

IBM Communications Server para Linux



Iniciação Rápida

Versão 6.2.3

IBM Communications Server para Linux



Iniciação Rápida

Versão 6.2.3

Nota:

Antes de usar estas informações e o produto a que elas se referem, leia as informações gerais em "Avisos", na página 109.

Terceira Edição (Dezembro de 2007)

Esta edição se aplica ao IBM IBM Communications Server para Linux, Versão 6.2.3, e a todos os releases e modificações subseqüentes, até que seja indicado de outra forma em novas edições ou newsletters técnicos.

Solicite as publicações a um representante IBM ou filial IBM que atenda sua localidade. As publicações não são armazenadas no endereço fornecido a seguir.

A IBM agradece seus comentários. Você poderá enviar seus comentários ao seguinte endereço:

IBM Brasil - Centro de Traduções
Rodovia SP 101 km 09
CEP 13185-900
Hortolândia, SP

Você pode enviar seus comentários eletronicamente utilizando um dos seguintes métodos:

- Fax (EUA e Canadá):

1-919-254-4028

Envie o fax para "A/C Communications Server for Linux Information Development."

- E-mail:

comsvrcf@us.ibm.com

Ao enviar informações para a IBM, você concede à IBM um direito não-exclusivo de utilizar ou distribuir essas informações da forma que ela achar apropriada, sem incorrer em qualquer obrigação para com você.

© Copyright International Business Machines Corporation 1998, 2007. Todos os direitos reservados.

Índice

Tabelas vii

Figuras ix

Bem-vindo ao IBM Communications

Server para Linux xi

Como Utilizar este Manual xi

Roteiro xi

Convenções Tipográficas xii

Abreviaturas Utilizadas neste Manual xii

O Que Há de Novo xiii

Novas Funções xiv

Funções Retiradas xiv

Capítulo 1. Sobre o IBM

Communications Server para Linux 1

IBM Communications Server para Linux - Recursos e Embalagem 1

IBM Communications Server para Linux 1

Recursos de Rede Avançados 6

Recursos e Benefícios 11

Blocos de Construção Versátil 11

Operação de Cliente/Servidor 12

Configuração Fácil 12

Opções Adicionais da Interface com o Usuário

para Administração 13

Melhor Desempenho 13

Opções de Segurança 13

Flexibilidade de Gerenciamento de Rede 14

Confiabilidade, Disponibilidade e Serviços 14

Integração, Crescimento e Alteração de Redes 15

Capítulo 2. Planejando a Rede e o IBM

Communications Server para Linux 17

Estágios do Planejamento da Rede 17

Identificando os Requisitos Funcionais da Rede 17

Determinando Como Configurar o

Communications Server para Linux 18

Identificando os Requisitos de Recursos para

Instalação e Operação 18

Endereçamento IPv4 e IPv6 23

Assegurando Compatibilidade entre Configurações

de Plataforma Cruzada 25

Convenções de Nomenclatura 25

Capítulo 3. Instalando o

Communications Server para Linux em

Servidores Linux 27

Como o Programa Licenciado Communications

Server para Linux Está Embalado 27

Preparando a Instalação do Communications Server

para Linux 28

Desativando Recursos Power Management 28

Instalando o Software de Pré-requisito 28

Exibindo os Detalhes da Instalação do Produto 28

Alterando a Variável Language Environment 29

Migrando de Níveis Anteriores do Communications

Server para Linux 29

Considerações 29

Processo de Migração 30

Instalando o Programa Licenciado Communications

Server para Linux 32

Instalando o Communications Server para Linux 33

Documentação On-line do Communications

Server para Linux 33

HACL (Host Access Class Libraries) 34

Configurando o WebSphere Application Server 34

Configurando o Certificado de Segurança do

WebSphere Application Server 34

Configurando o WebSphere Application Server 34

Instalando o Arquivo de Configuração do

Servidor 35

Procedimentos Pós-instalação 35

Operação de Cliente/Servidor 35

Visualizando Manuais em PDF 36

Revisando as Informações sobre o Release Atual 36

Configurando o SSL para Uso com o Servidor TN

ou Redirecionador TN 36

Fazendo Backup dos Arquivos de Configuração

do Communications Server para Linux 37

Restaurando uma Cópia de Backup de Arquivos

de Configuração do Communications Server para

Linux 38

Reinicializando os Arquivos de Configuração 38

Desinstalando o Communications Server para Linux 39

Capítulo 4. Instalando o IBM Remote

API Client no Linux 41

Requisitos de Hardware e Software 41

Requisitos de Hardware 41

Versão do Sistema Operacional Linux 42

Java 42

GSKIT 42

Exibindo os Detalhes da Instalação do Produto 42

Definindo a Variável Language Environment 43

Instalando o Remote API Client no Linux 43

Configurando Certificados de Segurança HTTPS

Utilizando GSKIT 44

Desinstalando o Remote API Client no Linux 45

Capítulo 5. Instalando IBM Remote API

Clients no Linux para System z 47

Requisitos de Hardware e Software 47

Requisitos de Hardware 47

Versão do Sistema Operacional Linux 47

Java 47

GSKIT 48

Exibindo os Detalhes da Instalação do Produto 48

Definindo a Variável Language Environment . . .	48
Instalando o Remote API Client no Linux para System z	48
Configurando Certificados de Segurança HTTPS Utilizando GSKIT	50
Desinstalando o Remote API Client no Linux para System z	51

Capítulo 6. Instalando IBM Remote API Clients em Sistemas AIX 53

Requisitos de Hardware e Software	53
Requisitos de Hardware	53
Versão do Sistema Operacional	53
Java	53
GSKIT	53
Alterando a Variável Language Environment	53
Instalando o Remote API Client no AIX	54
Instalando o Remote API Client Copiando Arquivos para a sua Estação de Trabalho AIX	54
Instalando o Remote API Client a partir do CD	55
Configurando Certificados de Segurança HTTPS Utilizando GSKIT	55
Desinstalando o Remote API Client no AIX.	56

Capítulo 7. Planejando e Instalando o Remote API Client no Windows 57

Requisitos de Hardware e Software	57
Acessando o Programa de Instalação	58
Instalando o Remote API Client no Windows Utilizando o Programa de Instalação	59
Opções Avançadas da Configuração do Remote API Client	62
Instalando o Software Remote API Client a partir da Linha de Comandos	63
Configurando Certificados de Segurança HTTPS Utilizando GSKIT	65
Personalizando o Software Remote API Client Depois da Instalação	66
Reinstalando o Software Remote API Client	66
Desinstalando o Software Remote API Client	67
Ajuda	67

Capítulo 8. Configurando e Utilizando o Communications Server para Linux . . . 69

Planejando a Configuração do Communications Server para Linux	70
Planilhas de Planejamento	70
Folhas de Tarefas	71
Utilizando o Programa de Administração Motif	71
Especificando o Caminho para os Programas do Communications Server para Linux	71
Ativando o Communications Server para Linux Gerenciando o Communications Server para Linux com o Programa de Administração Motif	72
Configurando Funções de Cliente/Servidor.	77
Configurando o Nó.	78
Configurando a Conectividade	79
Configurando um Link SDLC para Tráfego Dependente	80

Configurando um Link Ethernet para Suportar Tráfego Dependente e Independente	81
Configurando um Link do Enterprise Extender	82
Configurando LUs Tipo 0-3	83
Definindo LUs Tipo 0-3	83
Definindo um Conjunto de LUs	84
Configurando a Comunicação APPC	85
Configurando uma Rede APPN Simples.	86
Configurando o APPC Dependente	90
Configurando o CPI Communications	90
Configurando a LUA	91
Definindo um Conjunto de LUs	92
Configurando o Gateway SNA	93
Suportando LUs Implícitas de Recebimento de Dados	94
Definindo LUs de Recebimento de Dados	95
Configurando o DLUR	95
Configurando o Suporte DLUR no Nó Local	96
Configurando o Suporte DLUR de Passagem para Nós de Recebimento de Dados	97
Configurando o Servidor TN	98
Definindo LUs 3270	100
Definindo um Conjunto de LUs	100
Configurando o TN3270 Server	101
Configurando o Redirecionador TN	102
Configurando o Redirecionador TN	103
Desativando o Communications Server para Linux	103
Iniciando o Communications Server para Linux Automaticamente	104
Ativando o Communications Server para Linux	104
Inicializando o Nó SNA	105
Ativando Portas e Estações de Link	105
Iniciando o Communications Server para Linux na Reinicialização	105

Capítulo 9. Recursos de Informações do Communications Server para Linux e SNA 107

Biblioteca SNA	107
Informações Acessíveis pela Rede	107
Leitura Sugerida	108

Apêndice. Avisos. 109

Marcas Registradas	111
------------------------------	-----

Bibliografia 113

Publicações do Communications Server para Linux Versão 6.2.3	113
Publicações do SNA (Systems Network Architecture)	114
Publicações da Configuração do Host	114
Publicações do z/OS Communications Server	115
Publicações do TCP/IP	115
Publicações do X.25	115
Publicações do APPC.	115
Publicações de Programação	115
Outras Publicações de Rede da IBM	115

Índice Remissivo 117

**Comunicando Seus Comentários à
IBM. 121**

Tabelas

1. Roteiro Inicial.	xii	2. Convenções Tipográficas	xii
-----------------------------	-----	--------------------------------------	-----

Figuras

1. Gateway SNA Vinculando Vários Computadores Linux de Recebimento de Dados num Computador Host 7
2. Extensor de Ramificação 8
3. Servidor TN 10
4. Janela Nó 74
5. Barra de Ferramentas do Communications Server para Linux 76
6. Nó Communications Server para Linux que se Comunica Diretamente com um Host 78
7. Nó Communications Server para Linux numa Rede APPN 79
8. Gateway SNA. 93
9. Nó Communications Server para Linux Fornecendo DLUR 96
10. Nó Communications Server para Linux Configurado para Servidor TN 98
11. Servidor TN 99

Bem-vindo ao IBM Communications Server para Linux

Este manual apresenta o IBM Communications Server para Linux, um produto de software IBM destinado a permitir que um computador Linux troque informações com outros nós numa rede SNA (Systems Network Architecture).

Há duas variantes de instalação diferentes do IBM Communications Server para Linux, dependendo do hardware no qual opera:

Communications Server para Linux

Communications Server para Linux, produto de programa número 5724-i33, opera com as seguintes opções:

- Estações de trabalho Intel de 32 bits com a plataforma Linux (i686)
- Estações de trabalho AMD64/Intel EM64T de 64 bits com a plataforma Linux (x86_64)
- Computadores IBM pSeries com a plataforma Linux (ppc64)

Communications Server para Linux em System z

O Communications Server para Linux em System z, número de produto de programa 5724-i34, opera em mainframes System z que executam o Linux para System z (s390 ou s390x).

Há duas diferentes cópias do manual *Communications Server para Linux - Iniciação Rápida*, uma para cada uma dessas duas variantes de instalação. Certifique-se de que você tenha a cópia correta deste manual para a instalação do Communications Server para Linux. Este manual aplica-se ao Communications Server para Linux nas plataformas i686, x86_64 e ppc64.

O Communications Server para Linux fornece blocos de construção para uma ampla variedade de necessidades e soluções de redes. Eles podem ser utilizados para trocar informações com nós em redes SNA ou para fornecer acesso ao host para programas Telnet que estejam se comunicando em TCP/IP (Transmission Control Protocol/Internet Protocol).

Como Utilizar este Manual

Esta seção explica como as informações são organizadas e apresentadas neste manual.

Roteiro

Este manual destina-se às equipes de gerenciamento e técnica envolvidas no planejamento da rede, e a qualquer pessoa interessada no Communications Server para o sistema operacional Linux.

Para localizar as informações necessárias para iniciar com o Communications Server para Linux, utilize a Tabela 1 na página xii.

Como Utilizar este Manual

Tabela 1. Roteiro Inicial

Para...	Consulte...
Ler sobre o Communications Server para Linux	Capítulo 1, “Sobre o IBM Communications Server para Linux”, na página 1
Planejar como utilizar o Communications Server para Linux na sua rede	Capítulo 2, “Planejando a Rede e o IBM Communications Server para Linux”, na página 17
Instalar o Communications Server para Linux em servidores Linux	Capítulo 3, “Instalando o Communications Server para Linux em Servidores Linux”, na página 27
Instalar Remote API Clients no Linux (Intel de 32 bits, Intel/AMD de 64 bits ou pSeries)	Capítulo 4, “Instalando o IBM Remote API Client no Linux”, na página 41
Instalar Remote API Clients no Linux para System z	Capítulo 5, “Instalando IBM Remote API Clients no Linux para System z”, na página 47
Instalar Remote API Clients no AIX	Capítulo 6, “Instalando IBM Remote API Clients em Sistemas AIX”, na página 53
Instalar Remote API Clients no Windows	Capítulo 7, “Planejando e Instalando o Remote API Client no Windows”, na página 57
Configurar o Communications Server para Linux	Capítulo 8, “Configurando e Utilizando o Communications Server para Linux”, na página 69
Localizar informações sobre a documentação do Linux e outras publicações, inclusive informações on-line	Capítulo 9, “Recursos de Informações do Communications Server para Linux e SNA”, na página 107
Ler os avisos e as informações sobre marcas registradas	“Avisos”, na página 109

Convenções Tipográficas

Os estilos tipográficos usados neste documento são mostrados na Tabela 2.

Tabela 2. Convenções Tipográficas

Elemento Especial	Amostra de Tipografia
Palavras enfatizadas	faça backup dos arquivos antes da exclusão
Título do documento	<i>Communications Server for Linux Administration Guide</i>
Arquivo ou caminho	/usr/spool/uucp/meuarq.bkp
Programa ou aplicativo	snaadmin
Entrada do usuário	0p1
Saída do computador	CLOSE

Abreviaturas Utilizadas neste Manual

Este manual utiliza as seguintes abreviaturas:

AIX	Advanced Interactive Executive
-----	--------------------------------

API	Application Programming Interface
APPC	Advanced Program-to-Program Communication
APPN	Advanced Peer-to-Peer Networking
BrNN	Nó de Rede de Ramificação
COS	Class of Service
CPI-C	Common Programming Interface for Communications
CSV	Common Service Verb
DDDLU	Dynamic Definition of Dependent LUs
DES	Data Encryption Standard
DLC	Data Link Control
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
LAN	Rede Local
LDAP	Lightweight Directory Access Protocol
LEN	Low-Entry Networking
LLC2	Logical Link Control 2
LU	Unidade Lógica
LUA	Conventional LU Application Programming Interface
MDS-NMVT	Multiple Domain Support—Network Management Vector Transport
MPC	MultiPath Channel
MS	Management Services
NMVT	Network Management Vector Transport
NOF	Node Operator Facility
OSI	Open Systems Interconnection
PU	Unidade Física
RFC	Request For Comments
RLE	Run-Length Encoding
SAA	Systems Application Architecture
SAP	Service Access Point
SNA	Systems Network Architecture
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TN	Telnet
TP	Transaction Program
VT	Virtual Terminal
WAN	Wide Area Network

O Que Há de Novo

O Communications Server para Linux Versão 6.2.3 substitui o Communications Server para Linux Versão 6.2.2, o Communications Server para Linux Versão 6.2.1 e o Communications Server para Linux Versão 6.2.

Releases do produto ainda suportados:

- Communications Server para Linux Versão 6.2.2
- Communications Server para Linux Versão 6.2.1

Os seguintes releases do produto não são mais suportados:

- Communications Server para Linux Versão 6.2

O Que Há de Novo

- Communications Server para Linux Versão 6.0.1 (V6.0.1), que foi disponibilizado como PRPQ 5799–RQA ou 5799–RXL.

O Communications Server para Linux Versão 6.2.3 funciona com o IBM Remote API Client Versão 6.3.1 ou 6.3.0.

Novas Funções

As seguintes funções foram incluídas neste release do Communications Server para Linux:

- O endereçamento IPv6, além do IPv4, é agora suportado.
 - O Servidor TN e o Enterprise Extender (HPR/IP), que dependem de conectividade IP, podem se comunicar utilizando IPv4 ou IPv6.
 - Em uma implementação Cliente/Servidor, os Remote API Clients podem se comunicar com servidores utilizando o IPv4 ou o IPv6. (O IPv6 não suporta as difusões UDP; portanto, cada cliente deve ser configurado com, pelo menos, um nome de servidor.)
 - A API NOF, o programa de administração Motif e o programa de administração de linha de comandos aceitam endereços IPv6 hexadecimais de dois pontos ou endereços IPv4 decimais com pontos.
- O Communications Server para Linux normalmente inclui o Vetor de Controle de Informações TCP/IP (0x64) em um pedido NOTIFY para o host de uma sessão TN3270 ou para um aplicativo LUA em um Remote API Client. Esse vetor de controle fornece informações sobre o cliente que pode ser exibido no console de host ou utilizado pelo host (por exemplo, no faturamento), incluindo o endereço IP do cliente. Se o endereço do cliente for um endereço IPv6, mas o host estiver executando uma versão de nível inferior do VTAM que não possa interpretar endereços IPv6, o endereço do cliente poderá ser exibido incorretamente no console do host. Nesses casos, é possível desativar essa função, especificando o `NO_TCPIP_VECTOR` no parâmetro `ptf_flags` no comando `define_node`.
- O programa de administração da linha de comandos e a API NOF agora fornecem uma função para consultar Remote API Clients que estejam atualmente utilizando um determinado servidor. Um aplicativo NOF também pode registrar-se para receber as indicações quando os clientes se conectarem e desconectarem.
- O suporte é incluído para Reconhecimento do Alcance da Rede de Conexão, em conjunto com um suporte semelhante no computador host. Isso significa que se uma única rota em um SATF (Shared-Access Transport Facility) não estiver disponível (por exemplo, porque uma única rota de um roteador IP está desativada), as rotas alternativas serão utilizadas quando possível através desse recurso, antes de tentar novamente mais tarde a rota que falhou.
- A filtragem do log permite suprimir várias instâncias da mesma mensagem de log, de modo que cada mensagem de uma lista especificada seja registrada em log apenas uma vez. Isso reduz o volume das informações nos arquivos de log para que você possa se concentrar em mensagens de log novas ou importantes.

Funções Retiradas

Nenhuma função foi extraída nesse release.

Capítulo 1. Sobre o IBM Communications Server para Linux

Este capítulo explica o pacote do Communications Server para Linux e descreve suas funções, recursos e benefícios.

IBM Communications Server para Linux - Recursos e Embalagem

O Communications Server para Linux é um software de comunicação que executa no sistema operacional Linux. Ele consiste nos recursos descritos nas seções “IBM Communications Server para Linux” e “Recursos de Rede Avançados” na página 6.

IBM Communications Server para Linux

O IBM Communications Server para Linux se conecta aos aplicativos através das rede SNA e TCP/IP. Ele converte um computador Linux em um nó SNA, equipando-o com recursos e protocolos SNA. Isso permite que o computador Linux se comunique com outros computadores em uma rede SNA, incluindo os computadores host. Também fornece funções TCP/IP para permitir que o IBM Communications Server para Linux seja utilizado na rede TCP/IP ou no limite entre as redes TCP/IP e SNA.

O Communications Server para Linux fornece os seguintes serviços:

Suporte de Rede

O Communications Server para Linux suporta as redes ponto a ponto e da subárea:

Redes de Subárea SNA

Essas redes (também conhecidas como redes mediadas por host) são organizadas hierarquicamente, com um ou mais computadores host controlando a comunicação entre computadores, gerenciando a rede e fornecendo serviços de processamento e armazenamento de dados de alta capacidade. Todos os outros nós na rede são dependentes do controle de um host.

Computadores executando Linux podem participar de uma rede de subárea, sendo configurados como nós dependentes de host.

