie den CS-Linux-Knoten wahrscheinlich als Endknoten oder Zweignetzknoten 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.

Stellen Sie vor Beginn der Knotenkonfiguration die folgenden Informationen zusammen:

- Art der APPN-Unterstützung (Netzknoten, Zweignetzknoten, Endknoten).
- 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 Linux zeigt den Dialog für Knotenparameter an.
2. Geben Sie die Ebene der APPN-Unterstützung, den Steuerpunktnamen und (sofern erforderlich) die Standardknoten-ID an.
3. Klicken Sie auf OK, um den Knoten zu definieren. Wenn Sie den Knoten definieren, definiert CS Linux automatisch eine Standard-LU, die denselben Namen wie der Steuerpunkt hat.

   Wenn Sie die Dialoganzeige verlassen wollen, ohne die eingegebenen Werte zu sichern, klicken Sie auf die Schaltfläche `Abbrechen`.

Konnektivität konfigurieren

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

In Ihrem Computer können Adapter für ein oder mehrere Verbindungsprotokoll(e) installiert sein. Viele der Informationen, die Sie beim Konfigurieren der Konnektivität eingeben müssen, hängen vom verwendeten Verbindungsprotokoll ab. Eine Liste der von CS Linux unterstützten Verbindungsprotokolle finden Sie im Abschnitt „Installationsvoraussetzungen” auf Seite 19.

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 Linux* oder in der Onlinehilfe des Motif-Verwaltungsprogramms.

SDLC-Verbindung für abhängigen Datenverkehr konfigurieren

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

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

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

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

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

1. Konfigurieren Sie wie folgt den Port:
   a. Wählen Sie das Konnektivitätsteilfenster aus.
   b. Wählen Sie im Untermenü `Konnektivität` des Menüs `Dienste` den Eintrag `Neuer Port` aus (oder klicken Sie in der Symbolleiste auf 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 Linux den Dialog für SDLC-Ports an.
   d. Geben Sie in den Feldern der Dialoganzeige die entsprechenden Werte ein.
   e. Klicken Sie auf `OK`, um den Port zu definieren.

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

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

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

Ethernet-Verbindung für 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 (für Intel- und OSA2-Adapter in der Regel 04). Für einen OSA-Express-Adapter muss die lokale SAP-Nummer mit der Nummer übereinstimmen, die in der OSA/SF für die E/A-Einheitenadressen definiert wurde, die der ethX-Schnittstelle dieses Linux-Image entsprechen.
- die Information, ob der Port beim Start des Knotens automatisch aktiviert werden soll
- Name des Verbindungsnetzes (muss für alle Ports innerhalb eines Verbindungsnetzes identisch sein)

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

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

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

1. Konfigurieren Sie wie folgt den Port:
   a. Wählen Sie das Konnektivitätsteilfenster aus.
   b. Wählen Sie im Untermenü Konnektivität des Menüs Dienste den Eintrag Neuer Port aus (oder klicken Sie in der Symbolleiste auf 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 Linux den Ethernet-SAP-Dialog an.
   d. Geben Sie in den Feldern der Dialoganzeige die entsprechenden Werte ein.
   e. Klicken Sie auf OK, um den Port zu definieren.

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

      CS Linux zeigt den Dialog für Ethernet-Verbindungsstationen an.
   d. Geben Sie in den Feldern der Dialoganzeige die entsprechenden Werte ein.

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

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

Wenn Sie bei Systemen ohne RHEL7 LLC2-Verbindungen auf einer logischen Linux-Partition eines System z verwenden und der LPAR mehrere CPUs zugeordnet sind, können empfangene Pakete unabhängig von der Reihenfolge ihres Eingangs beim OSA-Adapter in die Warteschlange des SNA-Servers aufgenommen werden und so die Aktivierung der LLC2-Verbindungsstation verindern. Wenn die LLC2-Pakete der Reihe nach empfangen werden sollen, müssen Sie unter Linux RPS (Receive Packet Steering) konfigurieren. Verwenden Sie die Bittabelle rps_cpus, um anzugeben, dass pro Schnittstelle nur eine CPU für die Bearbeitung von LLC2-Paketen verwendet werden soll. Gehen Sie dazu wie folgt vor:

- Stellen Sie fest, welchen Namen die Schnittstelle hat. In der Regel ist dies ein Name wie `eth1` oder `ensp0`.
- Überprüfen Sie die Bittabelle. Sie sollte lauter Nullen enthalten. Die Ausgabe von `cat /sys/class/net/eth1/queues/rx-0/rps_cpus` lautet beispielsweise `00000000,00000000`.
- Setzen Sie in der Tabelle das Bit für die Zuordnung der zu verwendenden CPU. Im Beispiel wird die erste CPU (CPU_0) so definiert, dass sie LLC2-Interrupts von Warteschlangenpaketen mit `echo 1 > /sys/class/net/eth1/queues/rx-0/rps_cpus` behandelt.
- Legen Sie diese RPS-Einstellung als permanent fest. Definieren Sie sie dazu in der Verzeichnisdatei für Klassennetzregeln `/etc/udev/rules.d/70-persistent-net.rules`, indem Sie die Zeichenfolge `ATTR {0}/rps_cpus} = '1'` zur Netzeinstellung der Schnittstelle hinzufügen. Im folgenden Beispiel wird die queth-Einheitennummer 2f20 verwendet: `SUBSYSTEM=="net", ACTION=="add", Drivers=='qeth', KERNELS="0.0.2f20", ATTR{type}=="1",ATTR{queues/rx-0/rps_cpus}="1", KERNEL=="eth*", NAME="eth1"`

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 Linux den Dialog für IP-Ports an.

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

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

Der Port wird im Konnektivitätsteilfenster des Knotenfensters angezeigt.

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

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

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

c. Klicken Sie auf OK.

CS Linux zeigt den Dialog für IP-Verbindungsstationen an.

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

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

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

LUs 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 73 beschrieben.
- Konfigurieren Sie eine Verbindung für abhängigen LU-Datenverkehr. Lesen Sie dazu die Beschreibung im Abschnitt „Konnektivität konfigurieren” auf Seite 73.

  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 86 und „DLUR konfigurieren” auf Seite 88.

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

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

- 3270-Anzeige-LU
- unbeschränkte LU

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 Linux zeigt das Fenster für LU-Pools an.
2. Klicken Sie auf Neu.

   CS Linux zeigt den Konfigurationsdialog für LU-Pools an.

   Im rechten Feld sind LUs aufgelistet, die noch keinem Pool zugeordnet sind. Jede dieser LUs kann in den neuen Pool integriert werden.
3. Wählen Sie die LU oder LUs aus, die Sie zum Pool hinzufügen wollen, und klicken Sie auf 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 Mo-

dus 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 73 beschrieben.
2. Konfigurieren Sie die Konnektivität wie im Abschnitt „Konnektivität konfigurieren" auf Seite 73 beschrieben.

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

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

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

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

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

Benutzen die Anwendungen CPI-C, müssen Sie nach der Konfiguration von APPC möglicherweise zusätzliche Konfigurationsschritte für CPI-C ausführen (siehe Abschnitt „Konfiguration für CPI Communications" auf Seite 84). 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-Linux-Computer das aufrufende Transaktionsprogramm oder Quellen-TP ist (das den Dialog startet), müssen Sie für dieses Transaktionsprogramm möglicherweise Einträge mit Nebeninformationen definieren. Gehen Sie dazu wie im Abschnitt „Konfiguration für CPI Communications" auf Seite 84 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 79) 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 83 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 Linux*.

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 73 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 73 beschrieben. Konfigurieren Sie die Verbindung für die Unterstützung von unabhängigem Verkehr.

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

1. Wählen Sie im Knotenfenster den Port aus.
2. Klicken Sie auf `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 73 beschrieben. Wählen Sie für das Feld *APPN-Unterstützung* den Wert `Endknoten` aus.
2. Konfigurieren Sie die Konnektivität wie im Abschnitt „Konnektivität konfigurieren” auf Seite 73 beschrieben. Konfigurieren Sie die Verbindung für die Unterstützung von unabhängigem Verkehr und geben Sie für die Verbindungsstation die folgenden Informationen an:
   - Geben Sie für das Feld *Ferner Knoten* als Wert den Namen des Netzknotens ein (siehe Abschnitt „Netzknoten konfigurieren” auf Seite 80).
   - Geben Sie im Teilfenster 'Verbindungsinformationen' des Konfigurationsdialogs für die Verbindungsstation die MAC-Adresse und die SAP-Nummer des Ports auf dem Netzknoten ein.