Redes Ponto a Ponto

Para ambientes de processamento distribuído, o Communications Server para Linux suporta redes APPN. Nessas redes ponto a ponto, os computadores executando Linux retêm as funções de processamento e se comunicam diretamente uns com os outros como pontos. As redes ponto a ponto utilizam plenamente a capacidade do computador Linux, e hoje concorrem com computadores host caros.

Uma rede APPN consiste em nós de ponto dos seguintes tipos:

- Nó de rede APPN (que fornece controle de tráfego, computação de rota dinâmica, serviços de seleção e serviços de gerenciamento de rede)
- O nó de extremidade APPN (que utiliza serviços de nó de rede APPN para se comunicar com nós de ponto)
- Nó LEN (que se comunica diretamente com nós adjacentes ou nós configurados para aparecerem como adjacentes)

IBM Communications Server para Linux - Recursos e Embalagem

Nota: Os computadores host podem funcionar como nós ponto a ponto em uma rede APPN, utilizando a LU 6.2 independente para se comunicarem com computadores Linux e outros hosts na rede.

Fornecendo Funções de Subárea numa Rede APPN

A função do solicitador de LU dependente (DLUR) ativa o tráfego entre hosts e nós dependentes de host a ser conduzido em uma rede APPN.

Opções de Controle de Link de Dados

No nível de link, o Communications Server para Linux oferece opções de conectividade diferentes para ajudá-lo a atender às considerações sobre tamanho, velocidade, segurança e custo de sua rede. (Para obter uma lista detalhada dos tipos de link suportados, consulte a seção "Requisitos de Instalação" na página 19). Ele suporta links de dados para diferentes tipos de redes, como segue:

Redes Locais

Para conectividade em rede local, você pode instalar os links apropriados para se comunicar utilizando protocolos token ring, Ethernet padrão e Ethernet 802.3.

WANs (Wide Area Networks)

O Communications Server para Linux suporta a conectividade com SDLC e X.25 (QLLC). Isso depende do suporte ao adaptador de OEM em cada plataforma.

Conexão Local

O Communications Server para Linux suporta conectividade MPC (Multipath Channel) para conexão local (Communications Server para Linux em System z apenas).

Integração IP

Se a sua rede backbone corporativa basear-se em IP, você poderá utilizar o recurso Enterprise Extender (HPR/IP) do Communications Server para Linux para integrá-la ao SNA, permitindo que os aplicativos SNA se comuniquem por meio da rede IP.

Suporte LU

As LUs (Unidades Lógicas) são recursos de rede específicos do aplicativo que residem em cada nó em uma rede SNA. Cada LU atua como uma interface que os aplicativos utilizam para acessar links, a fim de se comunicar através da rede com aplicativos do parceiro em outros nós.

O Communications Server para Linux suporta tipos diferentes de LUs para classes diferentes de aplicativos.

- Numa rede de subárea, o Communications Server para Linux suporta LUs dependentes, que podem ser de qualquer um dos seguintes tipos:
 - LU 0
 - LU 1
 - LU 2
 - LU 3
 - LU 6.2

A LU 0 suporta comunicação programa-a-programa primitiva, tipicamente utilizada em transações de pontos de venda, em vendas a varejo ou bancos. A LU 2 suporta aplicativos de emulação de terminal;

esses permitem que o computador Linux emule um terminal IBM da família 3270. Os outros tipos de LU ativam os aplicativos a participarem de processamentos distribuídos ou a se comunicarem com diversas impressoras ou terminais de vídeo interativos.

O Communications Server para Linux suporta sistemas host que utilizam DDDLU (Dynamic Definition of Dependent LUs (DDDLU)), um recurso do host que ativa LUs dependentes no sistema SNA a serem adicionadas à configuração do host quando o link de comunicação partindo do sistema SNA para o host está estabelecido. Com DDDLU, as LUs não precisam ser configuradas estaticamente no host. (Ainda é necessário definir as LUs dependentes do nó Communications Server para Linux.) Isso reduz a configuração inicial requerida no host e facilita a expansão posterior.

O Communications Server para Linux pode se comunicar com hosts compatíveis ou não com DDDLU, sem nenhuma diferença na configuração necessária. Quando o link de comunicação do nó Communications Server para Linux para o host é estabelecido, um host compatível com DDDLU informa ao nó que possui suporte para DDDLU; o nó envia, então, as informações necessárias para definir as LUs dependentes que utilizam o link. Se o host não for compatível com DDDLU, o Communications Server para Linux não enviará tais informações; ele parte da premissa de que as LUs já foram definidas estaticamente no host.

- A LU 6.2 independentes suporta tráfegos independentes em redes APPN. A LU 6.2 independente suporta comunicação autônoma e gerenciamento de rede, bem como processamento distribuído. Além disso, a função DLUR do Communications Server para Linux permite que o tráfego de LUs dependentes seja transmitido por uma rede APPN.
- O suporte à RUI Primária fornece a capacidade para um aplicativo Communications Server para Linux para gerenciar LAN/WAN de recebimento de dados conectado a dispositivos LU dependentes, mesmo em um mainframe. Essa função tem algumas restrições de conectividade, mas permite que aplicativos transmitam dados entre dispositivos LU dependentes sem a necessidade de um aplicativo de mainframe completo.

Suporte de Sessão

Uma sessão é um canal lógico temporário entre LUs associadas. Geralmente, os aplicativos parceiros associados a cada LU se comunicam através da sessão. O Communications Server para Linux pode suportar milhares de sessões. O Communications Server para Linux também pode suportar sessões em forma de U (também conhecidas como “transparência local/remota”), nas quais as LUs primárias e secundárias residem no mesmo computador Linux. Isso permite que você desenvolva e teste um par de programas de transação de origem e destino em um computador sem requerer uma conexão de link.

Os dados que fluem em uma sessão entre duas LUs associadas podem ser compactados, para reduzir a largura de banda necessária.

- Para a LU tipo 6.2, o Communications Server for Linux permite especificar a utilização de compactação na configuração no modo utilizado pela sessão. Você pode especificar diferentes algoritmos de compactação para serem utilizados, cada um dos quais fornece um nível diferente de compactação (RLE, LZ9 ou LZ10). Você também pode

especificar diferentes níveis de compactação para os dados que fluem em direções diferentes na sessão, ou pode especificar a compactação em uma direção, mas não na outra.

- Para LUs tipos 0–3, o Communications Server para Linux permite especificar a utilização de compactação na configuração da estação de link ou da PU utilizada pela sessão. A compactação RLE é utilizada para a direção de entrada e a LZ9 para a direção de saída.

Suporte API

O Communications Server para Linux inclui APIs (Application Programming Interfaces) para desenvolver aplicativos para determinados tipos de LUs, para processamento distribuído, para gerenciamento de rede e para administração do próprio Communications Server para Linux. O Communications Server para Linux fornece um intervalo de APIs compatíveis com as fornecidas pelos membros da família do Communications Server em execução em outros sistemas operacionais.

Uma API é uma interface que ativa um TP (Programa de Transação) a se comunicar com suas LUs de suporte. Ela consiste em uma biblioteca de verbos (também chamados funções, chamadas e sub-rotinas). a partir dos quais o TP seleciona aqueles que necessita para passar para sua LU pedir uma ação, como ENVIAR_DADOS. A LU, por sua vez, processa os verbos e cria um fluxo de dados de acordo com o protocolo apropriado, anexa um cabeçalho indicando o endereço de destino e envia os dados através do link para as LUs associadas.

Common Programming Interface for Communications (CPI-C) é um dos mais poderosos recursos das APIs devido a sua portabilidade. Introduzida para suportar LU 6.2 dependente e independente, a CPI-C é compatível com mandatos SAA (Systems Application Architecture) para unificar plataformas e sistemas operacionais diferentes. A CPI-C utiliza um conjunto de regras de sintaxe que é comum a todos os sistemas. Ela tem, portanto, se tornado um padrão.

Como a API CPI-C padrão da linguagem C, o Communications Server para Linux também inclui uma API CPI-C para ser utilizada por aplicativos Java. Para obter informações adicionais, consulte o *Communications Server for Linux CPI-C Programmer's Guide*. Nos manuais do Communications Server para Linux, todas as referências à CPI-C englobam Java CPI-C, a menos que indicado de outra forma.

Outras APIs do Communications Server para Linux incluem:

- A API APPC para comunicações ponto a ponto entre programas aplicativos utilizando a LU 6.2. A API possui a opção de ser não-bloqueadora. Quando um TP utiliza verbos não-bloqueadores, a API pode retornar o controle para o TP antes que ação requerida tenha sido concluída. Posteriormente, o TP é informado quando a ação estiver concluída.
- API LUA para comunicações com aplicativos de host.
- API CSV (Common Service Verb) para funções de utilitário como tradução de caractere e controle de rastreamento de aplicativo.

Além disso, o Communications Server para Linux inclui as seguintes interfaces de programação proprietárias:

- API MS (Management Services) para funções de mensagem de rede.
- API NOF (Node Operator Facility) para aplicativos que configuram e gerenciam recursos do Communications Server para Linux.

IBM Communications Server para Linux - Recursos e Embalagem

Para obter informações mais detalhadas sobre uma API, consulte o manual de programação da API.

Suporte a Cliente/Servidor

Computadores que executam o Communications Server para Linux podem ser configurados para se comunicarem por meio de protocolos cliente/servidor. Quando esses protocolos são utilizados em uma rede, todos os computadores que os utilizam para se comunicar nessa rede são referidos como “domínio.”

Computadores executando o Communications Server para Linux numa configuração cliente/servidor podem desempenhar as seguintes funções:

- Um servidor contém um nó SNA e seus componentes de conectividade associados. O servidor fornece conectividade SNA para aplicativos no sistema local ou em outros computadores no domínio do Communications Server para Linux. Os servidores devem ser sistemas Linux.
- Um Remote API Client não contém componentes do nó SNA, mas os acessa por meio de um servidor. Um cliente pode acessar um ou mais servidores ao mesmo tempo e pode executar aplicativos simultâneos conforme necessário. Os clientes podem estar executando em AIX, Linux ou Windows. (Um computador Linux pode ser servidor ou cliente, mas não ambos; não é possível instalar o servidor e cliente no mesmo computador.)

Servidores e clientes se comunicam através do domínio do Communications Server para Linux via TCP/IP. Como alternativa, podem se comunicar utilizando HTTPS por meio de um servidor WebSphere, que utiliza certificados de segurança para autenticar conexões cliente. Normalmente, utilizar HTTPS será atraente quando os clientes se conectarem por uma rede pública.

Em um domínio com vários servidores Communications Server para Linux, um servidor contém a cópia master do arquivo de configuração do domínio do Communications Server para Linux. Esse servidor é conhecido como o servidor master. Você pode definir outros servidores no domínio para serem servidores de backup ou deixá-los como servidores de ponto a ponto. O arquivo de configuração de domínio é copiado para servidores de backup—quando eles são iniciados ou quando a cópia master é alterada—de forma que todos os servidores de backup retenham uma cópia das últimas informações. Um servidor de ponto a ponto obtém informações de configuração de domínio do servidor master conforme necessário, mas não pode funcionar como um servidor de backup.

Se o servidor master falhar, o primeiro servidor de backup na lista de servidores definidos para o domínio passa a funcionar como o servidor master. O arquivo de configuração de domínio nesse servidor é utilizado como a cópia master e é copiado para outros servidores conforme necessário. Quando o servidor master é reiniciado, ele recebe uma cópia da configuração do domínio do servidor de backup que está funcionando como master no momento e, em seguida, passa a funcionar como o master.

Suporte para Aplicativos Distribuídos

Em um sistema Communications Server para Linux cliente/servidor, os aplicativos em execução nos Remote API Clients cooperam com os recursos de conectividade nos servidores para executarem uma única tarefa. Aplicativos em execução em outros computadores (sem o Communications

Server para Linux) também podem cooperar com aplicativos em computadores com o Communications Server para Linux para executarem processamento distribuído.

O Communications Server para Linux suporta aplicativos distribuídos por meio do APPC (também conhecido como LU 6.2).

Recursos de Rede Avançados

Incluído no produto base do Communications Server para Linux há um conjunto de recursos para agregar-lhe as capacidades avançadas de rede. Esses recursos incluem o seguinte:

- O gateway SNA conecta as LANs às redes SNA da subárea.
- O suporte à LU Primária fornece a base para o controle de dispositivos LU dependentes de recebimento de dados do mesmo que um aplicativo do mainframe host.
- Extensor de Ramificação simplifica grandes redes APPN separando os recursos em localizações diferentes (por exemplo, em ramificações separadas de uma grande organização). Isso reduz a quantidade de informações de topologia que devem ser armazenadas, enquanto que ainda permite uma eficiente localização dos recursos.
- APPC Application Suite fornece aplicações selecionadas para uso em redes APPN.
- O Enterprise Extender (EE, também conhecido como HPR/IP) permite que o tráfego SNA seja transportado nativamente através de redes IP.
- O Servidor TN fornece acesso em SNA para clientes TN3270 e TN3270E, referidos coletivamente como clientes TN3270.
- O Redirecionador TN fornece acesso através de host TCP/IP para clientes TN3270, TN3270E, TN5250 e VT, referido coletivamente como clientes Telnet.

Gateway SNA

Um gateway é um dispositivo transparente ao usuário que conecta redes diferentes ou sistemas de computadores, suportando os dois ambientes que conecta. Os usuários finais se comunicam uns com os outros como se estivessem em uma mesma rede.

O gateway SNA permite que um computador Linux desempenhe o papel de um gateway que vincula vários computadores de recebimento de dados em uma rede SNA com uma ou mais PUs (Physical Units) do host, conforme ilustrado na Figura 1 na página 7. Para simplificar a conectividade do host e para eliminar o excesso de links, o gateway SNA atua como um concentrador da PU — trata os vários computadores como uma única PU (que parece residir no nó do gateway SNA) e se comunica com o host através de uma única conexão física.

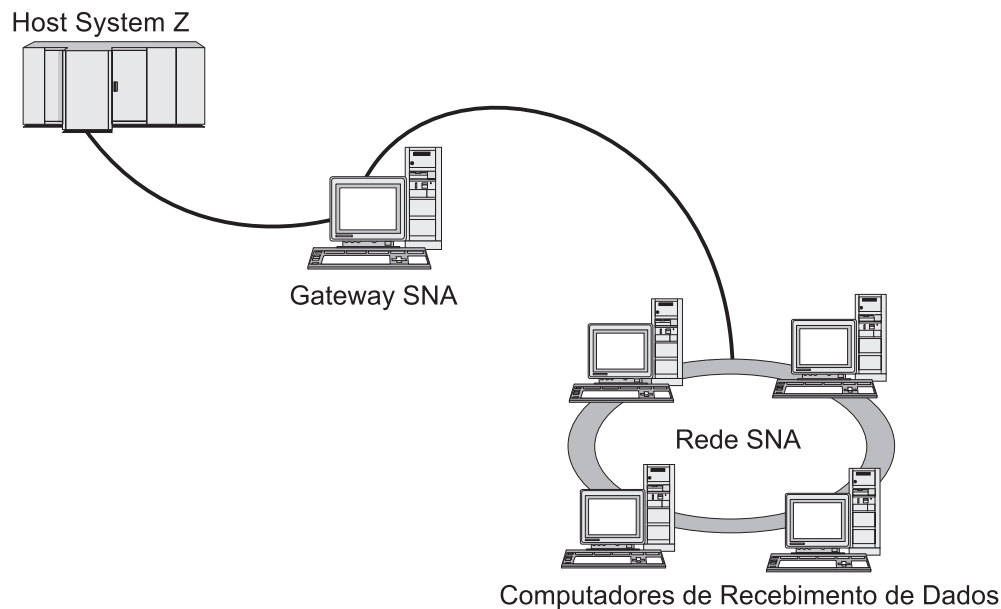


Figura 1. Gateway SNA Vinculando Vários Computadores Linux de Recebimento de Dados num Computador Host

Suporte à LU Primária

O suporte à LU Primária permite que um aplicativo do Linux controle dispositivos de LU dependentes de recebimento de dados como se fosse um aplicativo do mainframe host.

Aplicativos LUA normalmente se conectam aos mainframes host como LUs secundárias, de forma que o aplicativo host controle a definição das sessões e seja responsável pelo envio do BIND para iniciar uma sessão. O Communications Server para Linux também inclui a capacidade de atuar como uma LU primária para os dispositivos SNA dependentes de recebimento de dados por meio de uma LAN, utilizando a interface RUI Primária. Com essa interface, um aplicativo pode conectar sessões de LUs dependentes de recebimento de dados sem a necessidade de um mainframe host.

Para utilizar aplicativos da LU Primária, o nó deve ser configurado com LUs de recebimento de dados (ou um gabarito de PU de Recebimento de Dados) que utilizem o nome de LU host #PRIRUI#. Isso indica ao servidor que os aplicativos que utilizam a RUI Primária controlarão tais PUs e os recursos de LU atribuídos a elas. As PUs podem ser utilizadas em portas de LAN e de WAN. Consulte *Communications Server for Linux LUA Programmer's Guide* para obter informações sobre como programar aplicativos para utilizar a RUI Primária.

Extensor de Ramificação

Nós de rede em uma rede APPN precisam manter informações sobre topologia (sobre a localização de outros nós na rede e os links de comunicações entre eles), e direcionar essas informações pela rede quando a topologia mudar. Na medida em que a rede cresce em tamanho, a quantidade de informações armazenadas e o tráfego de rede relacionado à topologia torna-se maior e de difícil gerenciamento.

IBM Communications Server para Linux - Recursos e Embalagem

É possível evitar esses problemas separando a rede em sub-redes, de forma que cada nó precisa manter as informações sobre topologia dos nós em sua própria sub-rede. Contudo, isso resulta em maior tráfego de rede quando se tenta localizar recursos em outras sub-redes.

O recurso do Extensor de Ramificação do APPN, ilustrado na Figura 2, fornece uma solução para esses problemas.

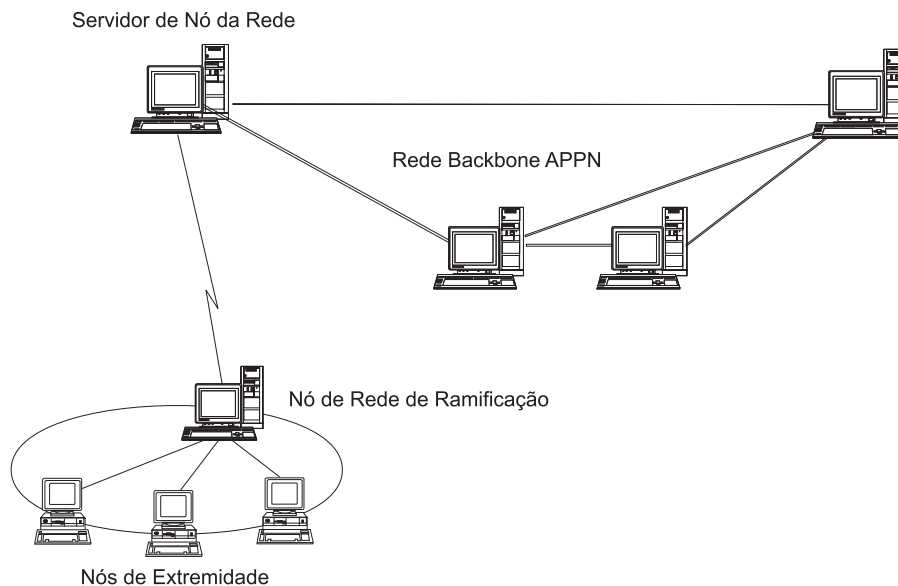


Figura 2. Extensor de Ramificação

Como o nome indica, o Extensor de Ramificação é projetado para redes que podem ser divididas em áreas distintas como ramificações separadas de uma grande organização. Ele trabalha separando as ramificações da rede APPN backbone (por exemplo, a rede nos comandos da empresa)

Cada ramificação contém um nó de um novo tipo chamado BrNN (Nó de Rede de Ramificação), é conectado a um Nó de Rede na rede backbone APPN principal. O BrNN combina as funções de um nó de rede APPN e um nó de extremidade APPN.

- Para a rede backbone, o BrNN aparece como um Nó de Extremidade, conectado a seu NNS (Servidor de Nó de Rede) na rede backbone:
 - Os nós na rede backbone não são cientes desses nós dentro da ramificação, reduzindo assim a quantidade de informações sobre topologia que devem ser armazenadas.
 - Como o BrNN aparece como um Nó de Extremidade, ele não recebe informações sobre topologia da rede backbone (as informações sobre topologia são transmitidas apenas entre Nós de Rede).
 - O BrNN registra todos os recursos na ramificação com seu NNS como se eles estivessem localizados no próprio BrNN. Isso significa que os nós na rede backbone podem localizar recursos na ramificação sem precisarem estar cientes dos nós separados na ramificação.
- Para uma rede de ramificação, o BrNN aparece como um Nó de Rede, atuando como o NNS de Nós de Extremidade na ramificação. Cada nó na ramificação pode ver o restante da rede como conectado através de seu NNS, da mesma forma como em um NNS padrão.

APPC Application Suite

O APPC Application Suite é um conjunto de aplicações que demonstram as capacidades de processamento distribuído de redes APPN, e pode ser útil para verificação da configuração e para determinação de problemas. Pode ser usado para fornecer suporte a operações como transferências de arquivos, que são freqüentemente executadas em uma rede.

O APPC Application Suite contém as seguintes aplicações:

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

Esses aplicativos podem ser acessados a partir de um servidor ou cliente Linux ou Windows.

Enterprise Extender

O Enterprise Extender (também conhecido como HPR/IP) fornece um mecanismo de integração de aplicativos SNA com uma rede IP.

As aplicações SNA são projetadas para utilizar protocolos SNA para se comunicarem em redes SNA com outras aplicações SNA. Quando instalado em uma rede TCP/IP utilizando o Enterprise Extender, as aplicações SNA ainda podem se comunicar; a função Enterprise Extender fornece um mecanismo para transporte de protocolos SNA através da rede IP. Em particular, fornece funcionalidade APPN HPR (High-Performance Routing), concedendo às aplicações os benefícios da duas conectividades, APPN e IP.

O Enterprise Extender no Communications Server para Linux está implementado simplesmente como um link de comunicação. Para conectar dois aplicativos SNA via IP, defina um link para o Enterprise Extender, do mesmo modo que para qualquer outro tipo de link, por exemplo, SDLC ou Ethernet.

Servidor TN

Programas de emulação 3270 que se comunicam em rede TCP/IP (no lugar de em rede SNA) são conhecidos como "programas TN3270" (programas de emulação Telnet 3270).

Os programas TN3270 também podem incluir suporte ao TN3270E (extensões padrão do Telnet 3270). TN3270E suporta emulação de dispositivo 3270 (incluindo terminais e impressoras) utilizando Telnet. Ativa um cliente Telnet a selecionar um dispositivo particular (especificando o nome da LU ou o nome de um conjunto de LU), e fornece suporte avançado para várias funções, incluindo as teclas ATTN e SYSREQ e tratamento de resposta SAN.

Nota: Este manual usa o termo TN3270 para informações que se aplicam aos protocolos TN3270, TN3287 e TN3270E.

O servidor TN do Communications Server para Linux fornece acesso a computadores host 3270 para usuários TN3270 em outros computadores. O servidor TN permite que usuários TN3270 compartilhem uma conexão de host com o Communications Server para Linux ou com outros usuários TN3270, em vez de

IBM Communications Server para Linux - Recursos e Embalagem

requerer um link direto. O Servidor TN também permite que usuários do TN3270 acessem hosts que não estejam executando o TCP/IP.

A função do servidor TN do Communications Server para Linux é ilustrado na Figura 3.

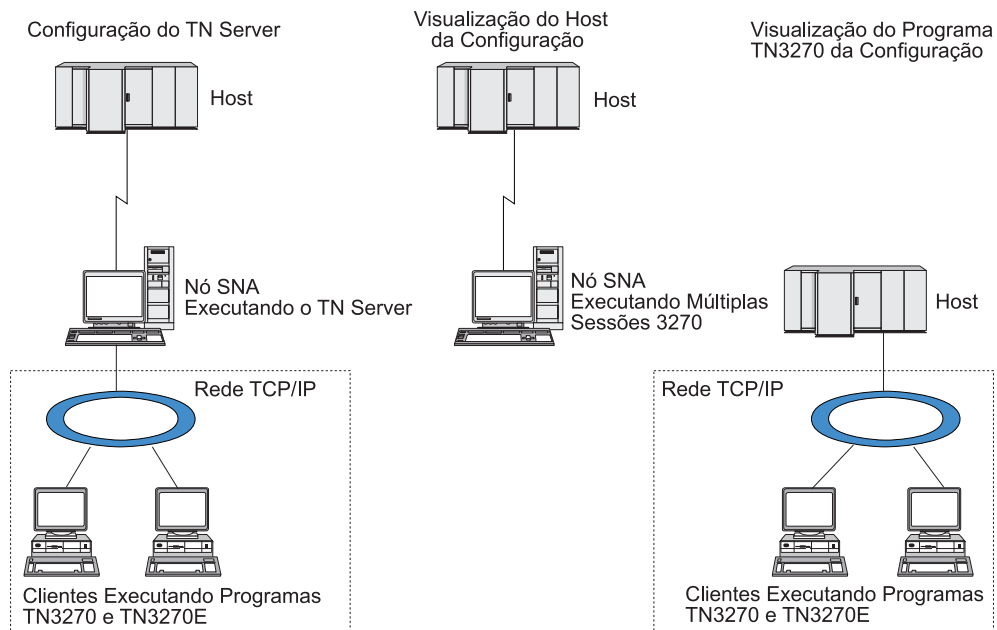


Figura 3. Servidor TN

O recurso do servidor TN do Communications Server para Linux fornece uma associação entre um usuário TN e a LU 3270 do Communications Server para Linux. Todos os dados do usuário de TN3270 são direcionados para a LU. Isso significa que a configuração do host e do usuário de TN3270 é feita como se eles fossem conectados diretamente; nenhum dos dois precisa saber que os dados estão sendo direcionados através do Servidor TN.

O servidor TN do Communications Server para Linux suporta todos os programas da emulação cliente TN3270 que implementam corretamente os protocolos definidos nos RFCs 1123, 1576, 1646, 1647 e 2355 do IETF.

Recursos de Segurança: O Servidor TN do Communications Server para Linux suporta a criptografia de dados, autenticação do servidor, autenticação do cliente e logon do Express, utilizando o software do SSL (Secure Sockets Layer):

- Criptografia de dados significa que os dados que fluem entre o Servidor TN e o emulador TN3270 estão em uma forma criptografada.
- A autenticação do servidor permite que um cliente TN3270 verifique se o Servidor TN ao qual está conectado é realmente o servidor que espera.
- A autenticação de cliente permite que um Servidor TN verifique se o cliente TN3270 ao qual está conectado é realmente o esperado. O Servidor TN também pode verificar uma lista de revogação em um servidor do diretório externo para assegurar que a autorização do cliente não tenha sido revogada.
- O Express Logon opera em conjunto com a autenticação de cliente, fazendo com que os clientes TN3270 não tenham necessidade de fornecer um ID de usuário e

uma senha ao se conectarem ao host. Em vez disso, o certificado de segurança do cliente é utilizado para recuperar as informações necessárias de ID do usuário e de senha.

Redirecionador TN

O recurso Redirecionador TN do Communications Server para Linux fornece serviços de passagem para sessões 3270, 5250 ou VT, via TCP/IP. O usuário da Telnet se comunica com o Communications Server para Linux por uma conexão TCP/IP; o Communications Server para Linux se comunica com o host por outra conexão TCP/IP.

O Redirecionador TN do Communications Server para Linux suporta criptografia de dados, autenticação do servidor e cliente, utilizando o software SSL (Secure Sockets Layer), da mesma forma que o Servidor TN para 3270. Isso permite que você utilize a verificação de segurança SSL (Secure Sockets Layer) quando necessário, não a conexão completa usuário para host. Por exemplo:

- Se os clientes estiverem se conectando ao Communications Server para Linux por uma LAN TCP/IP que não requer verificação, mas se conectarem a um host remoto que requeira SSL, você poderá utilizar o SSL por uma conexão TCP/IP entre o Communications Server para Linux e o host. Isso significa que a segurança é verificada apenas uma vez para cliente, e clientes individuais não precisam fornecer informações de segurança.
- Se o Communications Server para Linux estiver instalado no mesmo site que o host, mas os clientes estiverem se conectando a partir de sites externos, será possível utilizar SSL por meio das conexões do cliente para o Communications Server para Linux sem ser preciso instalar o software SSL no host.

Recursos e Benefícios

O Communications Server para Linux apresenta recursos e benefícios que variam desde simplificar a configuração até melhorar o diagnóstico de problemas para aprimorar o desempenho da rede.

Blocos de Construção Versátil

O Communications Server para Linux suporta a maioria dos ambientes e funções de nó. Em qualquer tipo de rede, subárea ou APPN, ele habilita o computador Linux para funcionar como qualquer um dos seguintes itens (ou uma combinação deles):

- Nó dependente de host
- Nó de ponto (veja uma descrição de nós de ponto APPN na discussão sobre redes ponto a ponto na seção “IBM Communications Server para Linux” na página 1)
- Parceiro (origem ou destino) em aplicativos distribuídos
- Nós de gateway que interconecta redes SNA

Com as APIs de gerenciamento de rede, o computador Linux também pode ser configurado para funcionar como um ponto de entrada dos Serviços de Gerenciamento (MS) para fornecer suporte ao gerenciamento de rede distribuída. No nível de link, o computador Linux pode ser conectado a várias LANs e WANs, utilizando qualquer um dos tipos de links suportados (descritos em “IBM Communications Server para Linux” na página 1 e “Requisitos de Instalação” na página 19).

Operação de Cliente/Servidor

A configuração de cliente/servidor oferece os seguintes benefícios:

- A concentração de recursos de SNA em servidores reduz a carga nos clientes, melhorando o desempenho do cliente e minimizando a memória necessária para fornecer serviços de SNA aos clientes.
- Um único link de dados pode ser compartilhado por vários usuários em máquinas diferentes, eliminando a necessidade de cada máquina ter uma conexão física de rede SNA.
- Múltiplos servidores podem fornecer conectividade redundante (por exemplo, múltiplos servidores proporcionando acesso ao mesmo host). Ter múltiplos caminhos para um recurso de SNA permite o equilíbrio de carga nos diferentes servidores e fornece backup imediato no caso de um servidor ou link específico falhar.
- Utilizando conjuntos de LUs em múltiplos servidores, o administrador pode configurar e incluir facilmente servidores e usuários.
- Ter menos links e PUs para conectividade do host reduz o tamanho da definição VTAM do host.
- Utilitários de administração podem ser utilizados para configurar e gerenciar recursos de nó (para qualquer computador no domínio) e recursos compartilhados. O suporte a cliente/servidor fornecido pelas ferramentas de administração do Communications Server para Linux permite a administração transparente de todos os recursos do domínio a partir de qualquer computador no domínio.
- Aplicativos SNA podem ser conectados via IPs (Internet Protocols) utilizando TCP/IP e HTTPS para atravessar firewalls, e para autenticação e segurança.

Configuração Fácil

O Communications Server para Linux foi desenvolvido com opções de configuração e recursos que reduzem o tempo de configuração e complexidade da rede. Por exemplo:

Programa de Administração Motif

O modo mais fácil de definir e modificar a configuração do Communications Server para Linux é utilizar o programa de administração Motif (**xsnaadmin**). Esse programa fornece uma interface gráfica com o usuário a partir da qual é possível visualizar e gerenciar os recursos do Communications Server para Linux. Este programa também simplifica a configuração expondo apenas os campos cujos valores geralmente variam de uma instalação para outra, utilizando valores padrão para os outros campos.

O programa de administração Motif inclui telas de ajuda que fornecem informações gerais para o SNA e o Communications Server para Linux, informações de referência para diálogos do Communications Server para Linux e orientação para executar tarefas específicas.

Configuração Dinâmica em Redes APPN

A configuração de um nó ou rede também é facilitada pela configuração dinâmica da rede APPN. Por exemplo, os nós de extremidade APPN e aplicações registram dinamicamente dados da configuração para suportar sessões LU 6.2, tornando assim a configuração da sessão opcional. Além disso, tendo o ponto de controle do nó atuando como a LU local padrão, você pode evitar a configuração da LU 6.2 completamente.

A APPN também suporta configuração de estação de link dinâmica na ausência de estações de link configuradas.

Opções Adicionais da Interface com o Usuário para Administração

O programa de administração Motif é a interface recomendada para configurar e gerenciar o Communications Server para Linux. No entanto, você tem uma variedade de interfaces do Communications Server para Linux, o que permite trabalhar com uma que se ajuste a seu equipamento, necessidades e preferências.

Programa de Administração da Linha de Comandos

O programa de administração da linha de comandos (**snaadmin**) pode ser utilizado para emitir comandos, a fim de gerenciar os recursos individuais do Communications Server para Linux. Você pode utilizar o **snaadmin** diretamente em um prompt de comandos do Linux ou de um script de shell.

API NOF

A API NOF do Communications Server para Linux apresenta as mesmas funções de gerenciamento que um programa de administração de linha de comandos, fornecendo uma interface apropriada para ser utilizada em um programa (em vez de um script de comandos). Você pode utilizar a API NOF para gravar seus próprios programas aplicativos para administrar o Communications Server para Linux.

Melhor Desempenho

O Communications Server para Linux melhora o desempenho naturalmente elevado das redes SNA e utiliza a operação Class of Service. O Communications Server para Linux também otimiza a velocidade da rede por meio da compactação de dados SNA para dados de sessão LU 0-3 e por meio de diferentes métodos de gerenciamento de tráfego que equilibram o fluxo de tráfego de acordo com o tamanho da rede:

- Em redes APPN, o Communications Server para Linux suporta HPR (High-Performance Routing) e o roteamento de sessão intermediária (ISR), e fornece opções de rede para conexão. Embora o ISR funcione eficientemente para redes pequenas, seu desempenho diminui em redes maiores.
- Para redes maiores que utilizam opções de conectividade de rede local (como Token Ring ou Ethernet) ou que utilizam o Enterprise Extender, você também pode utilizar a opção de rede de conexão para melhorar a eficiência da comunicação. A opção de rede de conexão cria um caminho de comunicações diretamente entre os nós. Isso permite que o tráfego desvie de nós de rede intermediários.
- Outro mecanismo de controle de tráfego, o pacing a nível de sessão adaptativo,, ajusta automaticamente o congestionamento regulando a taxa em que as LUs enviam as unidades de mensagens para as LUs associadas.

Opções de Segurança

Com redes se tornando cada vez mais complexas e caminhando no sentido de uma arquitetura aberta, a segurança surge como um assunto primordial. Em redes SNA executando o Communications Server para Linux, é possível proteger os recursos, definindo vários níveis de segurança na configuração ou implementando determinados tipos de links. Por exemplo:

- Num sistema cliente/servidor, é possível configurar um servidor WebSphere para fornecer acesso HTTPS dos Remote API Clients para os servidores. Isso

Recursos e Benefícios

significa que as conexões do cliente são autenticadas utilizando certificados de segurança. (Esse recurso requer algum software adicional, além do produto Communications Server para Linux padrão. Consulte a seção “Requisitos de Instalação” na página 19 para obter mais informações).

- Usuários de LU 6.2 podem definir até três níveis de segurança — sessão, recurso e conversação. Respectivamente, um garante que as próprias LUs estejam engajadas em uma sessão, outro restringe o acesso a todos os aplicativos associados a uma determinada LU e o outro restringe o acesso a um determinado aplicativo. Segurança adicional é possível através de rotinas de criptografia de dados.
- O Servidor TN e o Redirecionador TN do Communications Server para Linux podem fornecer criptografia de dados, autenticação de servidor e autenticação de cliente entre o Communications Server para Linux e os clientes TN3270 ou Telnet, utilizando o software SSL (Secure Sockets Layer). (Esse recurso requer algum software adicional, além do produto Communications Server para Linux padrão. Consulte a seção “Requisitos de Instalação” na página 19 para obter mais informações).

Flexibilidade de Gerenciamento de Rede

O Communications Server para Linux suporta o esquema de gerenciamento de rede MDS-NMVT (Multiple Domain Support-Network Management Vector Transport) o qual pode funcionar como um esquema de gerenciamento centralizado, distribuído ou hierárquico. Ele está baseado em uma arquitetura de ponto focal/ponto de entrada que fornece a você alto grau de flexibilidade.

Os pontos focais são nós de controle que gerenciam a rede de acordo com os dados que eles coletam dos pontos de entrada (aplicações de gerenciamento que residem em todos os outros nós na rede).

- Em gerenciamento centralizado, um único ponto focal atua como um ponto de controle de toda a rede.
- No gerenciamento distribuído, diversos pontos focais compartilham o gerenciamento da rede.
- No gerenciamento hierárquico, os pontos focais são aninhados de acordo com a função.

O MDS-NMVT pode ser adaptado para gerenciar redes de subárea, APPN padrão e APPN de grande porte.

Confiabilidade, Disponibilidade e Serviços

Para ajudar a manter a operação do sistema confiável, o Communications Server para Linux fornece uma série de funções de exibição e ferramentas de diagnóstico de problemas.

- O programa de administração Motif fornece configuração avançada e ferramentas de gerenciamento, incluindo o seguinte:
 - Atualizações imediatas das informações da configuração
 - Informações de status para links, sessões e recursos de nó.
- Os comandos de consulta e de status fornecem a você informações sobre:
 - Sessões LU-LU
 - Sessões imediatas APPN
 - Links Ativos
 - Banco de dados de topologia APPN, que armazena informações sobre o link.

- As ferramentas de diagnóstico de problemas estão disponíveis para auxiliar você durante os diferentes estágios da configuração e operação. Incluem o seguinte:
 - Ferramenta de coleção de informações de diagnóstico (**snagetpd**) para ativar você a coletar facilmente informações de serviços
 - As mensagens de status e de erro auxiliam você a resolver problemas nas rotinas de configuração e operação do sistema.
 - Os logs para coletar informações de erro da rede, falha e auditoria.
 - Recursos de rastreamento para reunir e formatar informações detalhadas de problemas.

Outros utilitários auxiliam você a testar a conectividade do link e a comunicação entre as aplicações.

O Communications Server para Linux também inclui os Serviços de Gerenciamento da API, utilizados para desenvolver ferramentas para envio e recepção de alertas de rede e dados do problema.

Todas essas ferramentas de gerenciamento e de diagnóstico de problemas estão totalmente integradas ao modelo Cliente/Servidor do Communications Server para Linux, portanto é possível gerenciar o domínio inteiro do Communications Server para Linux, ou coletar informações de diagnóstico a partir de um único ponto na rede.

Integração, Crescimento e Alteração de Redes

Para suportar a integração, o crescimento e a alteração da rede, as APIs do Communications Server para Linux, podem ser utilizadas para desenvolver aplicativos para uma determinada LU, plataforma ou sistema operacional conforme a necessidade de seus negócios. O CPI-C é uma API especialmente importante porque é consistente com plataformas e sistemas operacionais diferentes. É utilizado para desenvolver aplicações que podem ser executadas em qualquer sistema.

O Enterprise Extender também fornece um mecanismo para integrar redes SNA e TCP/IP.

Capítulo 2. Planejando a Rede e o IBM Communications Server para Linux

Este capítulo fornece uma visão geral dos estágios de planejamento de uma rede que executa o Communications Server para Linux. Também resume as funções que podem ser configuradas para o computador Linux e apresenta diretrizes para estimar os recursos necessários para suportar as funções.