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

Konnektivität zwischen zwei Knoten prüfen

In diesem Szenario wird vorausgesetzt, dass Sie einen Netzknoten gemäß der Beschreibung im Abschnitt „Netzknoten konfigurieren” auf Seite 80 und einen Endknoten gemäß der Beschreibung im Abschnitt „Endknoten konfigurieren” auf Seite 80 konfiguriert haben. Auf dem Endknoten können Sie die folgenden Schritte ausführen:

1. Wählen Sie im Knotenfenster die Verbindungsstation zum benachbarten Netzknoten aus.
2. Klicken Sie auf `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`).

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

Partner-LUs für einen LEN-Knoten konfigurieren

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

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

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

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

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

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

Mit dem Motif-Verwaltungsprogramm können Sie einen Aliasnamen für eine Partner-LU hinzufügen (siehe Abschnitt „Aliasnamen für Partner-LU definieren" auf Seite 82), eine Definition für eine Partner-LU auf

einem bestimmten fernen Knoten hinzufügen (siehe Abschnitt „Partner-LU auf einem fernen Knoten definieren” auf Seite 82) oder mehrere Partner-LUs unter Verwendung von Platzhaltern definieren (siehe Abschnitt „Mehrere Partner-LUs mit Platzhaltern definieren” auf Seite 83).

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

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

Aliasnamen für Partner-LU definieren

Für das Definieren des Aliasnamens einer Partner-LU benötigen Sie die folgenden Informationen:

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

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

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

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

Partner-LU auf einem fernen Knoten definieren

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

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

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

1. Wählen Sie den fernen Knoten aus.
2. Wählen Sie im Menü `Dienste` die Optionen APPC, `Neue Partner-LUs` und `Partner-LU auf fernem Knoten` aus (oder klicken Sie in der Symbolleiste auf die Schaltfläche Neu und wählen Sie die Option `Partner-LU auf fernem Knoten definieren` aus).

CS Linux zeigt den Konfigurationsdialog für Partner-LUs an.

3. Geben Sie in den Feldern der Dialoganzeige die entsprechenden Werte ein.
4. Klicken Sie auf OK, um die Partner-LU zu definieren. Der Aliasname der Partner-LU wird im Teilfenster für ferne Systeme des Knotenfensters unter dem fernen System angezeigt, zu dem die Partner-LU gehört.

Mehrere Partner-LUs 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,

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 Linux zeigt den Dialog für lokale LUs an.
3. Geben Sie in den Feldern der Dialoganzeige die entsprechenden Werte ein.
4. Klicken Sie auf OK, um die lokale LU zu definieren. Die abhängige LU wird im Konnektivitätsteilfenster unterhalb der Verbindungsstation angezeigt, zu der sie gehört.

Konfiguration für CPI Communications

Wenn Ihr System eine CPI-C-Anwendung unterstützt, die symbolische CPI-C-Bestimmungsorte verwendet, müssen Sie die CPI-C-Nebeninformationen definieren. Die Nebeninformationen ordnen dem symbolischen Bestimmungsort Informationen zum Partner-TP, zur Partner-LU, zum Modus und zur Dialogsicherheit zu.

Den symbolischen Bestimmungsort für CPI-C kann Ihnen der Anwendungsentwickler nennen. (Für Anwendungen eines anderen Herstellers können Sie den Bestimmungsort der Produktdokumentation entnehmen.)

Bevor Sie CPI-C-Nebeninformationen konfigurieren, benötigen Sie die folgenden Informationen:

- den Vom Transaktionsprogramm (TP) verwendeten symbolischen Bestimmungsort
- den Namen des Partner-TP
- den Namen oder Aliasnamen der Partner-LU
- den Modusnamen

Führen Sie im Knotenfenster die folgenden Schritte aus, um CPI-C-Nebeninformationen zu konfigurieren:

1. Wählen Sie im Untermenü APPC des Menüs `Dienste` den Eintrag `CPI-C` aus.

   CS Linux zeigt das Fenster für CPI-C-Bestimmungsorte an.
2. Klicken Sie auf Neu.

   CS Linux zeigt den Konfigurationsdialog für CPI-C-Bestimmungsorte an.
3. Geben Sie in den Feldern der Dialoganzeige die entsprechenden Werte ein.
4. Klicken Sie auf OK, um die CPI-C-Nebeninformationen zu definieren.

LUA konfigurieren

Die API LUA ist für Anwendungen geeignet, die über LUs 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 73 beschrieben.
2. Konfigurieren Sie Konnektivität für abhängigen Verkehr wie im Abschnitt „Konnektivität konfigurieren” auf Seite 73 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 78 beschrieben.

LU-Pool definieren

Sie können LU-Pools definieren, um die Benutzerkonfiguration zu vereinfachen und beim Aufbauen von Hostsitzungen mehr Flexibilität zu haben. Sie können beispielsweise mehrere LUs in einem Pool definieren und dann mehrere LUA-Anwendungen für die Verwendung dieses Pools konfigurieren. Dadurch wird die Konfiguration von Anwendungen einfacher, und alle Anwendungen können jede beliebige LU des Pools benutzen.

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

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

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

Zu einem Pool für 3270 können Sie LUs der folgenden Typen hinzufügen (ein Pool darf keine Mischung verschiedener LU-Typen enthalten):

- 3270-Anzeige-LU
- unbeschränkte LU

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

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

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

   CS Linux zeigt das Fenster für LU-Pools an.
2. Klicken Sie auf Neu.

   CS Linux zeigt den Konfigurationsdialog für LU-Pools an.

   Im rechten Feld sind LUs aufgelistet, die noch keinem Pool zugeordnet sind. Jede dieser LUs vom Typ Unbeschränkte LU kann in den neuen Pool für LUA integriert werden.
3. Wählen Sie die LU oder LUs aus, die Sie zum Pool hinzufügen wollen, und klicken Sie auf 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.

SNA Gateway konfigurieren

CS Linux ermöglicht nicht nur den Direktzugriff auf einen Host, sondern kann auch SNA-Gateway-Funktionen bereitstellen. Mit Hilfe dieses Features können andere Computer über einen CS-Linux-Knoten auf einen Host zugreifen, so dass keine gesonderte Verbindung von jedem einzelnen Computer zum Host erforderlich ist.

Das Feature SNA Gateway ist in Abbildung 7 auf Seite 86 veranschaulicht.

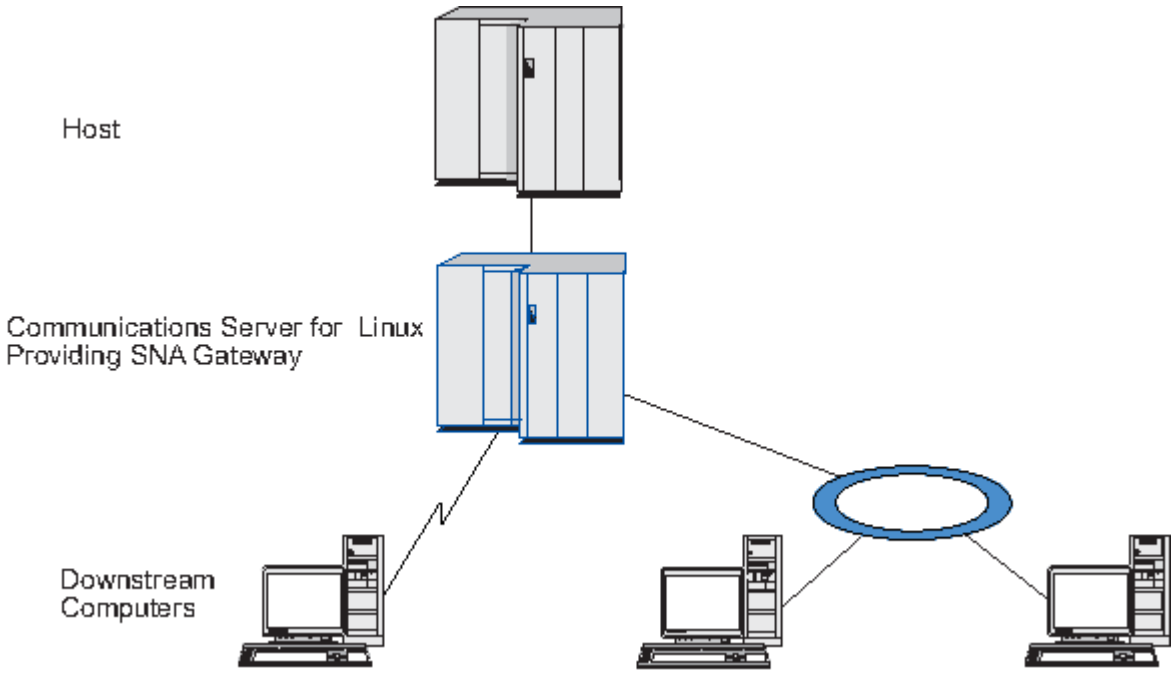


Abbildung 7. SNA Gateway

Der untergeordnete Computer muss über eine SNA-PU des Typs 2.0 oder 2.1 verfügen, um abhängige LUs unterstützen zu können. Der untergeordnete Computer könnte beispielsweise ein weiterer CS-Linux-Computer oder ein PC sein, auf dem Communications Server für Windows ausgeführt wird.