Estágios do Planejamento da Rede

Esta seção apresenta algumas diretrizes gerais para planejar, configurar e gerenciar redes por meio da utilização de vários utilitários do Communications Server para Linux e do Linux.

O planejamento de uma rede envolve um balanceamento de função, desempenho, recursos e custo. Embora não haja um único e melhor planejamento de uma rede, algumas orientações e técnicas gerais podem ajudar a garantir que seu plano atenda às suas necessidades. Para planejar uma rede, execute as seguintes tarefas

- Determine as funções que a rede deve fornecer (como transferência de arquivo ou emulação 3270) e os requisitos de seu desempenho.
- Determine como o Communications Server para Linux pode ser configurado para fornecer as funções necessárias.
- Faça uma estimativa dos recursos necessários para instalar o Communications Server para Linux, a fim de dar suporte aos requisitos de desempenho e capacidade, às funções do Communications Server para Linux, e identificar os custos associados.

Identificando os Requisitos Funcionais da Rede

Para determinar as funções que sua rede deve fornecer, você precisa considerar as seguintes questões:

- A rede será APPN?
- O Communications Server para Linux será executado como um sistema cliente/servidor? Em caso afirmativo, todos os computadores operarão em um único domínio do Communications Server para Linux ou será necessário definir dois ou mais domínios separados?
- Será necessário mais de um servidor no domínio do Communications Server para Linux a fim de prover o equilíbrio de carga dos recursos de conectividade? Em caso positivo, que servidor será o servidor de configuração master? Preciso fornecer um ou mais servidores de configuração de backup?
- Será necessário dar suporte aos Remote API Clients ao se conectar a servidores Communications Server para Linux utilizando HTTPS?
- Os aplicativos do usuário serão executados no servidor ou em computadores clientes com Linux?
- O servidor fornecerá recursos de conectividade para aplicativos Windows (como programas de transação de API) que executam em clientes Windows?
- Cada servidor deve ser um nó de extremidade para sessões ou deve ser um dos seguintes tipos de gateways?
 - APPN
 - LU 0

Estágios do Planejamento da Rede

- LU 2
- Servidor TN ou Redirecionador TN
- Quais os tipos de links físicos a rede utilizará?
- O Communications Server para Linux precisará suportar o IPv4, IPv6 ou ambos os tipos de conexões?

As respostas a esses tipos de perguntas ajudam a determinar quais funções do Communications Server para Linux são requeridas pela rede.

Determinando Como Configurar o Communications Server para Linux

Para determinar como o Communications Server para Linux deve funcionar, decida primeiro como o trabalho fluirá pela rede. As seguintes questões devem ser consideradas:

- Quais recursos (como aplicações) devem estar disponíveis na rede?
- Quantos usuários precisam ter acesso aos recursos remotos?
- Com que frequência cada recurso é acessado?
- Como os usuários podem ter acesso à rede?
- Como os requisitos dos usuários serão roteados através da rede?

É possível configurar o Communications Server para Linux para suportar muitas funções, incluindo, por exemplo, as que seguem:

- Nó de rede APPN para roteamento de sessão intermediária (ISR)
- Nó de extremidade APPN (que se comunica com autonomia com nós adjacentes mas utiliza serviços de nó de rede APPN para se comunicar com nós de ponto não-adjacentes)
- Nó de rede de entrada baixa (LEN) (que se comunica diretamente com nós adjacentes ou nó configurados para se parecerem com adjacentes)
- Utilização de LU 0, LU 1, LU 2, LU 3 e LU 6.2 (dependente e independente)
- Conexão de gateway SNA a um host

Um ou mais funções podem ser configuradas para um determinado nó, dependendo de suas necessidades. Por exemplo, é possível configurar o Communications Server para Linux como um nó de rede APPN para fornecer serviços de roteamento e ISR, e utilizar o mesmo nó do gateway SNA para rotar sessões LU dependentes, como a LU 0 e LU 2. Do mesmo modo, você pode configurar o Communications Server para Linux para executar o Servidor TN e dar suporte tanto a um banco de dados compartilhado quanto a uma conexão de LU 6.2 independente para o MQSeries no host.

Identificando os Requisitos de Recursos para Instalação e Operação

Para estimar o suporte para as funções do Communications Server para Linux, as seguintes perguntas devem ser feitas:

- Quais habilidades do pessoal você precisa?
- Qual mídia de transporte pretendo utilizar?
- Quais são os requisitos de instalação para a configuração que selecionei?
- Quanto de memória e espaço de paginação preciso para a operação?

As respostas a essas perguntas ajudam a identificar os tipos de recursos que o Communications Server para Linux utiliza quando configurado para dar suporte a uma ou mais funções descritas em “Identificando os Requisitos Funcionais da Rede” na página 17. Também ajuda a compreender o relacionamento entre as funções do Communications Server para Linux, os recursos do Linux e da rede.

A forma como você aloca os recursos para os nós determinará como a rede executará.

Requisitos de Pessoal

A instalação, operação e ajuste do Communications Server para Linux requerem a seguinte equipe:

- Administradores de rede, que planejam a rede, adicionam novos dispositivos e mantenham ou atualizem o desempenho geral da rede.
- Administradores de sistema, que instalam e mantêm o Communications Server para Linux e o hardware no qual opera, e configuram os sistemas para conexão de rede.
- Programadores, que desenvolvem aplicações personalizadas, como programas de transação ou rotinas de gerenciamento de rede.

Os administradores da rede e do sistema devem estar totalmente familiarizados com o hardware no qual o Communications Server para Linux opera e com o sistema operacional Linux. Eles devem conhecer as redes para as quais vários sistemas estão conectados e entender os conceitos SNA em geral. Devem também estar familiarizados com o seguinte:

- A interface do Motif
- **rpm**, a ferramenta de instalação do Linux
- O TCP/IP, se planejarem utilizar as funções do Cliente/Servidor, o servidor TN ou Enterprise Extender
- O sistema operacional Windows 2000, Windows XP, Windows Server 2003 ou Windows Vista, se o sistema Communications Server para Linux incluir Remote API Clients no Windows
- WebSphere Application Server, se o Communications Server para Linux incluir Remote API Clients que se conectem aos servidores utilizando HTTPS

Programadores que desenvolvem aplicativos personalizados para SNA devem ser experientes com a linguagem C (ou Java, se estiverem utilizando o Java CPI-C) e devem estar familiarizados com as APIs disponíveis no Communications Server para Linux.

Mídia de Transporte

Pode ser que o Communications Server para Linux necessite compartilhar o meio de transporte subjacente (como SDLC, Token Ring) com outros protocolos de comunicação. Portanto, os requisitos de largura de banda da camada física devem atender a todos os protocolos e aplicações que compartilham a mídia de transporte.

Nota: O Communications Server para Linux pode compartilhar adaptadores Token Ring e Ethernet com outros protocolos, por exemplo, TCP/IP. Você pode precisar especificar endereços de ponto de acesso de serviço exclusivo (SAP) para cada protocolo a ser utilizado.

Requisitos de Instalação

As funções que designa para o Communications Server para Linux (em “Identificando os Requisitos Funcionais da Rede” na página 17) também

Estágios do Planejamento da Rede

determinam os requisitos de instalação. Esta seção fornece uma visão geral dos recursos do computador requeridos para instalar o Communications Server para Linux. Para obter mais informações, consulte a documentação fornecida com cada produto.

Hardware

O Communications Server para Linux requer um computador suportado por uma das distribuições do Linux abaixo.

Utilize o comando **uname -m** para verificar a classe de CPU do computador de destino. A tabela a seguir mostra o hardware apropriado para cada tipo de servidor e a resposta de **uname -m** para tal hardware.

Tipo do Servidor	Hardware	resposta do uname
Intel de 32 bits	Pentium II ou sistema Intel posterior de 32 bits	i686
x86_64 de 64 bits	Sistema AMD64 ou Intel EM64T	x86_64
pSeries	Sistema pSeries POWER5 ou OpenPower	ppc64

Sistema Operacional Linux

Antes que seja possível instalar e utilizar o Communications Server para Linux na sua estação de trabalho Linux, esta deve apresentar uma versão de sistema operacional Linux apropriada instalada.

O Communications Server para Linux suporta as seguintes variantes do Linux. Para obter informações atualizadas sobre números de versão e builds de kernel específicos suportados por cada variante, além de requisitos adicionais para versões específicas, consulte o arquivo **LEIA-ME** na imagem do CD do Communications Server para Linux.

- RedHat Enterprise Linux 4 (RHEL4)
- RedHat Enterprise Linux Server 5 (RHEL5)
- SUSE Linux Enterprise Server 9 (SLES9)
- SUSE Linux Enterprise Server 10 (SLES10)

Hardware de Link

O hardware de link é necessário somente em um servidor, não em um cliente.

A instalação de um PC em uma ou mais redes requer links que estejam em conformidade com o protocolo de comunicação da rede selecionada. O hardware de link consiste em um adaptador de comunicação que é instalado no computador e em um cabo correspondente para conexão com a rede (também é necessário o software do driver de dispositivo).

Nota:

1. Os adaptadores de comunicação devem ser instalados com seus cabos correspondentes. Por exemplo, um adaptador Ethernet requer um cabo Ethernet para que o link funcione.
2. Se você estiver utilizando o Enterprise Extender como seu único tipo de link, os adaptadores listados nesta seção não serão requeridos; mas será necessário ter um dos adaptadores requeridos pelo TCP/IP.

O Communications Server para Linux suporta adaptadores de comunicação para os seguintes protocolos de link:

- Token Ring
- Ethernet (padrão ou IEEE 802.3)
- SDLC
- X.25 QLLC

Para obter informações sobre os adaptadores testados com o Communications Server para Linux, consulte <http://www.ibm.com/software/network/commsserver>. Se você tiver perguntas sobre o adaptador ou hardware apropriado para as suas necessidades, ligue para um Representante de Vendas IBM.

Software Adicional: Linux

O Communications Server para Linux requer o seguinte software adicional. Consulte o arquivo **LEIA-ME** na imagem do CD do Communications Server para Linux para obter mais detalhes sobre os requisitos específicos da versão (dependendo da variante do Linux), e para obter instruções sobre como instalar esses pacotes de software.

- LiS Streams. Consulte o arquivo **LEIA-ME** para obter detalhes da versão do LiS Streams requerida e instruções de instalação.
- OpenMotif (requerido somente em um servidor, não em um cliente). Ele é requerido para seja possível utilizar o programa de administração Motif, que é o método recomendado de configuração e gerenciamento do Communications Server para Linux.
- Java (requerido se você desejar utilizar Java CPI-C). Você precisará do Java Runtime Environment (JRE). Se precisar compilar novas classes Java para utilizar com um aplicativo Java CPI-C, você também precisará do Java SDK.

WebSphere Application Server (para Acesso HTTPS)

Se estiver executando um sistema cliente/servidor no qual os Remote API Clients se conectam aos servidores Communications Server para Linux utilizando HTTPS, será necessário executar o WebSphere Application Server para fornecer acesso HTTPS dos clientes aos servidores.

O Communications Server para Linux opera com o WebSphere Application Server Versão 5, que pode ser instalado em um computador que execute qualquer sistema operacional suportado pelo WebSphere. (Se necessário, ele pode ser instalado no mesmo computador Linux de um servidor Communications Server para Linux.) Consulte a documentação do WebSphere Application Server para obter informações adicionais sobre a instalação. Também será necessário instalar um plug-in adicional do Communications Server para Linux nesse computador para utilizar o WebSphere com o Communications Server para Linux, conforme descrito em “Configurando o WebSphere Application Server” na página 34.

Memória e Armazenamento

Para suportar uma variedade completa de configurações e serviços, uma estação de trabalho executando o Communications Server para Linux precisa da memória mínima exigida pela distribuição do Linux mais 64 MB, além de 200 MB de espaço em disco. Além disso, precisa de 250 MB de armazenamento temporário durante a instalação.

Se decidir instalar a documentação do Communications Server para Linux na forma de cópia eletrônica (PDF), precisará de armazenamento adicional em disco fixo. Para instalar todos os manuais em cópia eletrônica, você precisará de 80 MB de espaço em disco.

Estágios do Planejamento da Rede

Nota: Os requisitos de memória e disco fixo para outros programas licenciados, aplicativos de usuário e dados não estão incluídos nesses requisitos. Reveja atentamente todos os requisitos de sistema, memória e disco fixo com o representante IBM ou revendedor autorizado.

Configurações Avançadas

Se você pretende executar aplicativos que requerem mais de uma configuração básica, precisará de recursos extras de computador.

Normalmente, os requisitos de memória e armazenamento para executar o Communications Server para Linux dependem de vários fatores diferentes que podem variar com a operação da estação de trabalho Linux e de seu ambiente. Todavia, utilizando a regra prática, considerando que LUs, links ativos e sessões em andamento são consumidores dominantes dos recursos do computador, você pode estimar a quantidade de memória adicional e espaço em disco que é requerido para suportar a maior parte dos aplicativos em demanda.

Requisitos de Memória e de Armazenamento para Operação

Esta seção descreve os requisitos de memória e de armazenamento de uma estação de trabalho executando o Communications Server para Linux.

Memória do Kernel

O Linux utiliza a memória do kernel para ativar a comunicação entre os subsistemas de comunicação e os DLCs. A memória do kernel é um recurso compartilhado que deve ser gerenciado no nível de sistema. O Communications Server para Linux utiliza a memória do kernel para enviar e receber dados na rede, contudo ele é apenas um dos subsistemas que utilizam tal memória. A utilização de recursos da memória do kernel do Communications Server para Linux pode afetar o desempenho de outros subsistemas, como TCP/IP ou NFS. Coordene com o administrador da rede para determinar os requisitos de memória do kernel.

Memória, Disco e Armazenamento de Paginação

O Communications Server para Linux utiliza o armazenamento principal — também conhecido como memória principal e memória RAM (Random Access Memory) — o armazenamento permanente em disco e o armazenamento de paginação em disco (também conhecido como espaço de paginação):

- Os blocos de controle para recursos do SNA—como LUs, links e sessões—utilizam armazenamento principal.
- A memória do kernel utiliza somente armazenamento principal.
- Os executáveis, arquivos de configuração e publicações em cópia eletrônica do Communications Server para Linux utilizam armazenamento permanente em disco.
- Programas aplicativos, sessões e processos relacionados possuem requisitos de espaço de paginação que utilizam armazenamento permanente em disco.

Requisitos de memória e de armazenamento em disco dependem de vários fatores que diferem amplamente de um ambiente para outro. Os TPs (Transaction Programs) e sessões SNA são consumidores dominantes de memória e armazenamento em disco.

Um TP é um programa que utiliza a API (Application Programming Interface) SNA para acessar a rede. Uma sessão é um canal lógico temporário entre duas LUs e nós parceiros. Os TPs utilizam esse canal para se comunicarem uns com os outros.

O consumo de memória e armazenamento em disco é amplamente afetado pelo número total de sessões, o número de sessões alocadas (conversações), a intensidade do tráfego das conversações e o número de TPs de usuário ativo. Os requisitos de memória são principalmente afetados pela intensidade do tráfego de dados e pelo uso resultante da memória do kernel. Os requisitos de armazenamento em disco originam-se nos requisitos de espaço de paginação dos TPs, sessões e processos relacionados.

Para todos os tipos de LU, uma distinção é feita entre uma sessão ociosa e uma sessão alocada. Uma sessão ociosa é uma sessão ativa que não está sendo utilizada por TPs. Uma sessão alocada é uma que suporta uma conversação em andamento. Para estimar o requisito de memória total, você precisa estimar a intensidade do tráfego e a parte do número total de sessões que será alocada, em média, em um determinado tempo. Você também pode escolher configurar o sistema para lidar com a demanda máxima. Essas estimativas variam entre os ambientes.

Se você aumentar a carga de sessões além da capacidade de memória do sistema, recairá no custo de paginação.

Processos

O Communications Server para Linux requer um mínimo de 20 processos do Linux.

Endereçamento IPv4 e IPv6

Os computadores que executam o Communications Server para Linux Versão 6.2.3 podem utilizar os endereços IPv4 ou IPv6, com as seguintes restrições.

- Todos os servidores em um domínio de Cliente/Servidor devem utilizar o mesmo formato de endereçamento (IPv4 ou IPv6).
 - Se os servidores utilizarem IPv4, os clientes também deverão utilizar o IPv4.
 - Se os servidores utilizarem o IPv6, os clientes poderão utilizar o IPv6 ou o IPv4.
- Para o Servidor TN, se o Communications Server para Linux utilizar IPv4, os clientes TN que se conectam ao Servidor TN também devem utilizar o IPv4. Se o Communications Server para Linux utiliza o IPv6, os Clientes TN poderão utilizar IPv6 ou IPv4. Por padrão, o Servidor TN aceita as conexões de ambos os tipos de clientes, mas você pode configurá-los para atender em um determinado endereço IP (utilizando o parâmetro *listen_local_address* no programa de administração da linha de comandos ou de um aplicativo NOF) a fim de restringi-lo a um tipo de conexão do cliente.
- Para Redirecionador TN, se o Communications Server para Linux utilizar IPv4, ambas as conexões TCP/IP (do cliente para o Communications Server para Linux e do Communications Server para Linux para o host) também deverão utilizar o IPv4.

Se o Communications Server para Linux utilizar o IPv6, a conexão TCP/IP do cliente para o Communications Server para Linux seguirá as mesmas regras do Servidor TN. A conexão do Communications Server para Linux para o host pode utilizar IPv6 ou IPv4. Não há requisito para as duas conexões utilizarem o mesmo formato de endereçamento.

Endereçamento IPv4 e IPv6

- Para Enterprise Extender (HPR/IP), as portas em ambas as extremidades de um link devem utilizar o mesmo formato de endereçamento (IPv4 ou IPv6).
 - Se Communications Server para Linux utilizar IPv4, ele poderá conectar-se apenas a sistemas remotos que estiverem configurados para suportar o IPv4.
 - Se o Communications Server para Linux utilizar IPv6, você poderá configurá-lo para utilizar o IPv4 ou IPv6 em um link do Enterprise Extender. A opção que você escolhe deve corresponder à configuração no sistema remoto.

Além disso, todos os links na mesma porta do Enterprise Extender devem utilizar o mesmo formato de endereçamento (IPv4 ou IPv6). Se você precisar suportar os links com diferentes formatos de endereçamento, deverá utilizar portas separadas. De maneira semelhante, todas as portas do Enterprise Extender na mesma rede de conexão devem utilizar o mesmo formato de endereçamento.

Para verificar se um servidor Communications Server para Linux está em execução no IPv4 ou IPv6, utilize o comando **ifconfig -a** e consulte o endereço ou os endereços IP na saída. Eles são os endereços IPv4 decimais com pontos ou endereços IPv6 hexadecimais. Para um Remote API Client no Windows, o comando equivalente é **ipconfig** (sem opções de linha de comandos). Se você precisar alterar o formato de endereçamento IP do computador, consulte a documentação do sistema operacional.

Se você estiver fazendo upgrade de um Communications Server existente para o sistema Linux para a Versão 6.2.3, conforme descrito em “Migrando de Níveis Anteriores do Communications Server para Linux” na página 29, e também desejar alterar o endereçamento IPv6, poderá fazer os dois processos em ordem. No entanto, você não pode utilizar os novos recursos de endereçamento IPv6 na Versão 6.2.3 até que ambos os processos estejam concluídos.

- Para um sistema Cliente/Servidor, você deve alterar todos os servidores no domínio do IPv4 para o IPv6 ao mesmo tempo; não tente executar um domínio misto de servidores IPv4 e IPv6.
- Como o upgrade para o Communications Server para Linux Versão 6.2.3 também requer que você faça upgrade de todos os servidores ao mesmo tempo, é possível optar por fazer a alteração no endereçamento IPv6 ao mesmo momento do upgrade em cada servidor. Como alternativa, é possível alterar todos os servidores para IPv6 antes ou depois do upgrade para a Versão 6.2.3, o que for mais conveniente.
- Depois que todos os servidores forem alterados para utilizar o endereçamento IPv6, será possível alterar os Remote API Clients para utilizarem o endereçamento IPv6 conforme necessário. Os clientes IPv4 podem continuar operando com servidores IPv6; portanto, não há necessidade de alterar todos os clientes ao mesmo tempo.