Wenn der lokale CS-Linux-Knoten das Feature SNA Gateway nutzt, werden alle Daten, die zwischen dem Host und dem untergeordneten Computer übertragen werden, über den lokalen Knoten geleitet. Dadurch benötigt der untergeordnete Computer keine Direktverbindung und kann die Hostverbindung gemeinsam mit CS Linux oder mit anderen untergeordneten Computern nutzen. Sie könnten z. B. mehrere untergeordnete Computer installieren, die über ein lokales Token-Ring-Netz mit CS Linux verbunden sind. In diesem Fall könnten alle Computer auf dieselbe Standfernleitung von CS Linux zum Host zugreifen.

Die Verwendung von SNA Gateway vereinfacht darüber hinaus die Konfiguration auf dem Host, denn Sie müssen die untergeordneten Computer und die zu diesen führenden DFV-Verbindungen nicht definieren. Die Hostkonfiguration muss nur den CS-Linux-Computer und dessen Hostübertragungsleitung umfassen. Die LUs auf den untergeordneten Computern werden als Teil der Ressourcen des CS-Linux-Computers konfiguriert. Der Host hat keine Kenntnis von der Verwendung des Features SNA Gateway.

Bevor Sie SNA Gateway konfigurieren, müssen Sie die folgenden Konfigurationsschritte ausführen:

- Definieren Sie den lokalen Knoten wie im Abschnitt „Knoten konfigurieren” auf Seite 73 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 73 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 87).

- 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 78 beschrieben.

Implizite untergeordnete LUs unterstützen

Zur Unterstützung untergeordneter LUs, die noch nicht für CS Linux definiert wurden, können Sie für den Port eine Schablone für implizite untergeordnete PUs und LUs definieren. (Die wichtigsten Schritte der Port-Konfiguration sind im Abschnitt „Konnektivität konfigurieren" auf Seite 73 beschrieben.) Diese Schablonen bieten Unterstützung für untergeordnete LUs, so dass Sie nicht jede LU auf dem lokalen Knoten für die Unterstützung aller LUs auf einem untergeordneten Knoten konfigurieren müssen.

Bevor Sie eine untergeordnete LU für SNA Gateway konfigurieren, benötigen Sie die folgenden Informationen:

- Bereich der LUs (Nummern), die untergeordnete LUs unterstützen
- Name der Host-LU

Führen Sie die folgenden Schritte aus, um eine Schablone für implizite untergeordnete LUs zu definieren:

1. Wenn Sie den Port bereits konfiguriert haben, klicken Sie im Konnektivitätsteilfenster des Knotenfensters doppelt auf die Port-Definition. CS Linux zeigt den Konfigurationsdialog für Ports an.

   Sollten Sie den Port noch nicht konfiguriert haben, holen Sie dies jetzt nach. Gehen Sie dazu wie folgt vor:

   a. Wählen Sie im Knotenfenster das Konnektivitätsteilfenster aus.
   b. Klicken Sie auf `Neu`.
   c. Wählen Sie in der daraufhin erscheinenden Dialoganzeige die Option zum Definieren eines Ports und den Verbindungsprotokolltyp aus.

      CS Linux zeigt den Konfigurationsdialog für Ports an.
   d. Geben Sie gemäß der Beschreibung im Abschnitt „Konnektivität konfigurieren" auf Seite 73 die wichtigsten Port-Parameter ein.
2. Klicken Sie unten in der Dialoganzeige auf die Schaltfläche `Erweitert`.

   CS Linux zeigt 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 Linux zeigt den Konfigurationsdialog für Schablonen für untergeordnete LUs an.
5. Geben Sie in den Feldern der Dialoganzeige die entsprechenden Werte ein.
6. Klicken Sie auf `OK`, um die Schablone für implizite untergeordnete LUs zu definieren.

Untergeordnete LUs definieren

Bevor Sie eine untergeordnete LU für SNA Gateway konfigurieren, benötigen Sie die folgenden Informationen:

- LU-Name jeder untergeordneten LU (Dies ist ein lokaler Bezeichner, der nicht mit der Konfiguration des untergeordneten Systems übereinstimmen muss.)
- LU-Nummer jeder untergeordneten LU
- Verbindungsstation zum untergeordneten Knoten
- Name der übergeordneten LU (für die Host-LU)

Führen Sie die folgenden Schritte aus, um eine untergeordnete LU für SNA Gateway zu konfigurieren:

1. Wählen Sie im Konnektivitätsteilfenster des Knotenfensters die Verbindungsstation zum untergeordneten Knoten aus.
2. Klicken Sie auf Neu.
3. Wählen Sie die Option `Neue untergeordnete` LU aus und klicken Sie auf OK.

   CS Linux zeigt den Dialog für untergeordnete LUs an.
4. Geben Sie in den Feldern der Dialoganzeige die entsprechenden Werte ein.
5. Klicken Sie auf OK, um die untergeordnete LU zu definieren.

   Die LU-Definition wird im Konnektivitätsteilfenster des Knotenfensters unterhalb der Verbindungsstation zum untergeordneten Knoten angezeigt.

DLUR konfigurieren

CS Linux ermöglicht nicht nur den Direktzugriff auf einen Host, sondern kann auch DLUR-Funktionen bereitstellen. Bei Verwendung dieses Features können sich Sitzungen für abhängige LUs über mehrere Knoten in einem APPN-Netz erstrecken und benötigen keine Direktverbindung zum Host.

Normalerweise erfordert eine abhängige LU-Sitzung eine direkte DFV-Verbindung zum Host. Wenn in einem APPN-Netz viele Knoten (einschließlich eines Hostknotens) verbunden sind, haben einige von ihnen unter Umständen keine Direktverbindung zum Host, sondern nur eine indirekte Verbindung über einen anderen Knoten. LUs auf diesen indirekt mit dem Host verbundenen Knoten können keine abhängigen LU-Sitzungen mit dem Host aufbauen.

Dependent LU Requester (DLUR) ist ein APPN-Feature, das diese Einschränkung aufhebt.

Das Feature DLUR auf einem APPN-Knoten (z. B. einem CS-Linux-Knoten) arbeitet mit DLUS (Dependent LU Server) auf dem Host zusammen, um Sitzungen von abhängigen LUs auf dem DLUR-Knoten über das APPN-Netz zum DLUS-Host weiterzuleiten. Die Route zum Host kann sich über mehrere Knoten erstrecken und von den APPN-Funktionen für Netzverwaltung, für dynamische Ressourcenlokalisierung und Routenberechnung profitieren. DLUR muss auf dem Knoten verfügbar sein, auf dem sich die LUs befinden. DLUS muss auf dem Hostknoten verfügbar sein. Auf den Zwischenknoten der Sitzungsroute ist das Feature DLUR nicht erforderlich.

Wenn der CS-Linux-DLUR-Knoten ein Netzknoten oder ein Zweignetzknoten ist, kann er auch Durchgriff-DLUR-Funktionen für abhängige LUs auf untergeordneten Computern, die mit dem CS-Linux-Knoten verbunden sind, bereitstellen. Diese LUs können ebenso wie knoteninterne LUs DLUR auf dem CS-Linux-Knoten nutzen, um über das Netz auf den Host zuzugreifen. Die untergeordneten Computer führen DLUR nicht aus und müssen keine Kenntnis davon haben, dass DLUR verwendet wird.

Abbildung 8 auf Seite 89 zeigt einen als APPN-Netzknoten konfigurierten CS-Linux-Server mit einer Implementierung von Durchgriff-DLUR zur Unterstützung von Sitzungen zwischen LUs auf dem Host (dem übergeordneten Knoten) und LUs auf den Knoten im APPN Netz (untergeordneten Knoten).