Se você estiver instalando um novo sistema Communications Server para Linux, poderá instalá-lo apenas com endereçamento IPv6 em todos os servidores e clientes, se apropriado, ou poderá utilizar o endereçamento IPv4 inicialmente e, em seguida, ir para o IPv6 posterior (sujeito às restrições acima para domínios do Cliente/Servidor).

Assegurando Compatibilidade entre Configurações de Plataforma Cruzada

Os produtos SNA executando em plataformas diferentes — por exemplo, o IBM Personal Communications ou Communications Server para Windows, ou o VTAM NCP em um host — pode funcionar com o Communications Server para Linux se determinados requisitos forem satisfeitos.

Em geral, o release atual do produto de rede SNA pode funcionar com o Communications Server para Linux desde que suporte nós PU 2.1 e pelo menos um dos tipos de links suportados pelo Communications Server para Linux. No entanto, alguns releases muito antigos (como VTAM V2) podem não funcionar de modo confiável. As capacidades de cada produto de rede estão documentadas em seu respectivo manual do usuário.

Outros fatores a serem considerados são os seguintes:

- Se você estiver utilizando LU 6.2 independente e sua rede não for APPN, você precisa ter certeza que as LUs estejam definidas para o sistema local.
- Como os valores padrão de tamanhos de janela do DLC e os cronômetros variam de dispositivo para dispositivo, você deve assegurar que seus dispositivos remotos utilizam o valor correto. Por exemplo, um tamanho de janela do DLC que oferece bom desempenho com um nó do Communications Server para Windows pode não desempenhar bem com um nó 3172.
- Quando você trabalha em um ambiente heterogêneo (protocolos TCP/IP e SNA na mesma rede local) com vários segmentos da rede local, assegure que seus dispositivos de interconexão de rede local possam “rotear” TCP/IP e “efetuar ponte” de quadros SNA ao mesmo tempo.

Convenções de Nomenclatura

Você pode utilizar IDs de rede para dividir logicamente sua rede física. Também, se você pretende conectar-se a outras redes, é extremamente recomendado que você registre seus IDs da rede e evite conflitos de nomes na rede.

Você pode definir nomes de rede e de LU da seguinte forma:

Nomes de Rede

Você pode definir nomes de rede diferentes (IDs de rede) para fornecer segmentação de redes APPN. A segmentação limita o tamanho dos bancos de dados da topologia da rede e a frequência de requisitos LOCATE de difusão através de cada rede.

Para assegurar a exclusividade de um ID de rede, um administrador da rede pode registrar o ID da rede com o registro mundial da IBM. O registro IBM assegura que cada ID de rede seja exclusivo entre todos aqueles registrados com ela. Os padrões de registro são consistentes com os padrões de OSI (Open Systems Interconnection), incluindo códigos de país OSI, conforme estabelecidos pelo sistema ISO (International Organization for Standards). Para obter mais informações sobre o registro, consulte a publicação *User's Guide for SNA Network Registry*.

Nomes de LU

Você pode utilizar curingas para nomes de LU para minimizar a definição do sistema e pesquisas na rede.

Convenções de Nomenclatura

Capítulo 3. Instalando o Communications Server para Linux em Servidores Linux

Este capítulo fornece informações gerais sobre as etapas necessárias para instalar o Communications Server para Linux em um servidor Linux. Para obter instruções detalhadas, passo a passo, sobre o processo de instalação, consulte o arquivo **LEIA-ME** na imagem de CD do Communications Server para Linux; tal arquivo apresenta informações detalhadas e atualizadas, específicas para sua variante do Linux. O arquivo **LEIA-ME** inclui:

- Nomes exatos de pacote e/ou números de versão dos pacotes de software adicionais que você precisa
- Detalhes dos comandos de instalação e de configuração.

Como o Programa Licenciado Communications Server para Linux Está Embalado

O Programa Licenciado Communications Server para Linux é entregue em três imagens de CDs contendo o seguinte conteúdo.

CD #1: Início Rápido

Esse CD contém um conjunto completo da documentação em PDF do Communications Server para Linux (no diretório **/DOCS**).

CD #2: Servidor

Esse CD contém os arquivos necessários para instalar um servidor:

- Os arquivos **LEIA-ME** contendo informações sobre quaisquer alterações no produto posteriores à documentação do Communications Server para Linux
- Os scripts de instalação
- As imagens de instalação do servidor e dos manuais em PDF

CD #3: Clientes

Esse CD contém os arquivos **LEIA-ME**, e os scripts e imagens de instalação necessários para instalar cada tipo de cliente:

- Cliente Linux para Intel (i686) de 32 bits
- Cliente Linux para AMD64/Intel EM64T (x86_64) de 64 bits
- Cliente Linux para pSeries (ppc64)
- Cliente Linux para System z9 ou System z (s390 / s390x)
- Cliente AIX
- Cliente Windows de 32 bits
- Cliente Windows x64

Consulte os arquivos **LEIA-ME** para obter detalhes completos dos arquivos incluídos nas imagens de CDs.

Nota: Para consultar os requisitos de espaço em disco, consulte “Requisitos de Instalação” na página 19.

Preparando a Instalação do Communications Server para Linux

Antes de instalar o Communications Server para Linux, execute as seguintes tarefas:

- Verifique se o PC com o Linux não está executando com os recursos de Gerenciamento de Energia ativados.
- Assegure-se de que todos os softwares de pré-requisitos listados em “Requisitos de Instalação” na página 19 estejam instalados.

As seções a seguir fornecem informações sobre estas tarefas.

Desativando Recursos Power Management

Antes de instalar o Communications Server para Linux, é necessário verificar se o PC com o Linux inclui o Gerenciamento Avançado de Energia. Em caso afirmativo, você deverá assegurar que esses recursos estejam desativados. Muitos PCs agora incluem esses recursos, projetados para economizar energia se o teclado ou o mouse não estiver sendo utilizado (suspendendo a energia para dispositivos, como unidades de disco, e reduzindo a taxa de clock da CPU). O Advanced Power Management foi projetado para ser utilizado com o PC como uma estação de trabalho; ele não é apropriado quando o PC está operando como um servidor, pois um servidor pode estar operando normalmente sem que o teclado ou o mouse esteja funcionando.

Para desativar esses recursos, acesse a Configuração do BIOS durante a inicialização do PC (normalmente pressionando F1 durante a inicialização do hardware) e desative o Advanced Power Management e o Hardware Power Management.

Para remover o recurso Advanced Power Management do PC, utilize o seguinte comando:

```
rpm -e apmd
```

Instalando o Software de Pré-requisito

Antes de instalar o Communications Server para Linux, instale o software de pré-requisito listado em “Requisitos de Instalação” na página 19:

- LiS Streams
- OpenMotif
- Java
- SSL

Para obter todos os detalhes sobre os pacotes de software exigidos e instruções passo a passo para instalá-los, consulte o arquivo **LEIA-ME** na imagem de CD do Communications Server para Linux.

Exibindo os Detalhes da Instalação do Produto

É possível exibir informações sobre o Communications Server para Linux e os pacotes de software relacionados já instalados. Para listar todos os pacotes instalados, utilize o seguinte comando:

```
rpm -q -a
```

Para visualizar mais detalhes de um pacote específico, utilize o seguinte comando:

```
rpm -q -i packagename
```

packagename é o nome base do pacote instalado, por exemplo **ibm-commserver**.

Alterando a Variável Language Environment

Quando utilizar o Communications Server para Linux, certifique-se de que a variável LANG esteja configurada corretamente para indicar o idioma a ser utilizado.

Utilize o seguinte comando para alterar a variável LANG:

```
export LANG=language
```

Substitua *language* pelo identificador do idioma que deseja utilizar, o qual pode ser um dos seguintes:

Identificador	Idioma
en_US	Inglês (Estados Unidos)
ja_JP	Japonês (PC)
de_DE	Alemão
es_ES	Espanhol
fr_FR	Francês
ko_KR	Coreano
pt_BR	Português
zh_CN	Chinês (simplificado)
zh_TW	Chinês (tradicional)

Migrando de Níveis Anteriores do Communications Server para Linux

Considerações

Se você estiver fazendo upgrade para o Communications Server para Linux Versão 6.2.3 a partir de uma versão anterior do Communications Server para Linux, precisará considerar o seguinte.

1. Se você estiver executando o Communications Server para Linux em uma configuração Cliente/Servidor com dois ou mais servidores, será aconselhado a fazer upgrade de todos os servidores para a Versão 6.2.3 ao mesmo tempo, antes de fazer upgrade dos Remote API Clients.
 - Enquanto você estiver no processo de migração dos servidores, não conseguirá utilizar o programa de administração Motif ou o programa de administração da linha de comandos em um servidor compatível com níveis anteriores para visualizar e gerenciar os recursos em um servidor que execute a Versão 6.2.3.
 - As versões anteriores do Remote API Client não funcionarão com o Communications Server para Linux Versão 6.2.3.
 - A Versão 6.3.1.0 do Remote API Client não funcionará com o Communications Server para Linux 6.2.2, mas apenas se o sistema operacional no cliente não estiver configurado para utilizar o IPv6.
2. Diversas estruturas de dados na API NOF foram modificadas para aceitar formatos de endereços maiores necessários para endereços IPv6. Isso significa que, se você utilizar qualquer um dos seguintes verbos e/ou indicações em um aplicativo NOF existente (mesmo se não estiver utilizando os novos recursos de endereçamento IPv6), será necessário recompilar o aplicativo para utilizá-lo com o Communications Server para Linux Versão 6.2.3.

Migrando de Níveis Anteriores do Communications Server para Linux

- DEFINE_LS, DEFINE_PORT, QUERY_LS, QUERY_PORT quando utilizado com um Enterprise Extender (HPR/IP) LS ou porta
 - 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 (para qualquer tipo de LU)
 - TN_REDIRECTION_INDICATION
3. Se você deseja utilizar os novos recursos de endereçamento IPv6 da Versão 6.2.3, será necessário assegurar-se de que os servidores Communications Server para Linux estejam configurados para utilizar o endereçamento IPv6. Consulte “Endereçamento IPv4 e IPv6” na página 23 para obter mais detalhes.
 4. Se você estiver executando o SDLC ou o X.25 (QLLC) com um adaptador OEM, será necessário entrar em contato com o fabricante para obter drivers atualizados. Os drivers do 6.2.2 não funcionam com o Communications Server para Linux Versão 6.2.3.

Processo de Migração

Se você tiver uma versão anterior do Communications Server para Linux instalada e estiver migrando agora para a Versão 6.2.3, precisará executar as seguintes etapas:

Salvar Todos os Arquivos de Configuração Personalizados

Se qualquer um dos arquivos listados a seguir existir, salve-os em um diretório temporário. Nem todos esses arquivos existirão em todas as instalações.

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

Além disso, se tiver personalizado o arquivo de inicialização, `/etc/rc.d/init.d/snastart`, conforme descrito em “Ativando o Communications Server para Linux” na página 72 para remover o comando `sna start`, de modo que o Communications Server para Linux não inicie automaticamente na inicialização do sistema, tome note de todas as alterações feitas nesse arquivo.

Desinstalar o Release Antigo

Utilize os seguintes comandos no intuito de parar o Communications

Migrando de Níveis Anteriores do Communications Server para Linux

Server para Linux e desinstalá-lo. Dependendo da versão anterior instalada e de como foi instalada, pode que o seu sistema não possua todos os pacotes RPM.

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

Desinstalar o LiS

Utilize os comandos a seguir para desinstalar o nível atual do pacote de código aberto do LiS.

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

Alterar o PATH e Outras Variáveis de Ambiente

Se você modificou alguma das seguintes variáveis de ambiente para a versão anterior do Communications Server para Linux, remova as alterações feitas, visto que os caminhos podem ser diferentes para o produto do programa Communications Server para Linux Versão 6.2.3.

```
PATH
LD_LIBRARY_PATH
LD_RUN_PATH
LD_PRELOAD
CLASSPATH
```

Você poderá utilizar o comando **env** para verificar todas as variáveis de ambiente de referências ao **sna**:

```
env | grep sna
```

Outros Pacotes

É recomendável verificar a instalação do Java e, se necessário, atualizá-la para o nível mais recente.

Limpeza Final

O seguinte comando removerá quaisquer itens restantes do nível antigo do produto. Dependendo da versão anterior instalada, pode ser que o seu sistema não possua todos os diretórios listados.

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

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

Migrando de Níveis Anteriores do Communications Server para Linux

Instale o novo nível do produto do programa Communications Server para Linux Versão 6.2.3

Siga as instruções neste manual e no arquivo **LEIA-ME** para instalar o produto.

Restaurar a Configuração Salva

Se você salvou quaisquer arquivos de configuração na primeira etapa deste processo, agora é o momento de restaurá-los. Em primeiro lugar, pare o software do Communications Server para Linux com o seguinte comando:

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

Se salvou quaisquer arquivos **ibmcs.*** na primeira etapa do processo, remova **todos** os arquivos **ibmcs.*** do diretório **/etc/opt/ibm/sna** agora. Por exemplo, se salvou os arquivos **ibmcs.kdb** e **ibmcs.sth**, será necessário remover os arquivos **ibmcs.crl** e **ibmcs.rdb**, mesmo que não tenha os arquivos salvos para substituí-los. É importante não executar com uma mescla de arquivos salvos e novos.

Restaurar os arquivos salvos para o diretório **/etc/opt/ibm/sna**.

Além disso, se as alterações no arquivo de inicialização (**/etc/rc.d/init.d/snastart**) foram salvas, reproduza as mesmas alterações na nova cópia do arquivo, conforme descritas em “Ativando o Communications Server para Linux” na página 72, para garantir que o Communications Server para Linux não inicie automaticamente na inicialização do sistema.

Agora, inicie novamente o software do Communications Server para Linux com o seguinte comando:

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

Instalando o Programa Licenciado Communications Server para Linux

Depois de instalar o software de pré-requisito, conforme descrito em “Instalando o Software de Pré-requisito” na página 28, você está pronto para instalar o Communications Server para Linux. Utilize o seguinte procedimento:

1. Efetue login em uma sessão com privilégios de root.
2. Instale o Communications Server para Linux, conforme descrito em “Instalando o Communications Server para Linux” na página 33.
3. Se instalou o software GSKIT para utilizar o Servidor TN ou Redirecionador TN com o recurso SSL, precisará configurar o software SSL após a instalação do Communications Server para Linux. Consulte “Configurando o SSL para Uso com o Servidor TN ou Redirecionador TN” na página 36 para obter informações adicionais.
4. Personalize as informações de configuração do Communications Server para Linux à medida do necessário (consulte o Capítulo 8, “Configurando e Utilizando o Communications Server para Linux”, na página 69 ou *Communications Server for Linux - Administration Guide*).
5. Inicie o Communications Server para Linux. Observe que, após a instalação, isso ocorrerá automaticamente quando a máquina for reinicializada.

```
cd /  
sna start
```

Nota:

Instalando o Programa Licenciado Communications Server para Linux

1. A instalação do Communications Server para Linux reconfigura automaticamente os drivers de dispositivo do SNA no nó local. Se estiver instalando em um computador com memória limitada, por exemplo, 64 MB, talvez seja necessário reinicializar após a instalação do Communications Server para Linux, antes de iniciar o nó SNA.
2. Será possível instalar os adaptadores após a instalação do Communications Server para Linux. Ao incluir um adaptador, não é necessário reinstalar o Communications Server para Linux.

Instalando o Communications Server para Linux

1. Insira o CD de instalação na unidade apropriada, na estação de trabalho Linux.
2. Efetue login em uma sessão com privilégios de root.
3. Execute o programa **installibmcs** a partir do CD. Consulte o arquivo **LEIA-ME**, na imagem de CD do Communications Server para Linux, para obter detalhes sobre os comandos necessários para tal.

Normalmente, o programa solicita o seguinte:

- Confirmação de que os termos da licença do Communications Server para Linux foram lidos e aceitos.
- O nome do servidor que atuará como master no domínio do Communications Server para Linux. Para executar o Communications Server para Linux como um nó independente, não especifique esse parâmetro; nesse caso, o nó não suportará as funções de cliente/servidor.

Você pode substituir esses avisos especificando parâmetros adicionais no comando **installibmcs**, conforme descrito a seguir.

4. Para instalar a documentação em PDF do Communications Server para Linux, execute **installibmcsdocs** a partir do CD.
5. Personalize as informações de configuração do Communications Server para Linux (consulte Capítulo 8, “Configurando e Utilizando o Communications Server para Linux”, na página 69 ou *Communications Server for Linux Administration Guide*).

Se precisar executar uma instalação não assistida, é possível fornecer parâmetros adicionais no comando **installibmcs** para confirmar a aceitação dos termos da licença do Communications Server para Linux e especificar o nome do servidor master. Nesse caso, o script do shell será executado sem solicitar informações adicionais. Utilize o seguinte comando:

```
./installibmcs license_accepted [ master_name ]
```

master_name é o nome do servidor master. Para executar o Communications Server para Linux como um nó independente, não especifique esse parâmetro; nesse caso, o nó não suportará as funções de cliente/servidor.

Nota: A instalação do Communications Server para Linux reconfigura automaticamente os drivers de dispositivo do SNA no nó local.

Documentação On-line do Communications Server para Linux

Siga as etapas em “Instalando o Communications Server para Linux” para carregar o CD de instalação do Communications Server para Linux, efetuar login com privilégios de root e executar o script de shell **installibmcsdocs**:

```
./installibmcsdocs
```

HACL (Host Access Class Libraries)

Os arquivos HACL são instalados automaticamente durante a instalação do Communications Server para Linux. O código da biblioteca está no pacote **ibm-commserver-ecl**, em rpm. Esses arquivos podem ser localizados, inclusive o LEIA-ME, em `/opt/ibm/sna/ecl`, ou emitindo o comando a seguir:

```
rpm -ql ibm-commserver-ecl
```

Configurando o WebSphere Application Server

Se executar um sistema cliente/servidor no qual Remote API Clients se conectem aos servidores Communications Server para Linux via HTTPS, um computador precisa executar o WebSphere Application Server para prover acesso HTTPS desses clientes aos servidores, conforme descrito em “Requisitos de Instalação” na página 19.

Esta seção descreve como configurar o WebSphere para ser utilizado com o Communications Server para Linux:

- Configurando um certificado seguro no servidor WebSphere para ser apresentado aos clientes
- Configurando o WebSphere Application Server para trabalhar com o Communications Server para Linux
- Instalando o arquivo de configuração do servidor no servidor WebSphere

Também será necessário configurar o certificado de segurança do cliente e o arquivo de dados da rede do cliente em cada Remote API Client para acessar o WebSphere Application Server. Para obter informações adicionais, consulte o capítulo sobre como instalar o tipo de cliente apropriado.

Configurando o Certificado de Segurança do WebSphere Application Server

Consulte a documentação do WebSphere Application Server para obter instruções sobre como configurar um certificado de segurança no servidor. Esse certificado do servidor será apresentado a um Remote API Client no processo de autenticação, durante a tentativa de conexão via HTTPS.

É recomendado configurar o WebSphere de modo a tornar a autenticação do cliente mais rígida; consulte a documentação do WebSphere Application Server para obter mais informações. Isso significa que o WebSphere solicitará certificados de segurança dos Remote API Clients durante o processo de autenticação e aceitará uma conexão de entrada a partir de um Remote API Client apenas se for possível verificar a autenticidade do certificado do cliente.

Configurando o WebSphere Application Server

Para configurar o WebSphere Application Server de modo a operar com o Communications Server para Linux, execute as seguintes etapas. Consulte a documentação do WebSphere Application Server para obter informações adicionais.