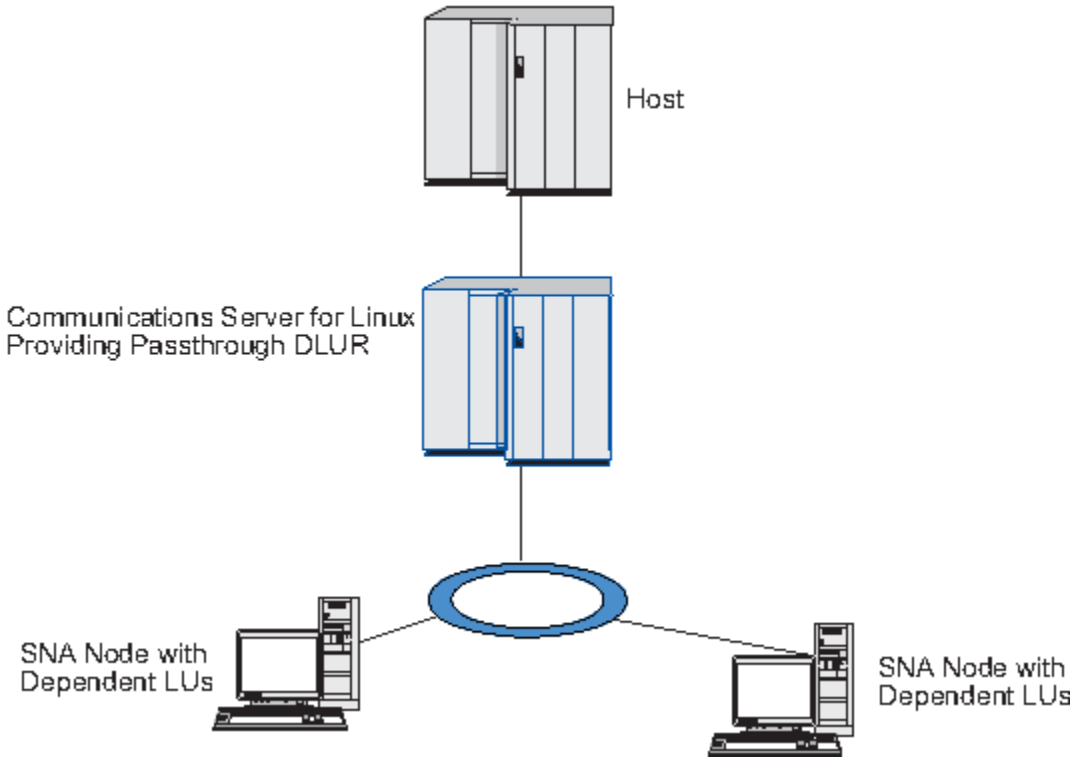


Abbildung 8. CS-Linux-Knoten, der DLUR bereitstellt

Anmerkung:

1. Auf einem LEN-Knoten können Sie DLUR nicht konfigurieren.
2. Durchgriff-DLUR können Sie nur auf einem Netzknoten oder Zweignetzknoten konfigurieren.
3. Wenn Sie Branch Extender verwenden, können Sie DLUR nicht auf einem Endknoten des Zweignetzes (dessen Netzknotenserver ein Zweignetzknoten ist) konfigurieren. Dieser Knoten kann jedoch abhängige LU-Anwendungen unterstützen, sofern Sie Durchgriff-DLUR auf den Zweignetzknoten konfigurieren (so dass der Endknoten im Zweignetz zwar nicht DLUR ausführt, jedoch Durchgriff-DLUR auf dem Zweignetzknoten verwendet).

Die für die DLUR-Konfiguration erforderlichen Schritte richten sich danach, ob sich die abhängigen LUs auf dem lokalen Knoten oder auf untergeordneten Knoten befinden.

DLUR-Unterstützung auf dem lokalen Knoten konfigurieren

Für diese Aufgabe benötigen Sie die folgenden Informationen:

- PU-ID der PU auf dem lokalen Knoten
- PU-Name (Dies ist ein lokaler Bezeichner, der nicht mit der Hostkonfiguration übereinstimmen muss.)
- Name des DLUS auf dem Host (und ggf. Name des Ausweich-DLUS)
- LU-Name, LU-Nummer und LU-Typ aller untergeordneten LUs. Die LU-Nummer muss mit der auf dem Host konfigurierten Nummer übereinstimmen.

Zum Konfigurieren der DLUR-Unterstützung auf dem lokalen Knoten müssen Sie die folgenden Konfigurationsschritte ausführen:

1. Definieren Sie den lokalen Knoten wie im Abschnitt „Knoten konfigurieren” auf Seite 73 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 73.

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 Linux den Konfigurationsdialog für DLUR-PUs an.

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

   c. Klicken Sie auf OK, um die DLUR-PU zu definieren.

      Die DLUR-PU wird im Konnektivitätsteilfenster unter dem DLUR-Eintrag angezeigt.

4. Wenn Sie DLUR für die Unterstützung von LUs auf dem lokalen Knoten konfigurieren wollen, müssen Sie die LUs auf dem lokalen Knoten hinzufügen. Die LUs müssen wie im Abschnitt „LUA konfigurieren” auf Seite 84 beschrieben für die Unterstützung von LUA konfiguriert werden. In Abhängigkeit von den Anforderungen der von den LUs unterstützten Benutzeranwendungen können weitere Konfigurationsschritte erforderlich sein.

Durchgriff-DLUR-Unterstützung für untergeordnete Knoten konfigurieren

Für diese Aufgabe benötigen Sie die folgenden Informationen:

- Name der untergeordneten PU für jeden untergeordneten Knoten oder für jede PU auf dem untergeordneten Knoten (Dies ist ein lokaler Bezeichner, der nicht mit der Hostkonfiguration übereinstimmen muss.)
- Name des DLUS auf dem Host

Zum Konfigurieren der Durchgriff-DLUR-Unterstützung für untergeordnete Knoten müssen Sie die folgenden Konfigurationsschritte ausführen:

1. Definieren Sie den lokalen Knoten als APPN-Netzknoten (siehe Abschnitt „Knoten konfigurieren” auf Seite 73).
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 73 beschrieben vor. (Sie müssen keine DLUR-PU für die Unterstützung von Durchgriff-DLUR für untergeordnete Knoten definieren.)
3. Ein untergeordneter Knoten kann mehrere PUs unterstützen. In einem solchen Fall ist jede untergeordnete PU einer anderen Verbindung zugeordnet, so dass Sie zwischen dem CS-Linux-DLUR-Knoten und dem untergeordneten Knoten mehrere Verbindungen konfigurieren und für jede Verbindung den Namen der untergeordneten PU kennen müssen.

TN Server konfigurieren

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

Einige TN3270-Programme bieten Unterstützung für TN3270E (Standarderweiterungen für Telnet 3270). TN3270E ist ein offenes Protokoll, das über Telnet die 3270-Einheitenemulation (von Terminals und Druckern) unterstützt. Das Protokoll ermöglicht einem Telnet-Client, eine bestimmte Einheit (durch Angabe des LU-Namens) auszuwählen, und stellt erweiterte Unterstützung für verschiedene Funktionen bereit, z. B. für die Schlüssel ATTN und SYSREQ und die Bearbeitung von SNA-Antworten.

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

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

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

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

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

Für jeden Benutzer von TN Server, der mit dem Feature TN3270 Server eine Verbindung zu CS Linux herstellt, ist normalerweise der Zugriff auf eine 3270-LU konfiguriert, so dass der Benutzer auf eine Hostsitzung beschränkt ist. Sie müssen einem Benutzer von TN Server jedoch nicht eine einzelne dedizierte 3270-LU zuordnen, sondern können für ihn auch den Zugriff auf einen Pool von 3270-LUs konfigurieren. Dadurch können Benutzer auf so viele TN-Server-Sitzungen zugreifen, wie LUs im Pool verfügbar sind.

Bevor Sie den Zugriff auf TN Server konfigurieren können, müssen Sie die folgenden Konfigurationsschritte ausführen:

- Definieren Sie den lokalen Knoten wie im Abschnitt „Knoten konfigurieren” auf Seite 73 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 73 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 91.
- Wenn Sie LU-Pools verwenden wollen, definieren Sie diese wie im Abschnitt „LU-Pool definieren” auf Seite 92 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 Linux 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-Linux-Knoten werden im Fenster für LU-Pools angezeigt. Dieses Fenster listet die auf dem lokalen System konfigurierten LU-Pools auf. Sie können in diesem Fenster LUs auswählen und zu einem LU-Pool hinzufügen.

Zu einem Pool für 3270 können Sie LUs der folgenden Typen hinzufügen (ein Pool darf keine Mischung verschiedener LU-Typen enthalten):

- 3270-Anzeige-LU
- unbeschränkte LU

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

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

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

   CS Linux zeigt das Fenster für LU-Pools an.
2. Klicken Sie auf `Neu`.

   CS Linux zeigt den Konfigurationsdialog für LU-Pools an.

   Im rechten Feld sind LUs aufgelistet, die noch keinem Pool zugeordnet sind. Jede dieser LUs kann in den neuen Pool integriert werden.
3. Wählen Sie die LU oder LUs aus, die Sie zum Pool hinzufügen wollen, und klicken Sie auf 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.

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.)

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 Linux zeigt daraufhin das TN-Server-Fenster an, in dessen oberem Teilfenster alle konfigurierten TN-Server-Zugriffseinträge und in dessen unterem Teilfenster alle TN-Server-Zuordnungseinträge aufgelistet sind.
   b. Wählen Sie das Teilfenster mit den TN3270-Zugriffseinträgen aus und klicken Sie auf die Schaltfläche `Neu`.

      CS Linux zeigt den Dialog für TN-Server-Zugriff an.
   c. Geben Sie in den Feldern der Dialoganzeige die entsprechenden Werte ein.
   d. Klicken Sie auf `OK`, um den TN-Server-Zugriffseintrag zu definieren. Der Eintrag wird im TN-Server-Fenster angezeigt.
2. Definieren Sie wie folgt einen TN-Server-Zugordnungseintrag:
   a. Wählen Sie im TN-Server-Fenster das Teilfenster mit den Zuordnungseinträgen aus und klicken Sie auf die Schaltfläche `Neu`.

      CS Linux zeigt den Dialog für TN-Server-Zuordnungseinträge an.
   b. Geben Sie in den Feldern der Dialoganzeige die entsprechenden Werte ein.
   c. Klicken Sie auf `OK`, um den TN-Server-Zuordnungseintrag zu definieren. Der Eintrag wird im TN-Server-Fenster angezeigt.
3. Falls Sie Druckerantworten erzwingen möchten, geben Sie für alle TN3270-Sitzungen eine Keepalive-Methode an. Geben Sie außerdem an, wie auf den externen LDAP-Server mit der Liste zur Überprüfung der Berechtigung von TN3270-Clients zugegriffen werden soll, oder verwenden Sie TN3270-SLP (Service Location Protocol). Diese Angaben können Sie im Dialog mit den erweiterten Parametern für TN Server machen.

Weitere Informationen zum Konfigurieren der SSL-Unterstützung für TN Server finden Sie auf den Supportwebseiten zu IBM Communications Server unter der Adresse https://www.ibm.com/mysupport/s/topic/0TO0z0000006v3OGAQ/communication-server.

TN Redirector konfigurieren

Das CS-Linux-Feature TN Redirector ermöglicht 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 Linux und CS Linux wiederum über eine weitere TCP/IP-Verbindung mit dem Host. Auf diese Weise kann bei Bedarf eine SSL-Sicherheitsprüfung (Secure Sockets Layer) durchgeführt werden, ohne diese auf die gesamte Benutzerhostverbindung zu erstrecken. Beispiele:

- Wenn Clients zu CS Linux eine Verbindung über ein TCP/IP-LAN ohne erforderliche Überprüfung herstellen, jedoch eine Verbindung zu einem fernen Host herstellen, der SSL erfordert, können Sie SSL für die TCP/IP-Verbindung zwischen CS Linux und dem Host verwenden. Auf diese Weise wird die Sicherheit für alle Clients überprüft. Die einzelnen Clients müssen keine Sicherheitsangaben machen.
- Wenn CS Linux 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 Linux verwenden und müssen die SSL-Software nicht auf dem Host installieren.

TN Redirector konfigurieren

Bevor Sie den Zugriff auf TN Redirector konfigurieren können, müssen Sie den lokalen Knoten wie im Abschnitt „Knoten konfigurieren” auf Seite 73 beschrieben definieren. Außerdem benötigen Sie die folgenden Informationen:

- Wenn nur bestimmte Clients zulässig sind, benötigen Sie den TCP/IP-Namen oder die TCP/IP-Adresse des Clients.
- die Nummer des vom Client für die Verbindung zum TN-Redirector-Knoten verwendeten TCP/IP-Ports
- den TCP/IP-Namen oder die TCP/IP-Adresse des Hosts
- die Nummer des vom TN-Redirector-Knoten für die Verbindung zum Host verwendeten TCP/IP-Ports
- die Information, ob zwischen dem Client und dem TN-Redirector-Knoten SSL-Datenverschlüsselung, 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 Linux zeigt daraufhin das TN-Server-Fenster an, in dem alle konfigurierten Zugriffseinträge und Zuordnungseinträge für TN3270 Server sowie alle Zugriffseinträge für TN Redirector aufgelistet sind.
2. Wählen Sie das Teilfenster mit den TN-Redirector-Zugriffseinträgen aus und klicken Sie auf die Schaltfläche `Neu`.

   CS Linux zeigt den Dialog für TN-Redirector-Zugriff an.
3. Geben Sie in den Feldern der Dialoganzeige die entsprechenden Werte ein.
4. Klicken Sie auf OK, um den TN-Redirector-Zugriffseintrag zu definieren. Der Eintrag wird im TN-Redirector-Teilfenster des TN-Server-Fensters angezeigt.

Anmerkung: Obwohl TN Redirector keine der SNA-Ressourcen des Knotens verwendet, muss der SNA-Knoten für die Verwendung von TN Redirector aktiv sein.

CS Linux inaktivieren

Durch Inaktivierung der Software CS Linux werden automatisch der CS-Linux-Knoten und die zugehörigen Konnektivitätskomponenten gestoppt. Nach Inaktivierung von CS Linux können andere Prozesse (z. B. eine LUA-Anwendung) auf diesem Server keine CS-Linux-Ressourcen mehr verwenden.

Sie sollten in der Regel nur einzelne Dienste stoppen, wenn diese von den Benutzern nicht mehr benötigt werden. Eine Inaktivierung des Systems ist nur anzuraten, wenn keine CS-Linux-Aktivität vorliegt.

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

Wenn Sie die Software CS Linux inaktivieren, werden Anwendungen, die die API APPC, CSV, LUA, NOF oder MS benutzen, durch einen Rückkehrcode `COMM_SUBSYSTEM_ABENDED` und CPI-C-Anwendungen durch einen Rückkehrcode `CM_PRODUCT_SPECIFIC_ERROR` benachrichtigt.

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

```
sna stop
```

Wenn CS Linux erfolgreich inaktiviert wurde, gibt `sna stop` den Exit-Code `0` zurück. Jeder andere Exit-Code gibt an, dass ein Fehler aufgetreten ist und die Software CS Linux nicht inaktiviert wurde. Weitere Informationen zu den Werten von Exit-Codes finden Sie im *IBM Communications Server for Data Center Deployment on Linux Diagnostics Guide*.

Automatischer Start von CS Linux

Das Starten von CS Linux bis zur vollen Betriebsbereitschaft kann als ein Prozess mit mehreren Schritten betrachtet werden:

- Aktivieren der Software CS Linux
- Initialisieren des SNA-Knotens
- Aktivieren der Ports und Verbindungsstationen, die auf dem Knoten konfiguriert sind.

Jeder dieser Schritte kann einzeln verwaltet werden. Gegebenenfalls können alle Schritte zur Boot-Zeit ausgeführt werden. Im verbleibenden Teil dieses Abschnitts sind diese Schritte beschrieben. Außerdem wird erläutert, wie die Schritte zur Boot-Zeit gesteuert werden können.

CS Linux aktivieren

Für den Betrieb von CS Linux müssen mehrere Kernel-Module geladen werden. Diese Module werden geladen, wenn Sie die Software CS Linux zum ersten Mal aktivieren, und erst wieder entladen, wenn Sie die Kernel-Ausführungsstufe ändern.

CS Linux erfordert außerdem, dass eine Reihe von Dämonen (Programmen) aktiv ist. Sie können CS Linux erst konfigurieren oder verwenden, wenn diese Dämonen aktiv sind.

- Setzen Sie den Befehl `sna start` ab, um die Dämonen zu starten und die Software CS Linux zu aktivieren.
- Setzen Sie den Befehl `sna stop` ab, um die Dämonen zu stoppen und die Software CS Linux zu inaktivieren.

Initialisieren des SNA-Knotens

Wenn die Software CS Linux aktiviert ist, können Sie den SNA-Knoten und seine Ressourcen konfigurieren. In der Regel werden Sie dazu das Motif-Verwaltungsprogramm xsnaadmin verwenden. Der Knoten kann jedoch erst verwendet werden, nachdem er initialisiert wurde. Sie können ihn im Befehlszeilenverwaltungsprogramm mit dem Befehl `snaadmin init_node` oder im Motif-Verwaltungsprogramm xsnaadmin initialisieren.

Ports und Verbindungsstationen aktivieren

Ports und Verbindungsstationen können so konfiguriert werden, dass sie unter verschiedenen Umständen gestartet werden:

- Nur per Bedienereingriff
- Bedarfsgesteuert (wenn eine Anwendung gestartet wird, die eine Ressource der Verbindung verwendet)
- Beim Start des Knotens (wenn der Befehl `snaadmin init_node` abgesetzt oder der Knoten im Motif-Verwaltungsprogramm gestartet wird).