1. Copie ou transfira por FTP os arquivos **snahttpsrv.ear** e **snahttpsrv.cfg** do diretório **ibm-commserver-https** no Remote API Client para um diretório no computador no qual o console de administração do WebSphere executa, ou para um diretório de rede acessível a tal computador.

Se o console de administração estiver executando no Windows, não é necessário copiar os arquivos uma vez que é possível acessá-los diretamente

no CD. Apenas insira o CD de instalação do Remote API Client na unidade de disco de CD-ROM do computador Windows.

2. Inicie o console de administração do WebSphere.
3. Observe as orientações na documentação do WebSphere para criar um host virtual acessível apenas via uma conexão segura SSL. Esse host virtual será utilizado para o plug-in Java que gerencia as conexões HTTPS do SNA.
4. Na barra de menus, selecione Aplicativos, Instalar Novo Aplicativo.
5. Especifique o local do arquivo **snahttpsrv.ear**. Selecione o botão Avançar.
6. Ao receber um aviso para especificar o nome de um host virtual nas primeiras duas telas, insira o nome do host virtual configurado para HTTPS. Para os demais parâmetros, você pode aceitar as opções padrão, exceto se precisar utilizar qualquer configuração específica do WebSphere; clique no botão Avançar nos seguintes diálogos até ele ser substituído pelo botão Concluir, em seguida, pressione o botão Concluir. A tela deve apresentar **Aplicativo instalado com êxito**.
7. Clique em Salvar para Configuração Master e pressione o botão Salvar.
8. Na barra de menus, selecione Aplicativos, Aplicativos do Enterprise.
9. Localize **SnaHttpTransport** na lista de aplicativos, marque a caixa de opções ao lado dele e clique no botão Iniciar para iniciá-lo. (Depois disso, o aplicativo iniciará automaticamente quando o WebSphere Application Server for iniciado.)
10. Na barra de menus, selecione Ambiente, Atualizar Plug-in do Servidor da Web, e clique no botão OK. Isso atualiza a configuração do WebSphere.

Instalando o Arquivo de Configuração do Servidor

Para operar com o Communications Server para Linux, o WebSphere Application Server requer uma lista dos servidores Communications Server para Linux que serão acessados via HTTPS. Crie e instale essa lista utilizando as etapas a seguir.

1. Na barra de menus do console de administração do WebSphere, selecione Ambiente, Gerenciar Variáveis do WebSphere.
2. Procure a variável **USER_INSTALL_ROOT** nessa lista e observe seu valor (que é o caminho de um diretório no servidor WebSphere). A lista de variáveis do ambiente pode se estender por duas ou mais páginas, portanto, utilize o botão Avançar para rolar a lista, se necessário.
3. Copie o arquivo **snahttpsrv.cfg** do local em que foi salvo no “Configurando o WebSphere Application Server” na página 34 (ou do CD de instalação) para o diretório especificado pela variável **USER_INSTALL_ROOT**, e edite o arquivo utilizando um editor de texto de modo a incluir uma lista de servidores Communications Server para Linux acessíveis aos Remote API Clients via HTTPS. Cada servidor deve ser especificado numa linha separada do arquivo, no seguinte formato:

```
server=servername.domainname.com
```

Procedimentos Pós-instalação

Esta seção explica como executar tarefas de manutenção que podem ser necessárias após a instalação do Communications Server para Linux.

Operação de Cliente/Servidor

Depois da instalação, o Communications Server para Linux inicialmente opera um servidor independente (com todos os componentes num sistema Linux). Para executá-lo como um servidor em um domínio cliente/servidor, consulte o capítulo

Procedimentos Pós-instalação

Gerenciando Sistemas Cliente/Servidor do Communications Server para Linux no *Communications Server para Linux: Guia de Administração* para obter instruções.

Visualizando Manuais em PDF

Os manuais incluídos na mídia de instalação deste produto estão no formato PDF (Portable Document Format). O formato eletrônico permite que você pesquise, percorra ou imprima as informações mais facilmente, utilizando links de hipertexto para obter informações relacionadas. Também facilita o compartilhamento de biblioteca no seu site, pois os visualizadores de PDF estão disponíveis para muitas plataformas diferentes.

Se você escolher instalar os manuais em PDF quando instalar o produto, eles serão instalados no diretório `/opt/ibm/sna/docs`. Os manuais também são incluídos no diretório `/DOCS` na mídia de instalação do Communications Server para Linux.

Você pode ler os manuais em PDF utilizando qualquer visualizador de PDFs, como o Adobe Acrobat no Windows ou o `xpdf` no Intel Linux.

Revisando as Informações sobre o Release Atual

A atualização mais recente do arquivo **LEIA-ME** do produto, contido no diretório `/opt/ibm/sna`, possui informações sobre quaisquer alterações do produto posteriores à publicação da biblioteca do Communications Server para Linux. Esse arquivo também é incluído no diretório raiz da mídia de instalação do Communications Server para Linux. Reveja o arquivo **LEIA-ME** sempre que receber atualizações do produto.

Configurando o SSL para Uso com o Servidor TN ou Redirecionador TN

Se instalou o software GSKIT para utilizar o Servidor TN ou Redirecionador TN com o recurso SSL, precisará configurar o software SSL após a instalação do Communications Server para Linux.

O software SSL requer dois componentes:

- Um par de chaves é requerido para executar a criptografia e decriptografia dos dados.
- Um certificado é requerido para permitir a autenticação do servidor.

O certificado e o par de chaves formam um único registro em um banco de dados do conjunto de chaves, que é armazenado no servidor Communications Server para Linux que executa o Servidor TN ou o Redirecionador TN. O Communications Server para Linux utiliza o banco de dados para implementar o SSL.

Para gerenciar o banco de dados do conjunto de chaves, digite o seguinte comando no prompt de comandos do Linux:

snakeyman

O comando **snakeyman** ativa um programa Java. Consulte o auxílio fornecido com este programa para obter mais instruções.

Cada registro no banco de dados é identificado por um nome exclusivo conhecido como um rótulo. Se você tiver dois ou mais registros a utilizar em diferentes sessões do Servidor TN ou Redirecionador TN, você precisa tomar nota dos rótulos

que atribuiu quando estava configurando o banco de dados; esses rótulos são utilizados para identificar quais registros devem ser utilizados em cada sessão. Você também pode identificar um dos registros como o padrão, assim as sessões utilizarão este registro, a menos que você especifique explicitamente o rótulo de um registro diferente.

Depois de utilizar o **snakeyman** para atualizar os certificados do servidor, saia do programa **snakeyman**, pare e reinicie o nó Communications Server para Linux a fim de utilizar os certificados atualizados. Utilize os seguintes comandos para parar e reiniciar o nó:

```
snaadmin term_node  
snaadmin init_node
```

Fazendo Backup dos Arquivos de Configuração do Communications Server para Linux

O Communications Server para Linux faz backup automaticamente do nó, do domínio e dos arquivos de configuração do TP todas as vezes que fizer alterações que afetem tais arquivos (utilizando alguma ferramenta de administração do Communications Server para Linux). Por exemplo, ao fazer uma alteração que afete o arquivo de configuração do nó (**sna_node.cfg**), o Communications Server para Linux cria um arquivo de backup denominado **sna_node.bk n** , onde n é 1 ou 2:

- A primeira vez que você alterar o arquivo, a configuração existente é salva em **sna_node.bk1**.
- A segunda vez que você alterar o arquivo, a configuração é salva em **sna_node.bk2**, deixando o arquivo **sna_node.bk1** inalterado.
- A terceira vez que você alterar o arquivo, e as vezes subseqüentes, o arquivo **sna_node.bk1** é descartado, **sna_node.bk2** é renomeado para **sna_node.bk1**, e a configuração existente é salva em **sna_node.bk2**.

Esse processo significa que existe um máximo de dois arquivos cópia de segurança para o arquivo de configuração do nó em qualquer momento. O mesmo processo é utilizado para gerar extensões de nome de arquivo para outros arquivos cópia de segurança.

Além dos arquivos de cópia de segurança automáticos, faça arquivos de cópia de segurança dos arquivos de configuração para proteger-se contra perda de dados em uma das seguintes condições:

- Antes de instalar um novo nível do sistema operacional Linux
- Antes de instalar um novo release do Communications Server para Linux
- Depois de criar uma nova configuração

É possível fazer backup de todos arquivos de configuração com os seguintes comandos:

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

Restaurando uma Cópia de Backup de Arquivos de Configuração do Communications Server para Linux

Para restaurar os arquivos de configuração do Communications Server para Linux a partir do backup, conforme descrito em “Fazendo Backup dos Arquivos de Configuração do Communications Server para Linux” na página 37, execute o procedimento a seguir:

1. Verifique que o Communications Server para Linux não esteja ativo. Para saber se está ou não, digite o seguinte comando:

```
snaadmin status_node
```

Se o Communications Server para Linux estiver ativo, o comando exibirá informações sobre o status do nó local; caso contrário, exibirá uma mensagem indicando que o Communications Server para Linux está inativo.

Se o Communications Server para Linux estiver ativo, digite o seguinte comando para desativá-lo:

```
sna stop
```

2. Digite os seguintes comandos:

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

Nesse comando, *Devicename* é o caminho e o nome de arquivo do dispositivo que você utilizou ao fazer o backup dos arquivos.

Esse comando substitui quaisquer arquivos de configuração existentes com os mesmos nomes no diretório */etc/opt/ibm/sna*.

Reinicializando os Arquivos de Configuração

Se os arquivos de configuração do Communications Server para Linux forem inadvertidamente modificados de modo que as informações contidas neles não possam mais ser utilizadas, talvez seja necessário reinicializar os arquivos para que possa reconfigurar o Communications Server para Linux como se fosse recém-instalado. Isso deve ser feito somente se você tiver certeza de que as informações de configuração não podem ser recuperadas.

Nota: Se você tiver arquivos de configuração de backup que são válidos, poderá copiar esses arquivos para o diretório */etc/opt/ibm/sna* e utilizá-los para inicializar o nó utilizando o comando **sna start**.

É possível reinicializar os seguintes arquivos de configuração:

- O arquivo de configuração de nó, **sna_node.cfg**
- O arquivo de configuração de domínio, **sna_domn.cfg**
- O arquivo de configuração de TP, **sna_tps**
- O arquivo do banco de dados do conjunto de chaves SSL e o arquivo stash de senha

Siga estas etapas para reinicializar os arquivos de configuração:

1. Saia do programa de administração, se estiver ativo, e desative o Communications Server para Linux emitindo o seguinte comando:

```
sna stop
```

2. Crie um arquivo de segurança dos arquivos de configuração existentes copiando os arquivos que estão sendo reinicializados para outro local.

3. Elimine os arquivos que estão sendo reinicializados.
4. Se excluiu o arquivo de configuração de domínio, emita o seguinte comando para recriá-lo (copiando do arquivo de configuração de domínio vazio fornecido com o Communications Server para Linux):

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

Esse comando cria um novo arquivo de configuração de domínio, que é requerido para iniciar o Communications Server para Linux.

5. Se excluiu o arquivo de banco de dados do conjunto de chaves SSL, emita o comando a seguir para recriá-lo (copiando do arquivo de amostra fornecido com o Communications Server para Linux):

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

6. Emita o seguinte comando para reiniciar o Communications Server para Linux:

```
sna start
```

7. Inicie o programa de administração Motif:

```
xsnaadmin &
```

Se o arquivo **sna_node.cfg** não existir, o programa de administração solicitará a configuração do nó. Você pode continuar configurando o nó e outros recursos, conforme descrito no Capítulo 8, “Configurando e Utilizando o Communications Server para Linux”, na página 69 ou no *Communications Server for Linux Administration Guide*.

Se você tiver usado um arquivo **sna_node.cfg** válido, o novo arquivo de configuração será usado para inicializar o nó.

Desinstalando o Communications Server para Linux

Você pode desinstalar o produto Communications Server para Linux a qualquer momento. Utilize o seguinte procedimento:

1. Efetue login em uma sessão com privilégios de root.
2. Verifique que o Communications Server para Linux não esteja ativo. Para saber se está ou não, digite o seguinte comando:

```
snaadmin status_node
```

Se o Communications Server para Linux estiver ativo, o comando exibirá informações sobre o status do nó local; caso contrário, exibirá uma mensagem indicando que o Communications Server para Linux está inativo.

Se o Communications Server para Linux estiver ativo, digite o seguinte comando para desativá-lo:

```
sna stop
```

3. Remova o pacote do Communications Server para Linux e os pacotes de software associados utilizando as seguintes instruções:

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

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

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

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

Capítulo 4. Instalando o IBM Remote API Client no Linux

Este capítulo descreve como instalar o IBM Remote API Client no Linux, permitindo que uma estação de trabalho do Linux execute aplicativos SNA sem ter uma instalação completa da pilha SNA. Um Remote API Client no Linux pode se conectar a um ou mais servidores Communications Server para Linux (ou servidores CS/AIX, contudo não ambos ao mesmo tempo) utilizando uma rede TCP/IP. (Servidores CS Linux não podem operar no mesmo domínio que os servidores CS/AIX.)

Este capítulo se aplica a Remote API Clients IBM executando em Intel (i686) de 32 bits, AMD64/Intel EM64T (x86_64) de 64 bits e pSeries (ppc64). Se você estiver instalando o IBM Remote API Client em um computador System z (s390 / s390x), consulte Capítulo 5, “Instalando IBM Remote API Clients no Linux para System z”, na página 47.

O programa de instalação e arquivos associados, incluindo o arquivo LEIA-ME do IBM Remote API Client, estão localizados no CD de instalação, no diretório apropriado para seu tipo de cliente:

Tipo de Cliente	Diretório no CD
Intel de 32 bits (i686)	<code>/ibm-commserver-clients/linux</code>
AMD64/Intel EM64T (x86_64) de 64 bits	<code>/ibm-commserver-clients/linux-x86_64</code>
pSeries (ppc64)	<code>/ibm-commserver-clients/linux—ppc64</code>

É recomendado ler o arquivo LEIA-ME do IBM Remote API Client antes de instalar o software.

Se você estiver fazendo upgrade de uma versão anterior do Communications Server para Linux e Remote API Clients, recomenda-se que faça upgrade de todos os servidores antes de fazer upgrade dos Remote API Clients. Consulte “Migrando de Níveis Anteriores do Communications Server para Linux” na página 29 para obter mais detalhes.

Requisitos de Hardware e Software

Requisitos de Hardware

O IBM Remote API Client requer um computador suportado por uma das distribuições do Linux abaixo.

Utilize o comando **uname -m** para verificar a classe de CPU do computador de destino. A tabela a seguir mostra o hardware apropriado para cada tipo de cliente e a resposta de **uname -m** para tal hardware.

Tipo de Cliente	Hardware	resposta do uname
Intel de 32 bits	Pentium II, sistema Intel posterior ao de 32 bits ou sistema baseado em Opteron	i686

Requisitos de Hardware e Software

Tipo de Cliente	Hardware	resposta do uname
AMD64/Intel EM64T de 64 bits	Sistema x86_64 (AMD64 ou Intel EM64T)	x86_64
pSeries	Sistema pSeries POWER5 ou OpenPower	ppc64

Versão do Sistema Operacional Linux

A versão atual do IBM Remote API Client foi testada com as seguintes versões do sistema operacional Linux. Também pode executar satisfatoriamente em outras distribuições do Linux.

- RedHat Enterprise Linux 4 (RHEL4)
- RedHat Enterprise Linux 5 (RHEL5)
- SUSE Linux Enterprise Server 9 (SLES9)
- SUSE Linux Enterprise Server 10 (SLES10)

Consulte o arquivo **LEIA-ME** no CD de instalação para obter detalhes sobre quais pacotes opcionais podem ser necessários.

Java

Se utilizar a API Java CPI-C, precisará do software Java. Consulte o arquivo **LEIA-ME** no CD de instalação para obter detalhes.

GSKIT

Se o cliente se conectar aos servidores Communications Server para Linux utilizando HTTPS, o software GSKIT será necessário para ativar o acesso HTTPS aos servidores por meio de um servidor WebSphere. O software GSKIT está incluído no CD de instalação, mas talvez precise de alguns pacotes opcionais do sistema operacional Linux para instalá-lo; consulte o arquivo **LEIA-ME** no CD de instalação para obter detalhes sobre quais pacotes opcionais podem ser necessários.

Se todos os pacotes de pré-requisitos estiverem instalados ao executar o processo de instalação do cliente, descrito mais tarde neste capítulo, o software GSKIT será automaticamente instalado como parte desse processo. Caso contrário, você pode instalá-lo mais tarde.

Exibindo os Detalhes da Instalação do Produto

É possível exibir informações sobre o Remote API Client e os pacotes de software relacionados já instalados. Para listar todos os pacotes instalados, utilize o seguinte comando:

```
rpm -q -a
```

Para visualizar mais detalhes de um pacote específico, utilize o seguinte comando:

```
rpm -q -i packagename
```

packagename é o nome base do pacote instalado, por exemplo **ibm-commserver-client**.

Definindo a Variável Language Environment

Utilize o comando a seguir para alterar a variável LANG para indicar o idioma a ser utilizado:

```
export LANG=language
```

Substitua *language* pelo identificador do idioma que deseja utilizar, o qual pode ser um dos seguintes:

Identificador	Idioma
en_US	Inglês (Estados Unidos)
ja_JP	Japonês (PC)
de_DE	Alemão
es_ES	Espanhol
fr_FR	Francês
ko_KR	Coreano
pt_BR	Português
zh_CN	Chinês (simplificado)
zh_TW	Chinês (tradicional)

Instalando o Remote API Client no Linux

Depois de instalar o software de pré-requisito, você está pronto para instalar o IBM Remote API Client.

Se tiver um nível anterior do IBM Remote API Client instalado, siga as etapas na seção “Desinstalando o Remote API Client no Linux” na página 45 para removê-lo antes de instalar esse novo nível. Quaisquer informações de configuração serão mantidas para serem utilizadas pela nova instalação.

1. Efetue login em uma sessão com privilégios de root.
2. Monte o CD e altere o diretório para ele.

```
mount /dev/cdrom
cd /media/cdrom
```

O nome do diretório **/media/cdrom** pode ser diferente se você tiver uma unidade de DVD. Utilize o comando **df** para verificar se o Linux montou o CD.

3. Altere para o subdiretório apropriado no CD e execute o script do shell para instalar o cliente. O exemplo abaixo mostra o diretório **/linux** de um cliente Intel (i686) de 32 bits; substitua-o pelo **/linux-x86_64** ou **/linux-ppc64**, se necessário.

```
cd ibm-commsrver-clients/linux
./installibmccli
```

O script de shell testará certos pré-requisitos e emitirá mensagens de aviso se não forem atendidos. Você receberá um aviso para ler e aceitar o acordo de licença; em seguida, a ferramenta de script instalará os RPMs. Se os pré-requisitos apropriados já estiverem presentes, o script instalará o software GSKIT.

4. Inclua os diretórios binários do IBM Remote API Client em PATH. Você pode desejar alterar o seu perfil para fazer isso automaticamente:

```
export PATH="$PATH:/opt/ibm/sna/bin"
export LD_LIBRARY_PATH=/usr/lib:/opt/ibm/sna/lib
```

Instalando o Remote API Client no Linux

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

Para aplicativos Java CPI-C, você também deve definir a seguinte variável de ambiente:

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

Para alguns aplicativos, você também pode precisar definir a variável de ambiente LD_PRELOAD, mas não deve fazer disso uma alteração global em seu perfil:

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

5. Inicie o IBM Remote API Client. Após a instalação, isso acontecerá automaticamente quando a máquina for reinicializada. Certifique-se de não estar nos diretórios do CD ao fazer isso.

```
cd /  
sna start
```

Nota: Antes que o IBM Remote API Client possa se conectar a servidores via HTTPS, utilize o programa do gerenciador de chaves GSKIT para definir a configuração do certificado de segurança no cliente. Consulte “Configurando Certificados de Segurança HTTPS Utilizando GSKIT” para obter informações adicionais.