Der Start durch den Bediener ist die Standardeinstellung. Sie können diese Einstellung für einen bestimmten Port bzw. eine bestimmte Verbindung ändern. Verwenden Sie dazu das Befehlszeilenverwaltungsprogramm oder das Motif-Verwaltungsprogramm.

Anmerkung: Wenn ein Port gestartet wurde, kann er Anrufe von anderen Computern empfangen, jedoch keine abgehenden Anrufe durchführen. Das Starten einer Verbindungsstation bedeutet, dass CS Linux versucht, Kontakt zum fernen Computer aufzunehmen.

CS Linux beim Warmstart starten

CS Linux wird wie andere Linux-Dienste beim Warmstart aktiviert. Das heißt, nach einem Warmstart wird standardmäßig der Befehl `sna start` abgesetzt, der SNA-Knoten jedoch nicht gestartet.

Diese Initialisierung wird im Boot-Initialisierungs-Script von CS Linux `/etc/rc.d/init.d/snastart` ausgeführt. Wie für Start-Scripts üblich, ist dieses Script mit `/etc/rc?.d/init.d/snastart` für die verschiedenen Boot-Ebenen verknüpft.

Sie können `/etc/rc.d/init.d/snastart` bearbeiten und die Aktionen beim Warmstart ändern. Die häufigste Änderung ist das Hinzufügen der Knoteninitialisierung. Der Befehl hierfür, `snaadmin init_node`, ist bereits in der Datei enthalten, jedoch auf Kommentar gesetzt. Sie müssen somit nur das Kommentarzeichen vor dem Befehl entfernen. Wenn Sie diesen Befehl aufnehmen, lösen Sie auch die Aktivierung von Ports und Verbindungsstationen aus, deren Aktivierung beim Start des Knotens konfiguriert ist.

Anwendungen, die CS Linux verwenden, sollten erst nach der Initialisierung des Knotens gestartet werden. Gegebenenfalls können Sie diese Anwendungen automatisch beim Booten starten und alle weiteren `snaadmin`-Befehle, die zur Boot-Zeit ausgeführt werden sollen, auf eine der beiden folgenden Arten hinzufügen:

- Fügen Sie die Befehle am Ende von `/etc/rc.d/init.d/snastart` nach dem Befehl `snaadmin init_node` hinzu.
- Erstellen Sie ein Script `/etc/rc?.d/init.d` mit einer Zahl größer als 95. Dadurch wird sichergestellt, dass das Script nach dem Start von CS Linux ausgeführt wird und die Befehle zu diesem Script hinzugefügt werden.

Anmerkung: Änderungen, die Sie an der Datei `/etc/rc.d/init.d/snastart` vornehmen, werden nicht gespeichert, wenn Sie für CS Linux ein Upgrade auf eine neuere Version durchführen. Vergewissern Sie sich stets, dass Sie eine Kopie der Änderungen haben, damit Sie sie nach einem Upgrade erneut anwenden können.

Kapitel 9. Informationsquellen für CS Linux und SNA

In diesem Kapitel werden die verschiedenen Veröffentlichungen der SNA-Bibliothek erläutert, die Informationen zur SNA-Technologie sowie zu zahlreichen Netzprodukten und Services von IBM enthalten. Außerdem wird erläutert, welche Informationen über Netzforen verfügbar sind.

SNA-Bibliothek

Die SNA-Bibliothek enthält Marketingbroschüren, Bücher, Benutzerhandbücher und Lernprogramme mit Einführungsinformationen sowie weiterführende Informationen zu folgenden Themen:

- SNA-Theorie
- SNA-Produkte
- Produktimplementierung
- System- und Netzkonfigurationen
- SNA-Anwendungsprogramme und -APIs
- Gesamtplanung, Leistung und Optimierung
- Problemanalyse
- Netzverwaltung
- Netzsicherheit

Sie können alle IBM Veröffentlichungen bei Ihrem IBM Ansprechpartner oder bei der örtlichen IBM Niederlassung anfordern.

Eine Liste der wichtigsten Veröffentlichungen zu CS Linux 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 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 zu IBM Software für den Netzbetrieb, einschließlich CS Linux, zugreifen. Gezielte Informationen zu CS Linux finden Sie unter https://www.ibm.com/products/communications-server-for-data-center.

Ausführlichere Hinweise zur Unterstützung für CS Linux 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.

© Copyright IBM Corp. 1998, 2021

Information zu IBM Software können Sie unter http://www.ibm.com/software abrufen. Von dieser Seite aus sind Verbindungen zu Seiten für CS Linux und alle IBM Softwareserver verfügbar.

Empfohlene Literatur

Wenn Sie Ihre Kenntnisse zur SNA vertiefen wollen, finden Sie in den folgenden Veröffentlichungen theoretische Informationen zu SNA und praktische Hinweise zur Verwendung von CS Linux. Diese Veröffentlichungen sind sowohl für Anfänger als Einstieg in die SNA-Materie als auch für Fachleute zur umfassenden Vertiefung des Themas geeignet.

- *Systems Network Architecture: Technical Overview* (IBM Form GC30-3073)
- *Verwaltungshandbuch für IBM Communications Server for Data Center Deployment für Linux*
- 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"
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/.

© Copyright IBM Corp. 1998, 2021

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

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 Linux Version 7.1
- Systemnetzwerkarchitektur (SNA)
- Hostkonfiguration
- z/OS Communications Server
- Transmission Control Protocol/Internet Protocol (TCP/IP)
- X.25
- Advanced Program-to-Program Communication (APPC)
- Programmierung
- andere IBM Produkte für den Netzbetrieb

Zu den Handbüchern der CS-Linux-Bibliothek sind Kurzbeschreibungen vorhanden. Für andere Bücher sind hier nur die Titel und Bestellnummern angegeben.

Veröffentlichungen zu CS Linux 7.1

Die Bibliothek zu CS Linux 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 Linux* . Für die Installation dieser Softcopyhandbücher benötigen Sie (in Abhängigkeit von den installierten Landessprachen) 9-15 MB Festplattenspeicherplatz.

- *Einstieg in IBM Communications Server for Data Center Deployment für Linux* (GC12-3362 und GC12-3364)

  Dieses Handbuch enthält eine allgemeine Einführung in CS Linux und Informationen zu unterstützten Netzkenndaten sowie zu Installation, Konfiguration und Betrieb. Es gibt zwei Versionen dieses Handbuchs:

  – GC12-3362 gilt für CS Linux auf den Plattformen i686, x86_64 und ppc64

  – GC12-3364 gilt für CS Linux auf System z.

- *Verwaltungshandbuch für IBM Communications Server for Data Center Deployment für Linux* (SC12-3363)

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

- *IBM Communications Server for Data Center Deployment on Linux Administration Command Reference* (SC31-6770)

  Dieses Handbuch enthält Informationen zu SNA- und CS-Linux-Befehlen.

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

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

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

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

© Copyright IBM Corp. 1998, 2021

- *IBM Communications Server for Data Center Deployment on AIX or Linux LUA Programmer's Guide* (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* (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* (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 Linux NOF Programmer's Guide* (SC31-6778)

  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 Linux Diagnostics Guide* (SC31-6779)

  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* (SC23-8595)

  Dieses Handbuch enthält Informationen zu APPC-Anwendungen, die zusammen mit CS Linux eingesetzt werden können.
- *IBM Communications Server for Data Center Deployment on Linux Glossary* (GC31-6780)

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

Veröffentlichungen zur Systemnetzwerkarchitektur (SNA)

Die folgenden Handbücher enthalten Informationen zu SNA-Netzen:

- *Systems Network Architecture: Format and Protocol Reference Manual - Architecture Logic for LU Type 6.2* (IBM Form SC30-3269)
- *Systems Network Architecture: Formats* (IBM Form GA27-3136)
- *Systems Network Architecture: Guide to SNA Publications* (IBM Form GC30-3438)
- *Systems Network Architecture: Network Product Formats* (IBM Form LY43-0081)
- *Systems Network Architecture: Technical Overview* (IBM Form GC30-3073)
- *Systems Network Architecture: APPN Architecture Reference* (IBM Form SC30-3422)
- *Systems Network Architecture: Sessions between Logical Units* (IBM Form GC20-1868)
- *Systems Network Architecture: LU 6.2 Reference - Peer Protocols* (IBM Form SC31-6808)
- *Systems Network Architecture: Transaction Programmer's Reference Manual for LU Type 6.2* (IBM Form GC30-3084)
- *Systems Network Architecture: 3270 Datastream Programmer's Reference* (IBM Form GA23-0059)
- *Networking Blueprint Executive Overview* (IBM Form GC31-7057)
- *Systems Network Architecture: Management Services Reference* (IBM Form SC30-3346)