Também será necessário atualizar o arquivo de dados da rede do cliente a fim de especificar os servidores Communications Server para Linux aos quais o cliente poderá se conectar, e o nome do servidor WebSphere que suportará o HTTPS. Consulte a seção sobre como gerenciar o Remote API Clients no *Communications Server for Linux Administration Guide* para obter mais detalhes.

Configurando Certificados de Segurança HTTPS Utilizando GSKIT

Se o cliente se conectar com servidores Communications Server para Linux via HTTPS, o software do gerenciador de chaves GSKIT deve estar instalado. Isso normalmente ocorrerá como parte da instalação do cliente, desde que os pré-requisitos do sistema operacional Linux esteja instalado como descrito no arquivo **LEIA-ME** no CD de instalação. Se o GSKIT não foi instalado como parte da instalação do cliente, mas agora os pré-requisitos estiverem presentes, instale o software do GSKIT utilizando as etapas a seguir, se for o caso.

1. Efetue login em uma sessão com privilégios de root.
2. Monte o CD e altere o diretório para ele.

```
mount /dev/cdrom  
cd /media/cdrom
```

O nome do diretório **/media/cdrom** pode ser diferente se você tiver uma unidade de DVD. Utilize o comando **df** para verificar se o Linux montou o CD.

3. Altere para o subdiretório apropriado no CD e execute o script de shell para instalar o software GSKIT. O exemplo abaixo mostra o diretório **/linux** de um cliente Intel (i686) de 32 bits; substitua-o pelo **/linux-x86_64** ou **/linux-ppc64**, se necessário.

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

Configurando certificados de segurança HTTPS utilizando GSKIT

Antes que o IBM Remote API Client possa se conectar aos servidores via HTTPS, utilize o programa do gerenciador de chaves GSKIT para definir a configuração do certificado de segurança no cliente. Execute as seguintes etapas.

1. Execute o gerenciador de chaves GSKIT, utilizando o comando a seguir:

```
/opt/ibm/sna/bin/snakeyman
```

Dentro da interface do usuário do gerenciador de chaves, abra o arquivo de banco de dados de chaves `/etc/opt/ibm/sna/ibmcs.kdb`, que se encontra no formato CMS.

2. A senha inicial do banco de dados de chaves é `ibmcs`. Antes de configurar os certificados de segurança, você **deve** alterá-la para manter a segurança da configuração. No diálogo para alterar a senha, marque a caixa de opções "Fazer stash da senha para um arquivo?" a fim de garantir que a nova senha seja salva quando o banco de dados de chaves for aberto.
3. Obtenha uma cópia do certificado da Autoridade de Certificação (CA) utilizado para subscrever o certificado de segurança do Web Server, e instale no banco de dados de chaves. Para fazer isso, selecione os Certificados Signatários da interface com o usuário do gerenciador de chaves, e clique em Incluir.
4. Se o servidor WebSphere estiver configurado para solicitar certificados de segurança do cliente, este deverá possuir um certificado emitido por uma CA cujo certificado esteja presente no banco de dados de certificados de segurança do Servidor da Web. Para solicitar um novo certificado:
 - a. Selecione Criar, Novo Pedido de Certificado na interface com o usuário do gerenciador de chaves, e preencha os detalhes solicitados.
 - b. Salve e, em seguida, extraia o certificado para um arquivo, e envie-o para a CA.
 - c. Quando o certificado for emitido, armazene-o no banco de dados do Servidor da Web. Para fazer isso, selecione os Certificados Pessoais da interface com o usuário do gerenciador de chaves, e clique em Receber.Como medida temporária para seu teste interno, é possível criar um certificado cliente auto-assinado em vez de obter um certificado da CA. Contudo, tal certificado não provê o nível de segurança necessário e não deve ser utilizado num sistema de trabalho. Para criar um certificado auto-assinado:
 - a. Selecione Criar, Novo Certificado Auto-assinado, na interface com o usuário do gerenciador de chaves, e preencha os detalhes solicitados.
 - b. Salve e, em seguida, extraia o certificado para um arquivo.
 - c. Armazene o arquivo de certificados no banco de dados do Servidor da Web. Para fazer isso, selecione os Certificados Pessoais da interface com o usuário do gerenciador de chaves, e clique em Receber.
5. Saia do gerenciador de chaves GSKIT ao concluir a configuração dos certificados.

Desinstalando o Remote API Client no Linux

Você pode desinstalar o Remote API Client no Linux utilizando os seguintes comandos.

```
/opt/ibm/sna/bin/sna stop  
rpm -e ibm-commserver-ptf  
rpm -e ibm-commserver-docs  
rpm -e ibm-commserver-ecl  
rpm -e ibm-commserver-cli
```

Desinstalando o Remote API Client no Linux

```
rpm -e ibm-commserver  
rpm -e gsk7bas  
/sbin/shutdown -r now
```

Nem todos os pacotes listados nesses comandos serão instalados em todos os sistemas.

A desinstalação do IBM Remote API Client no Linux ignorará todas as informações de configuração personalizadas a fim de serem utilizadas por uma instalação posterior.

Capítulo 5. Instalando IBM Remote API Clients no Linux para System z

Este capítulo descreve como instalar o IBM Remote API Client no Linux, que permite a um mainframe System z executar aplicativos SNA sem ter uma instalação de pilha SNA completa. Um Remote API Client no Linux para System z pode se conectar a um ou mais servidores Communications Server para Linux (ou servidores CS/AIX) utilizando uma rede TCP/IP.

É recomendado ler o arquivo LEIA-ME do IBM Remote API Client antes de instalar o software. Esse arquivo está localizado no diretório `/ibm-commserver-clients/linux-systemz` do CD de instalação.

Se você estiver fazendo upgrade de uma versão anterior do Communications Server para Linux e Remote API Clients, recomenda-se que faça upgrade de todos os servidores antes de fazer upgrade dos Remote API Clients. Consulte “Migrando de Níveis Anteriores do Communications Server para Linux” na página 29 para obter mais detalhes.

Requisitos de Hardware e Software

Requisitos de Hardware

O IBM Remote API Client requer um sistema System z de 31 ou de 64 bits suportado por uma das distribuições do Linux listadas em “Versão do Sistema Operacional Linux”.

Utilize o comando `uname -m` para verificar a classe da CPU. Ele deve informar `s390` para indicar um ambiente de 31 bits, ou `s390x` para indicar um ambiente de 64 bits.

Versão do Sistema Operacional Linux

A versão atual do IBM Remote API Client foi testada com as seguintes versões do sistema operacional Linux. Também pode executar satisfatoriamente em outras distribuições do Linux.

- RedHat Enterprise Linux 4 para S/390 (RHEL4-s390)
- RedHat Enterprise Linux 4 para zSeries (RHEL4-s390x)
- RedHat Enterprise Linux 5 para System z (RHEL5-s390x)
- SUSE Linux Enterprise Server 9 para IBM Mainframe (SLES9-s390*)
- SUSE Linux Enterprise Server 10 para IBM Mainframe (SLES10-s390x)

Consulte o arquivo **LEIA-ME** no CD de instalação para obter detalhes sobre quais pacotes opcionais podem ser necessários.

Java

Se utilizar a API Java CPI-C, precisará do software Java. Consulte o arquivo **LEIA-ME** no CD de instalação para obter detalhes.

GSKIT

Se o cliente se conectar aos servidores Communications Server para Linux utilizando HTTPS, o software GSKIT será necessário para ativar o acesso HTTPS aos servidores por meio de um servidor WebSphere. O software GSKIT está presente no CD de instalação, mas talvez precise de alguns pacotes opcionais do sistema operacional Linux para instalá-lo; consulte o arquivo **LEIA-ME** no diretório **/ibm-commserver-clients/linux-systemz** do CD de instalação para obter detalhes sobre quais pacotes opcionais podem ser necessários.

Se todos os pacotes de pré-requisitos estiverem instalados ao executar o processo de instalação do cliente, descrito mais tarde neste capítulo, o software GSKIT será automaticamente instalado como parte desse processo. Caso contrário, você pode instalá-lo mais tarde.

Exibindo os Detalhes da Instalação do Produto

É possível exibir informações sobre o Remote API Client e os pacotes de software relacionados já instalados. Para listar todos os pacotes instalados, utilize o seguinte comando:

```
rpm -q -a
```

Para visualizar mais detalhes de um pacote específico, utilize o seguinte comando:

```
rpm -q -i packagename
```

packagename é o nome base do pacote instalado, por exemplo **ibm-commserver-client**.

Definindo a Variável Language Environment

Utilize o comando a seguir para alterar a variável LANG para indicar o idioma a ser utilizado:

```
export LANG=language
```

Substitua *language* pelo identificador do idioma que deseja utilizar, o qual pode ser um dos seguintes:

Identificador	Idioma
en_US	Inglês (Estados Unidos)
ja_JP	Japonês (PC)
de_DE	Alemão
es_ES	Espanhol
fr_FR	Francês
ko_KR	Coreano
pt_BR	Português
zh_CN	Chinês (simplificado)
zh_TW	Chinês (tradicional)

Instalando o Remote API Client no Linux para System z

Depois de instalar o software de pré-requisito, você está pronto para instalar o IBM Remote API Client.

Instalando o Remote API Client no Linux para System z

Se tiver um nível anterior do IBM Remote API Client instalado, siga as etapas na seção “Desinstalando o Remote API Client no Linux para System z” na página 51 para removê-lo antes de instalar esse novo nível. Quaisquer informações de configuração serão mantidas para serem utilizadas pela nova instalação.

1. Copie ou transfira por FTP o arquivo **ibm-commserver-client-6.3.1.0-s390x.tgz** a partir do diretório **/ibm-commserver-clients/linux-systemz** no CD-ROM para o sistema Linux System z. Certifique-se de que está utilizando o modo binário para copiar ou transferir por FTP o arquivo.
2. Efetue login no sistema Linux System z como root.
3. Descompacte o arquivo tar em um diretório temporário vazio:

```
mkdir /tmp/ibmcs
```

```
cd /tmp/ibmcs
```

```
tar —xzf ibm-commserver-client-6.3.1.0-s390x.tgz
```

4. Execute o script do shell **installibmcscli**:

```
./installibmcscli
```

Esse script do shell testará determinados pré-requisitos e enviará mensagens de aviso se eles não forem satisfeitos. Também solicita a confirmação da leitura e aceitação dos termos de licença do Communications Server para Linux. Você pode substituir esse aviso especificando parâmetros adicionais no comando **installibmcscli**, conforme descrito a seguir. Quando você tiver respondido ao aviso, o script do shell instalará os pacotes **rpm**. Se os pré-requisitos apropriados já estiverem presentes, o script instalará o software GSKIT.

5. Inclua os diretórios binários do IBM Remote API Client em PATH. Você pode desejar alterar o seu perfil para fazer isso automaticamente:

```
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
```

Se estiver executando aplicativos de 64 bits, utilize:

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

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

Para aplicativos Java CPI-C, você também deve definir a seguinte variável de ambiente:

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

Para alguns aplicativos, também pode ser necessário definir a variável de ambiente LD_PRELOAD, mas essa não deve ser uma alteração global no perfil:

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

6. Inicie o IBM Remote API Client. Após a instalação, isso acontecerá automaticamente quando a máquina for reinicializada. Certifique-se de não estar nos diretórios do CD ao fazer isso.

```
cd /
```

```
sna start
```

7. Quando tiver concluído a instalação, você poderá apagar o arquivo **tgz** e o diretório temporário que foram criados durante o processo de instalação.

Nota: Antes que o IBM Remote API Client possa se conectar a servidores via HTTPS, utilize o programa do gerenciador de chaves GSKIT para definir a configuração do certificado de segurança no cliente. Consulte “Configurando Certificados de Segurança HTTPS Utilizando GSKIT” na página 50 para obter informações adicionais.

Instalando o Remote API Client no Linux para System z

Também será necessário atualizar o arquivo de dados da rede do cliente a fim de especificar os servidores Communications Server para Linux aos quais o cliente poderá se conectar, e o nome do servidor WebSphere que suportará o HTTPS. Consulte a seção sobre como gerenciar o Remote API Clients no *Communications Server for Linux Administration Guide* para obter mais detalhes.

Configurando Certificados de Segurança HTTPS Utilizando GSKIT

Se o cliente se conectar com servidores Communications Server para Linux via HTTPS, o software do gerenciador de chaves GSKIT deve estar instalado. Isso normalmente ocorrerá como parte da instalação do cliente, desde que os pré-requisitos do sistema operacional Linux esteja instalado como descrito no arquivo **LEIA-ME** no CD de instalação. Se o GSKIT não foi instalado como parte da instalação do cliente, mas agora os pré-requisitos estiverem presentes, instale o software do GSKIT utilizando as etapas a seguir, se for o caso.

1. Copie ou transfira por FTP o arquivo **ibm-commserver-client-6.3.1.0-s390x.tgz** a partir do diretório **/ibm-commserver-clients/linux-systemz** no CD-ROM para o sistema Linux System z. Certifique-se de que está utilizando o modo binário para copiar ou transferir por FTP o arquivo.
2. Efetue login no sistema Linux System z como root.
3. Descompacte o arquivo tar em um diretório temporário vazio:

```
mkdir /tmp/ibmcs  
cd /tmp/ibmcs  
tar -xzf ibm-commserver-client-6.3.1.0-s390x.tgz
```
4. Execute o script do shell **installgskit**:

```
./installgskit
```
5. Quando tiver concluído a instalação, você poderá apagar o arquivo **tgz** e o diretório temporário que foram criados durante o processo de instalação.

Antes que o IBM Remote API Client possa se conectar aos servidores via HTTPS, utilize o programa do gerenciador de chaves GSKIT para definir a configuração do certificado de segurança no cliente. Execute as seguintes etapas.

1. Execute o gerenciador de chaves GSKIT, utilizando o comando a seguir:

```
/opt/ibm/sna/bin/snakeyman
```

Dentro da interface do usuário do gerenciador de chaves, abra o arquivo de banco de dados de chaves **/etc/opt/ibm/sna/ibmcs.kdb**, que se encontra no formato CMS.

2. A senha inicial do banco de dados de chaves é **ibmcs**. Antes de configurar os certificados de segurança, você **deve** alterá-la para manter a segurança da configuração. No diálogo para alterar a senha, marque a caixa de opções "Fazer stash da senha para um arquivo?" a fim de garantir que a nova senha seja salva quando o banco de dados de chaves for aberto.
3. Obtenha uma cópia do certificado da Autoridade de Certificação (CA) utilizado para subscrever o certificado de segurança do Web Server, e instale no banco de dados de chaves. Para fazer isso, selecione os Certificados Signatários da interface com o usuário do gerenciador de chaves, e clique em Incluir.
4. Se o servidor WebSphere estiver configurado para solicitar certificados de segurança do cliente, este deverá possuir um certificado emitido por uma CA cujo certificado esteja presente no banco de dados de certificados de segurança do Servidor da Web. Para solicitar um novo certificado:

Configurando certificados de segurança HTTPS utilizando GSKIT

- a. Selecione Criar, Novo Pedido de Certificado na interface com o usuário do gerenciador de chaves, e preencha os detalhes solicitados.
- b. Salve e, em seguida, extraia o certificado para um arquivo, e envie-o para a CA.
- c. Quando o certificado for emitido, armazene-o no banco de dados do Servidor da Web. Para fazer isso, selecione os Certificados Pessoais da interface com o usuário do gerenciador de chaves, e clique em Receber.

Como medida temporária para seu teste interno, é possível criar um certificado cliente auto-assinado em vez de obter um certificado da CA. Contudo, tal certificado não provê o nível de segurança necessário e não deve ser utilizado num sistema de trabalho. Para criar um certificado auto-assinado:

- a. Selecione Criar, Novo Certificado Auto-assinado, na interface com o usuário do gerenciador de chaves, e preencha os detalhes solicitados.
 - b. Salve e, em seguida, extraia o certificado para um arquivo.
 - c. Armazene o arquivo de certificados no banco de dados do Servidor da Web. Para fazer isso, selecione os Certificados Pessoais da interface com o usuário do gerenciador de chaves, e clique em Receber.
5. Saia do gerenciador de chaves GSKIT ao concluir a configuração dos certificados.

Desinstalando o Remote API Client no Linux para System z

É possível desinstalar o Remote API Client no Linux para System z utilizando os seguintes comandos.

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

Nem todos os pacotes listados nesses comandos serão instalados em todos os sistemas.

A desinstalação do IBM Remote API Client no Linux para System z ignorará todas as informações de configuração customizadas para uso em uma instalação posterior.

Capítulo 6. Instalando IBM Remote API Clients em Sistemas AIX

Este capítulo descreve como instalar o IBM Remote API Client no AIX, permitindo que uma estação de trabalho do AIX execute aplicativos SNA sem ter uma instalação completa da pilha SNA. Um Remote API Client no AIX pode se conectar a um ou mais servidores Communications Server para Linux (ou servidores CS/AIX) utilizando uma rede TCP/IP.

É recomendado ler o arquivo LEIA-ME do IBM Remote API Client antes de instalar o software. Este arquivo está localizado no diretório **/ibm-commserver-clients/aix** no CD de instalação. Se você estiver fazendo upgrade de uma versão anterior do Communications Server para Linux e do Remote API Clients, recomenda-se que faça upgrade de todos os servidores antes de fazer upgrade dos Remote API Clients. Consulte “Migrando de Níveis Anteriores do Communications Server para Linux” na página 29 para obter mais detalhes.

Requisitos de Hardware e Software

Requisitos de Hardware

O IBM Remote API Client requer um sistema pSeries suportado por um dos sistemas operacionais AIX listados em “Versão do Sistema Operacional”.

Versão do Sistema Operacional

A versão atual do IBM Remote API Client foi testada com as seguintes versões do sistema operacional.

- AIX v5.2–ML7 ou posterior
- AIX v5.3–ML3 ou posterior
- AIX 6.1 ou posterior

Java

Se utilizar a API Java CPI-C, precisará do software Java. O mais recente Java SDK disponível em <http://www.ibm.com/developerworks/java/jdk> satisfaz todos os requisitos.

Instale o pacote Java SDK com o comando **installp**.

GSKIT

Se o cliente se conectar aos servidores Communications Server para Linux utilizando HTTPS, o software GSKIT será necessário para ativar o acesso HTTPS aos servidores por meio de um servidor WebSphere. Consulte o arquivo **LEIA-ME**, no diretório **/ibm-commserver-clients/aix** do CD de instalação, para obter mais detalhes. O software GSKIT é instalado como parte do processo de instalação do cliente principal, descrito posteriormente neste capítulo.

Alterando a Variável Language Environment

Quando utilizar o Remote API Client, verifique se a variável LANG não está configurada como C.

Requisitos de Hardware e Software

Utilize o procedimento a seguir para mostrar qual variável LANG está em uso, ou para alterar a variável LANG:

1. No menu principal do SMIT, selecione **Ambientes do Sistema**.
2. No próximo menu do SMIT, selecione **Gerenciar Ambiente de Idioma**.
3. No menu subsequente do SMIT, selecione **Alterar/Mostrar Ambiente de Idioma Primário**.
4. No próximo menu do SMIT, selecione **Alterar/Mostrar Convenção Cultural, Idioma ou Teclado**.
5. Selecione o idioma a ser utilizado. Por exemplo, se utilizar mensagens em inglês americano, selecione `en_US`.

Instalando o Remote API Client no AIX

Depois de instalar o software de pré-requisito, você está pronto para instalar o IBM Remote API Client.

Se tiver um nível anterior do IBM Remote API Client instalado, siga as etapas na seção “Desinstalando o Remote API Client no AIX” na página 56 para removê-lo antes de instalar esse novo nível. Quaisquer informações de configuração serão mantidas para serem utilizadas pela nova instalação.