Veröffentlichungen zur Hostkonfiguration

Die folgenden Handbücher enthalten Informationen zur Hostkonfiguration:

- *ES-9000, ES-3090 IOCP User's Guide Volume A04* (IBM Form GC38-0097)

- *3174 Establishment Controller Installation Guide* (IBM Form GG24-3061)
- *3270 Information Display System 3174 Establishment Controller: Planning Guide* (IBM Form GA27-3918)
- *OS/390 Hardware Configuration Definition (HCD) User's Guide* (IBM Form SC28-1848)

Veröffentlichungen zu z/OS Communications Server

Die folgenden Handbücher enthalten Informationen zu z/OS Communications Server:

- *z/OS V1R7 Communications Server: SNA Network Implementation Guide* (IBM Form SC31-8777)
- *z/OS V1R7 Communications Server: SNA Diagnostics* (Band 1: IBM Form GC31-6850, Band 2: IBM Form GC31-6851)
- *z/OS V1R6 Communications Server: Resource Definition Reference* (IBM Form SC31-8778)

Veröffentlichungen zu TCP/IP

Die folgenden Handbücher enthalten Informationen zum Netzprotokoll TCP/IP (Transmission Control Protocol/Internet Protocol):

- *z/OS V1R7 Communications Server: IP Configuration Guide* (IBM Form SC31-8775)
- *z/OS V1R7 Communications Server: IP Configuration Reference* (IBM Form SC31-8776)
- *z/VM V5R1 TCP/IP Planning and Customization* (IBM Form SC24-6125)

Veröffentlichungen zu X.25

Die folgenden Handbücher enthalten Informationen zum Netzprotokoll X.25:

- *Communications Server for OS/2 Version 4 X.25 Programming* (IBM Form SC31-8150)

Veröffentlichungen zu APPC

Die folgenden Handbücher enthalten Informationen zu APPC (Advanced Program-to-Program Communication):

- *APPC Application Suite V1 User's Guide* (IBM Form SC31-6532)
- *APPC Application Suite V1 Administration* (IBM Form SC31-6533)
- *APPC Application Suite V1 Programming* (IBM Form SC31-6534)
- *APPC Application Suite V1 Online Product Library* (IBM Form SK2T-2680)
- *APPC Application Suite Licensed Program Specifications* (IBM Form GC31-6535)
- *z/OS V1R2.0 Communications Server: APPC Application Suite User's Guide* (IBM Form SC31-8809)

Veröffentlichungen zur Programmierung

Die folgenden Handbücher enthalten Informationen zur Programmierung:

- *Common Programming Interface Communications CPI-C Reference* (IBM Form SC26-4399)
- *Communications Server for OS/2 Version 4 Application Programming Guide* (IBM Form SC31-8152)

Veröffentlichungen zu anderen IBM Produkten für den Netzbetrieb

Die folgenden Handbücher enthalten Informationen zu anderen Themen mit Bezug auf CS Linux:

- *SDLC Concepts* (IBM Form GA27-3093)
- *Local Area Network Concepts and Products: LAN Architecture* (IBM Form SG24-4753)
- *Local Area Network Concepts and Products: LAN Adapters, Hubs and ATM* (IBM Form SG24-4754)

- *Local Area Network Concepts and Products: Routers and Gateways* (IBM Form SG24-4755)
- *Local Area Network Concepts and Products: LAN Operating Systems and Management* (IBM Form SG24-4756)
- *IBM Network Control Program Resource Definition Guide* (IBM Form SC30-3349)

Index

Numerische Stichwörter

3270-LU
    definieren 91
    für TN Server 10, 91

A

Abfragebefehle 14
Abhängige LU 6.2 83
Advanced Program-to-Program Communication (APPC) 6
Aktivieren der Software CS Linux 95
Aktivieren einer Ressource 70
Aktivieren von Ports und Verbindungsstationen 96
Alerts 14
Aliasnamen für Partner-LU definieren 82
Ändern der Konfiguration 70
Anforderungen
    Personal und Qualifikation 18
Angepasste Nachrichtendosierung auf Sitzungsebene 13
Anwendungsprogrammierschnittstelle (API) 4
Anzeigen der Konfiguration 70
API
    Arten für CS Linux 5
    für CS-Linux-Verwaltung 13
    Unterstützung 4
APPC
    abhängige LU 6.2 83
    Application Suite 6, 8
    Konfiguration 78
    online 97
    unabhängige LU 6.2 81
    Unterstützung für verteilte Anwendungen 6
APPC Application Suite 8
APPN
    Anwendungen 6, 8
    DLUR-Unterstützung 3
    dynamische Konfiguration 12
    Endknoten 3
    Hostunterstützung für APPN 3
    Knotentypen 2
    Konfiguration 79, 80
    Netzknoten 2
    Routing 13
    Segmentierung von Netzen 23
    unabhängige LU-Unterstützung 4
    Unterbereichsfunktionen 3
    Verbindungsnetz 13
Arbeitsblätter für Planung 66

DLUR *(Forts.)*
Konfiguration 88
PU konfigurieren 90
Unterstützung für untergeordnete Knoten 90
DLUS 88
Dokumentation, online 97
Domäne 5
Domäne (Parameter) 56
dpkg 19
Dynamische Konfiguration 12
Dynamisches Definieren abhängiger LUs (DDDLU) 3

E

Eingangspunkt 13
Empfohlene Literatur 98
Enterprise Extender
Dialog für Ports 76
Überblick 9
Verbindungskonfiguration 76
Ethernet
SAP-Dialoganzeige 75
Verbindungskonfiguration 75

F

feedback
email template 99
sending reader comments 99
Fehler
Daten 14
Diagnosetools 14
Fehlerbehebungstools 14
Fenster 68
Ferner Knoten
Konfiguration 81, 82
Partner-LU konfigurieren 82
Festplattenspeicher 21
Firewall 22
Foren, online 97
Funktionen 4
Funktionsanforderungen 17

G

Gateway
Definition 6
SNA Gateway 6
GSKit
Remote API Client für AIX 49, 51
Remote API Client für Linux 38, 40
Remote API Client für Linux auf System z 43, 46
Remote API Client für Windows 60

H

Hardware
Verbindung 20
Hardwarevoraussetzungen
Remote API Client für AIX 49
Remote API Client für Linux 37
Remote API Client für Linux auf System z 43
Remote API Client für Windows 53
Hardwarevoraussetzungen *(Forts.)*
Server 19
Hilfe
Motif-Verwaltungsprogramm 12
Webverwaltungsprogramm 12
Hinzufügen einer Ressource 70
Host
im APPN-Netz 3
im Unterbereichsnetz 2
LU-Unterstützung 3
HPR
im Vergleich zu ISR 13
HPR/IP 9
HTTPS
konfigurieren 31
Remote API Client für AIX 51
Remote API Client für Linux 40
Remote API Client für Linux auf System z 46
Remote API Client für Windows 60
Voraussetzungen 20

I

Implizite untergeordnete LU konfigurieren 87
Inaktivieren einer Ressource 70
Informationsquellen 97
Initialisieren des SNA-Knotens 95
Installation
Einzelangaben zu vorhandenen Paketen 26
Remote API Client für AIX 50, 51
Remote API Client für Linux 39
Remote API Client für Linux auf System z 44
Verwaltung nach der Installation 33
vorbereiten 26
Installation von Remote API Client für AIX 50, 51
Installation von Remote API Client für Linux 39
Installation von Remote API Client für Linux auf System z 44
Installationsabschluss, Prozeduren 33
Installationsvoraussetzungen 19
Installationsvorbereitungen 26
Intermediate Session Routing (ISR) 13
International Organization for Standards (ISO) 23
IP-Adressformate 21
IP-Port, Dialog 76
iptables 22
IPV4-Adresse 21
IPV6-Adresse 21
ISO (International Organization for Standards) 23
ISR (Intermediate Session Routing) 13

J

Java
Remote API Client für AIX 49
Remote API Client für Linux 38
Remote API Client für Linux auf System z 43

K

Knoten
fern 81, 82
initialisieren 95
Konfiguration 73

Knoten *(Forts.)*
lokal 89
übergeordnet 88
untergeordnet 90
Knoten für Low-Entry Networking (LEN-Knoten) 75
Knotenfenster 68
Komponentenverwaltung 68
Komprimierung von LU-Sitzungsdaten 4
Konfiguration
ändern 70
anzeigen 70
APPC-Kommunikation 78
Beispiele 88
CPI-C-Nebeninformationen 84
Dateien 34, 35
DLUR 88
ferner Knoten 82
implizite untergeordnete LU 87
Knoten 73
Konnektivität 73
LU 6.2 81, 83
LU-Typen 0-3 77
Partner-LUs für einen LEN-Knoten 81
Planung 66
Port 74
sichern 34
Standardeinstellungen für TN Redirector 94
TN-Server-Standardeinstellungen 93
TN-Server-Zuordnungseinträge 93
untergeordnete LUs für SNA Gateway 86
Konfigurationsfenster für Remote API Client für Windows
erweiterte Parameter 57
Parameter 55
Konfigurationsserver
entfernen 72
hinzufügen 72
Konnektivität
Konfiguration 73
Optionen 3

L

LAN (Local Area Network) 3
LEN-Knoten
Beschreibung 3
fernen Knoten identifizieren 75
Partner-LU konfigurieren 81
Lizenzierungsmechanismen 25
Lizenzprogramm
Remote API Client für AIX 50
Remote API Client für Linux 39
Remote API Client für Linux auf System z 44
Logische Einheit (LU) 3, 87
Lokale LU definieren 81
Lokales Netz (LAN) 3
Löschen einer Ressource 70
LU
Konfiguration 81, 83, 91
Namenskonventionen 23
Partner-LU definieren 81
Pool 85, 91, 92
untergeordnet 86, 87
Unterstützung 3
LU-Pool
LU-Pool *(Forts.)*
anzeigen 78
definieren 78
Konfiguration 78
LU-Typen 0-3 77

M

MAC (Medium Access Control) 75
Maximale Broadcast-Versuche (Parameter) 57
MDS-NMVT (Multiple Domain Support - Network Management Vector Transport) 13
Medium Access Control (MAC) 75
Mehrere Server in einer Domäne 5
Migrieren früherer Versionen von CS Linux 27
Motif-Verwaltungsprogramm
Beschreibung 12
Hilfe 12
Verwaltungsfähigkeit 14
verwenden 65
Multiple Domain Support - Network Management Vector Transport (MDS-NMVT) 13

N

Nachrichtendosierung auf Sitzungsebene 13
Namenskonventionen 23
Netz
Alerts 14
Namenskonventionen 23
Peer-zu-Peer 2
Planung 17, 18, 23
über das Netz verfügbare Informationen 97
Unterbereichsnetz 2
Unterstützung 2
Verwaltung 13
NOF (API) 13

O

Online
APPC 97
Diskussionsgruppen 97
Dokumentation 97
Foren 97
Hilfe 12
Onlinedokumentation zu CS Linux 31
Open Systems Interconnection (OSI) 23
Optionen für Datenübertragungssteuerung 3
OSI (Open Systems Interconnection) 23

P

Partner-LU
Aliasname 82
auf fernem Knoten 82
Konfiguration 81
mit Platzhaltern definieren 83
Partneranwendungen 6
PDF, Handbücher anzeigen 33
Peer
Netz 2
Peer-Server 5

Personalanforderungen 18
Pfad für ausführbare CS-Linux-Programme 67
Physische Einheit (PU) 6
Planungsblätter 66
Platzhalter 83
Port
  aktivieren 96
Port-Konfiguration 74–76
Primary RUI 4
Prozeduren
  Remote API Client für Windows installieren 54, 57
PU (physische Einheit) 6
PU-Konzentration 86
PU-Konzentrator 6

Q

Qualifikationsanforderungen 18

R

reader comments
  methods of sending feedback 99
Releaseinformationen 33
Remote API Client
  AIX-Hardwarevoraussetzungen 49
  Hardwarevoraussetzungen für Linux auf System z 43
  Linux-Hardwarevoraussetzungen 37
  Softwarevoraussetzungen für AIX 49
  Softwarevoraussetzungen für Linux 37
  Softwarevoraussetzungen für Linux auf System z 43
Remote API Client für Linux
  Einzelangaben zu vorhandenen Paketen 38
Remote API Client für Linux auf System z
  Einzelangaben zu vorhandenen Paketen 43
Remote API Client für Windows
  installieren 53
  mit dem Setup-Programm installieren 54
  von der Befehlszeile aus installieren 57
Ressource
  aktivieren 70
  Anforderungen 18
  definieren 70
  Einträge 71
  inaktivieren 70
  Informationen 97
  löschen 70
  Verwaltung 68
rpm 19

S

SAA (Systemanwendungsarchitektur) 4
Sammelpunkt 13
SAP (Service Access Point) 19, 75
Schaltflächen in Ressourcenfenstern 71
Schnittstellenauswahl 12
SDK-Software
  Remote API Client für Windows 53
SDLC
  für abhängigen Datenverkehr 74
  Konfiguration 74
SE Linux 20
Secure Sockets Layer (SSL)
  Clientauthentifizierung 93, 94
  Datenverschlüsselung 33, 93, 94
  Serverauthentifizierung 33, 93, 94
Security Enhanced Linux 20
Server
  entfernen 72
  hinzufügen 72
  Linux-Hardwarevoraussetzungen 19
Server, Telnet 9
Servername 56
Service Access Point (SAP) 75
Servicezugriffspunkt 19
Sicherheitsoptionen 13
Sichern
  Konfigurationsdateien 34
Sicherung
  zurückschreiben 34
Sitzung
  Nachrichtendosierung 13
  Routing 13
  U-förmig 4
  Unterstützung 4
SNA
  Bibliothek 97
SNA Gateway
  Konfiguration 86
  Überblick 6
snaadmin (Programm) 12
snastart (Datei) 68
Softwarefeatures 6
Softwarevoraussetzungen
  Remote API Client für AIX 49
  Remote API Client für Linux 37
  Remote API Client für Linux auf System z 43
  Remote API Client für Windows 53
Speicherbedarf 21
Sprachumgebungsvariable
  Remote API Client für Linux 38
  Remote API Client für Linux auf System z 44
start (Befehl) 67
Start von CS Linux beim Warmstart 96
Starten von CS Linux, automatisch 95
Statusbefehle 14
Steuerung für synchrone Datenübertragung (SDLC) 74
stop (Befehl) 95
Symbolleistenschaltflächen 71
Systemanwendungsarchitektur (SAA) 4

T

technical problems
  methods of resolving 99
TN Redirector
  Konfiguration 94
  Standardeinstellungen konfigurieren 94
  Überblick 11
  Zugriffseintrag konfigurieren 94
TN Server
  Benutzer 91
  Konfiguration 90
  Standardeinstellungen konfigurieren 93
  Überblick 9
  Unterstützung für mehrere Sitzungen 91

TN Server *(Forts.)*
Zugriffseintrag konfigurieren 93
Zuordnungseinträge konfigurieren 93
TN3270
Programme 9
Server 9
TN3270-Benutzer 10, 91
TN3270-Programme 90
TP (transaction program) 4
Transaktionsprogramm 4
Transparenz zwischen lokalem und fernem Sitzungspartner 4

U

U-förmige Sitzungen 4
Übergeordneter Knoten 88
Übertragungsmedien 19
Unabhängige LU 6.2 konfigurieren 81
Untergeordnete LU
für SNA Gateway 86
Hardwarebeispiele 86
Konfiguration 87
Untergeordneter Computer 86
Unterroutinen 4
Utergeordneter Knoten 88

V

Verben 4
Verbindungshardware 20
Verbindungsnetz 13
Verbindungsnetz, Konfiguration 75
Verbindungsstation
aktivieren 96
für Port definieren 74
Version der IP-Adresse 21
Verteilte Verarbeitung
Anwendungsunterstützung 6
Umgebung 2
Verwaltungsprogramm
API NOF 13
Befehlszeile 12
Motif 12, 14
Web 12
Verzeichnis für ausführbare CS-Linux-Programme 67
Voraussetzungen
Betriebssystem 19
Hauptspeicher und Speicher 21
HTTPS 20
Installation 19
Software 19, 20
WebSphere Application Server 20
Vorversionen von CS Linux migrieren 28

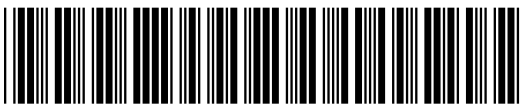
W

WAN (Wide Area Network) 3
WebSphere Application Server
konfigurieren 31
Voraussetzungen 20
Webverwaltungsprogramm
Beschreibung 12
Webverwaltungsprogramm *(Forts.)*
Hilfe 12
Weitverkehrsnetz (WAN) 3

X

xsnaadmin (Programm) 12, 65

Z

Zeitlimit für LAN-Zugriff (Parameter) 57
Zeitlimit für Verbindungswiederherstellung (Parameter) 57
Zweignetzknoten 7

GC12-3369-05