Instalando o Remote API Client Copiando Arquivos para a sua Estação de Trabalho AIX

Para instalar o Remote API Client, execute as etapas a seguir.

1. Copie ou transfira por FTP o arquivo `sna.client.6.3.1.0.I` a partir do diretório `/ibm-commserver-clients/aix` no CD-ROM para a estação de trabalho AIX. Certifique-se de que está utilizando o modo binário para copiar ou transferir por FTP o arquivo.
Se o cliente se conectar a servidores Communications Server para Linux via HTTPS, copie ou transfira por FTP os arquivos `gskta.*.I` e `gksa.*.I` no mesmo diretório do CD. Esses arquivos contêm o software GSKIT necessário para o acesso HTTPS a partir do cliente.
2. Efetue login na estação de trabalho AIX como root.
3. Instale o Cliente AIX, utilizando o `smit` ou `installp`. Para obter instruções sobre como fazer isso, consulte o arquivo `LEIA-ME` no diretório `/ibm-commserver-clients/aix` do CD de instalação.
4. Se o cliente se conectar a servidores Communications Server para Linux via HTTPS, instale arquivos GSKIT de acordo com as instruções no arquivo `LEIA-ME`.
5. Quando o processo de instalação for concluído, será possível excluir o arquivo `sna.client.6.3.1.0.I` e os arquivos do GSKIT do diretório de trabalho.
6. Inicie o IBM Remote API Client. Após a instalação, isso acontecerá automaticamente quando a máquina for reinicializada.

```
cd /  
sna start
```

Nota: Antes que o IBM Remote API Client possa se conectar a servidores via HTTPS, utilize o programa do gerenciador de chaves GSKIT para definir a configuração do certificado de segurança no cliente. Consulte “Configurando Certificados de Segurança HTTPS Utilizando GSKIT” na página 55 para obter informações adicionais.

Também será necessário atualizar o arquivo de dados da rede do cliente a fim de especificar os servidores Communications Server para Linux aos quais o cliente poderá se conectar, e o nome do servidor WebSphere que suportará o HTTPS. Consulte a seção sobre como gerenciar o Remote API Clients no *Communications Server for Linux Administration Guide* para obter mais detalhes.

Instalando o Remote API Client a partir do CD

Para instalar o Remote API Client, execute as etapas a seguir.

1. Efetue login na estação de trabalho AIX como root.
2. Monte o CD na estação de trabalho AIX, utilizando o seguinte comando:
mount -o ro /dev/cd0 /mnt
3. Instale o Cliente AIX, utilizando o **smit** ou **installp**. Para obter instruções sobre como fazer isso, consulte o arquivo **LEIA-ME** no diretório **/ibm-commserver-clients/aix** do CD de instalação.
4. Se o cliente se conectar a servidores Communications Server para Linux via HTTPS, instale arquivos GSKIT de acordo com as instruções no arquivo **LEIA-ME**.
5. Na conclusão do processo de instalação, desmonte o CD utilizando o seguinte comando.
umount /mnt
6. Inicie o IBM Remote API Client. Após a instalação, isso acontecerá automaticamente quando a máquina for reinicializada. Certifique-se de não estar nos diretórios do CD ao fazer isso.

```
cd /  
sna start
```

Nota: Antes que o IBM Remote API Client possa se conectar a servidores via HTTPS, utilize o programa do gerenciador de chaves GSKIT para definir a configuração do certificado de segurança no cliente. Consulte “Configurando Certificados de Segurança HTTPS Utilizando GSKIT” para obter informações adicionais.

Também será necessário atualizar o arquivo de dados da rede do cliente a fim de especificar os servidores Communications Server para Linux aos quais o cliente poderá se conectar, e o nome do servidor WebSphere que suportará o HTTPS. Consulte a seção sobre como gerenciar o Remote API Clients no *Communications Server for Linux Administration Guide* para obter mais detalhes.

Configurando Certificados de Segurança HTTPS Utilizando GSKIT

Antes que o IBM Remote API Client possa se conectar aos servidores via HTTPS, utilize o programa do gerenciador de chaves GSKIT para definir a configuração do certificado de segurança no cliente. Execute as seguintes etapas.

1. Execute o gerenciador de chaves GSKIT, utilizando o comando a seguir:

```
/usr/bin/snakeyman
```

Dentro da interface do usuário do gerenciador de chaves, abra o arquivo de banco de dados de chaves **/etc/sna/ibmcs.kdb**, que se encontra no formato CMS.

Configurando certificados de segurança HTTPS utilizando GSKIT

2. A senha inicial do banco de dados de chaves é `ibmcs`. Antes de configurar os certificados de segurança, você **deve** alterá-la para manter a segurança da configuração. No diálogo para alterar a senha, marque a caixa de opções "Fazer stash da senha para um arquivo?" a fim de garantir que a nova senha seja salva quando o banco de dados de chaves for aberto.
3. Obtenha uma cópia do certificado da Autoridade de Certificação (CA) utilizado para subscrever o certificado de segurança do Web Server, e instale no banco de dados de chaves. Para fazer isso, selecione os Certificados Signatários da interface com o usuário do gerenciador de chaves, e clique em Incluir.
4. Se o servidor WebSphere estiver configurado para solicitar certificados de segurança do cliente, este deverá possuir um certificado emitido por uma CA cujo certificado esteja presente no banco de dados de certificados de segurança do Servidor da Web. Para solicitar um novo certificado:
 - a. Selecione Criar, Novo Pedido de Certificado na interface com o usuário do gerenciador de chaves, e preencha os detalhes solicitados.
 - b. Salve e, em seguida, extraia o certificado para um arquivo, e envie-o para a CA.
 - c. Quando o certificado for emitido, armazene-o no banco de dados do Servidor da Web. Para fazer isso, selecione os Certificados Pessoais da interface com o usuário do gerenciador de chaves, e clique em Receber.Como medida temporária para seu teste interno, é possível criar um certificado cliente auto-assinado em vez de obter um certificado da CA. Contudo, tal certificado não provê o nível de segurança necessário e não deve ser utilizado num sistema de trabalho. Para criar um certificado auto-assinado:
 - a. Selecione Criar, Novo Certificado Auto-assinado, na interface com o usuário do gerenciador de chaves, e preencha os detalhes solicitados.
 - b. Salve e, em seguida, extraia o certificado para um arquivo.
 - c. Armazene o arquivo de certificados no banco de dados do Servidor da Web. Para fazer isso, selecione os Certificados Pessoais da interface com o usuário do gerenciador de chaves, e clique em Receber.
5. Saia do gerenciador de chaves GSKIT ao concluir a configuração dos certificados.

Desinstalando o Remote API Client no AIX

Você pode desinstalar o Remote API Client utilizando os seguintes comandos:

1. Pare o software do cliente se estiver em execução, utilizando o comando a seguir.
sna stop
2. Efetue login em uma sessão com privilégios de root.
3. Remova os pacotes do Remote API Client e dos softwares associados utilizando um dos seguintes comandos.

Para remover o pacote utilizando o **installp**:

installp -u sna.client

Para remover o pacote utilizando o **smit**:

smit remove

Capítulo 7. Planejando e Instalando o Remote API Client no Windows

Este capítulo descreve como instalar o IBM Remote API Client no Windows, permitindo que um PC execute aplicativos SNA mesmo que não possua uma instalação completa da pilha SNA. Um Remote API Client no Windows pode se conectar a um ou mais servidores Communications Server para Linux (ou servidores CS/AIX) utilizando uma rede TCP/IP.

Se você estiver fazendo upgrade de uma versão anterior do Communications Server para Linux e Remote API Clients, recomenda-se que faça upgrade de todos os servidores antes de fazer upgrade dos Remote API Clients. Consulte “Migrando de Níveis Anteriores do Communications Server para Linux” na página 29 para obter mais detalhes.

Há duas variantes do IBM Remote API Client no Windows, dependendo do hardware específico e da versão do Windows que está sendo utilizada. As informações nesse capítulo aplicam-se a ambas variantes, exceto quando as diferenças são claramente observados.

- O cliente de 32 bits é executado em um computador baseado em Intel de 32 bits executando o Microsoft Windows 2000, 2003, XP ou Vista de 32 bits.
- O cliente x64 é executado em um computador AMD64 ou Intel EM64T executando o Microsoft Windows Server 2003 x64 Edition, Microsoft Windows XP Professional x64 Edition ou Microsoft Windows Vista de 64 bits.

As interfaces fornecidas pelo IBM Remote API Client no Windows são amplamente compatíveis com as fornecidas pelos produtos IBM Communications Server para Windows e Microsoft Host Integration Server.

O IBM Remote API Client no Windows Software Development Kit (SDK) é um pacote opcional que permite utilizar o Remote API Client para desenvolver programas de aplicativos utilizando APIs APPC, CPI-C, LUA e CSV. Consulte o guia de referência apropriado do programador para obter mais informações sobre essas APIs. Não será necessário instalar esse pacote se o Remote API Client for utilizado somente para executar aplicativos existentes (não para desenvolver novos).

Requisitos de Hardware e Software

Para executar o programa de **Instalação** e o Remote API Client no Windows, o computador deve satisfazer os seguintes requisitos:

- Deve estar executando um dos seguintes sistemas operacionais:
 - Para o cliente Windows de 32 bits:
 - Windows 2000
 - Windows XP
 - Windows 2003
 - Windows Vista de 32 bits
 - Para o cliente Windows x64:
 - Microsoft Windows XP Professional x64 Edition
 - Microsoft Windows Server 2003 x64 Edition

Requisitos de Hardware e Software

- Windows Vista de 64 bits
- É necessário ter acesso a um ou mais servidores Communications Server para Linux, utilizando um dos seguintes mecanismos:
 - Acesso ao servidor por uma rede TCP/IP
 - Acesso a um servidor WebSphere que fornece acesso HTTPS aos servidores Communications Server para Linux.

Nota: Dependendo da versão do Windows utilizada, pode haver alguma configuração adicional que você precisa executar antes de poder instalar e utilizar o Remote API Client no Windows. Consulte as informações do cliente Windows no arquivo **LEIA-ME** no CD de instalação para obter detalhes adicionais.

Acessando o Programa de Instalação

O Remote API Client, o software SDK, o software GSKIT e o programa de **Instalação** estão presentes no CD de instalação, no formato do Windows, e, portanto, podem ser instalados a partir do CD no computador Windows. Você deve instalar o software Remote API Client em cada PC com cliente Windows; isso também instalará o software GSKIT automaticamente. O SDK só será preciso se você utilizar o cliente para desenvolver novos aplicativos utilizando as APIs Remotas do Windows; e ele não será necessário caso seja utilizado apenas para executar os aplicativos existentes.

A imagem de instalação do Remote API Client no Windows é um arquivo ZIP executável, presente no CD de instalação.

- No caso do cliente de 32 bits, é o arquivo **i_w32cli.exe** no diretório **/ibm-commserver-clients/windows** do CD.
- No caso do cliente x64, é o arquivo **i_w64cli.exe** no diretório **/ibm-commserver-clients/win-x64** do CD.

É possível copiar esse arquivo para outros PCs Windows no âmbito da rede, de modo que seja possível instalá-los sem acesso direto no CD de remessa do Communications Server para Linux. Ao executar esse executável, ele descompacta a imagem de instalação e inicia automaticamente o programa de **Instalação**. A fim de descompactar simplesmente a imagem de instalação para um diretório temporário, por exemplo, para executar o programa de **Instalação** a partir da linha de comandos, carregue o executável ZIP de auto-extração no seu programa de descompactação.

A primeira vez que executar o programa de **Instalação** em um computador específico, ele será executado a partir da origem selecionada. O programa executa o processo de instalação completo, define uma configuração básica e, além disso, instala e cria um ícone para si próprio. Após a conclusão da instalação, utilize o programa de **Instalação** (selecionando-o no Gerenciador de Arquivos ou clicando em seu ícone) se precisar reinstalar o software.

Depois de extrair a imagem de instalação do Remote API Client num diretório temporário, será possível instalar o software em um dos seguintes dois modos:

- Execute o programa de **Instalação** pelo Windows, conforme explicado em “Instalando o Remote API Client no Windows Utilizando o Programa de Instalação” na página 59. Utilize esse método para instalar o SDK.

- Digite o comando **setup** na linha de comandos, conforme explicado em “Instalando o Software Remote API Client a partir da Linha de Comandos” na página 63. Esse método não permite instalar o SDK.

Nota: Antes que o IBM Remote API Client possa se conectar aos servidores utilizando HTTPS, é necessário atualizar o arquivo de dados de rede do cliente para especificar os servidores Communications Server para Linux aos quais o cliente pode se conectar e o nome do servidor WebSphere que fornece suporte HTTPS. Consulte a seção sobre como gerenciar os Remote API Clients no *Communications Server para Linux: Guia de Administração* para obter detalhes adicionais.

Instalando o Remote API Client no Windows Utilizando o Programa de Instalação

Execute o programa de **instalação**, automaticamente como parte da execução do arquivo ZIP executável de auto-extração **i_w32cli.exe** (cliente de 32 bits) ou **i_w64cli.exe** (cliente x64), ou manualmente na linha de comandos. Inicialmente, o programa exibe a tela Escolher Idioma da Instalação.

1. Selecione o idioma a ser utilizado para instalar e configurar o Remote API Client, e clique em **OK**.

O programa exibe uma tela Bem-vindo que apresenta o programa de **Instalação**.

2. Escolha **Avançar** para continuar com a instalação.

O programa exibe o Software Licensing Agreement, o qual você deve ler e entender.

3. Se estiver de acordo com os termos da licença, escolha **Aceitar** para continuar.

O programa solicita que você especifique um diretório de destino em que os arquivos devem ser instalados.

4. Digite o diretório de destino.

O programa solicita que você escolha o tipo de instalação desejado:

Padrão

Escolha essa opção se não for necessário instalar o SDK. O SDK só será preciso se você utilizar o cliente para desenvolver novos aplicativos utilizando as APIs Remotas do Windows; e ele não será necessário caso seja utilizado apenas para executar os aplicativos existentes.

Desenvolvedor

Selecione essa opção para instalar o SDK: ou seja, se for necessário utilizar o cliente para desenvolver novos aplicativos que utilizam APIs Remotas do Windows.

Nota: Para instalar o SDK, escolha **Desenvolvedor**.

5. Escolha o tipo de instalação.

Nessa altura, o programa solicita a inserção do nome da pasta de programas no qual os ícones do Remote API Client no Windows devem figurar.

6. Digite o nome da pasta.

7. Se o diretório System já contiver arquivos **.DLL** com nomes idênticos aos utilizados pelo programa de **Instalação** que não sejam arquivos do Remote API Client (por exemplo, que pertençam a algum outro software SNA), o programa o instruirá a executar uma das seguintes opções:

Instalando o Remote API Client no Windows Utilizando o Programa de Instalação

- Copiar os arquivos **.DLL** do Remote API Client, sobrescrevendo os arquivos **.DLL** existentes
- Copiar os arquivos **.DLL** existentes para um subdiretório com o nome **OTHERSNA** do diretório de instalação e instalar os arquivos **.DLL** do Remote API Client. Essa opção permite restaurar a configuração original anterior à instalação do Remote API Client, se desinstalar os arquivos posteriormente (consulte “Desinstalando o Software Remote API Client” na página 67).
- Cancele a instalação do software do cliente.

Se os arquivos **.DLL** do Remote API Client já estiverem presentes, o programa de **Instalação** exibirá uma mensagem indicando isso. Novos arquivos **.DLL** sobrescreverão os arquivos **.DLL** existentes somente se estes tiverem números de versão inferiores aos arquivos **.DLL** do programa de **Instalação**.

8. Neste ponto, o programa de **Instalação** copia arquivos da origem especificada e instala-os nos locais apropriados. Durante este processo, uma barra de informações exibe que parte da instalação está concluída. Os arquivos **.DLL** são copiados para o diretório System ou equivalente e os outros arquivos são copiados para o diretório de destino especificado na Etapa 2. Durante cada operação de transferência de arquivos, um registro é gravado no arquivo **setup.log**, que é criado no diretório especificado. Se qualquer um dos arquivos a ser gravado for “somente leitura” ou se algum arquivo não puder ser copiado por algum outro motivo, os novos arquivos serão removidos e você receberá uma mensagem aconselhando-o a verificar o arquivo **setup.log**.
9. Se a origem a partir da qual está executando o programa de **Instalação** não contiver todos os arquivos necessários, o programa solicitará que forneça um nome de diretório. Digite o nome de um diretório no qual os arquivos necessários estão localizados.

Se as informações especificadas não forem suficientes para localizar as cópias dos arquivos do Remote API Client, o programa exibirá essa tela novamente.

10. Quando os arquivos necessários tiverem sido copiados, o programa de **Instalação** exibirá a janela Configuração.

Os valores de configuração padrão são obtidos do arquivo de configuração de domínio. Para obter informações adicionais, consulte *Communications Server for Linux Administration Guide*. Se você não desejar utilizar esses valores padrão, poderá configurá-los conforme mostrado a seguir:

Domínio

Especifique o nome do domínio cliente/servidor do Communications Server para Linux.

Se o cliente utilizar o endereçamento IPv6, será necessário configurar as seguintes configurações. Elas são opcionais, se o cliente utilizar o endereçamento IPv4.

Nome do Servidor

A tela mostra uma lista de até nove servidores aos quais este cliente pode ser conectado. A ordem em que os servidores aparecem nessa lista é a ordem em que o cliente seleciona esses servidores. Se o cliente não puder ser conectado ao primeiro servidor na lista, será feita uma tentativa com o próximo servidor.

Se o cliente utilizar o endereçamento IPv6, será necessário configurar pelo menos um servidor. Se o cliente utilizar o endereçamento IPv4, não será necessário especificar qualquer servidor se você utilizar a

Instalando o Remote API Client no Windows Utilizando o Programa de Instalação

opção *difusões UDP*; se você especificar um ou mais servidores, por sua vez, o cliente os tentará, se ele não puder contatar um servidor utilizando as difusões UDP.

- Para incluir um novo servidor na lista, utilize o botão **Incluir**.
- Para remover um servidor da lista, selecione-o e utilize o botão **Remover**.
- Para mover um servidor para cima ou para baixo na lista, selecione o servidor e utilize os botões deslizantes da lateral da lista.

Se o cliente estiver na mesma rede privada que os servidores e acessá-los via TCP/IP, cada servidor será identificado simplesmente pelo nome do servidor.

Se o cliente utilizar HTTPS para acessar os servidores, identifique cada um deles especificando o nome do servidor WebSphere que fornece suporte para HTTPS e o nome do servidor Communications Server para Linux, no seguinte formato:

```
webservername : servername1
```

Esse parte da premissa que o WebSphere está configurado para utilizar a porta 443, a porta padrão para conexões HTTPS. Se o administrador da rede configurou o WebSphere para utilizar um número de porta diferente, inclua o número da porta no seguinte formato:

```
webservername : portnumber : servername1
```

Para obter mais detalhes sobre como configurar o WebSphere para dar suporte a conexões do HTTPS, consulte “Configurando o WebSphere Application Server” na página 34.

Difusões UDP

Especifique se este cliente utilizará difusões UDP para ser conectado a um servidor. Quando essa opção estiver selecionada, o cliente enviará difusões UDP na rede para localizar uma conexão de servidor, em vez de tentar se conectar diretamente a um servidor específico.

A configuração padrão é utilizar difusões UDP. Para alterar esta configuração, clique na caixa.

Se o cliente utilizar o endereçamento IPv6, as difusões UDP não serão suportadas. Desative a opção para utilizar as difusões UDP e especifique pelo menos um *Nome do Servidor*.

As seguintes configurações são opcionais:

Avançado

Para fornecer valores adicionais, em vez dos valores padrão fornecidos pelo programa de **Instalação**, clique no botão **Avançado** na parte inferior da janela. O programa de **Instalação** exibe a janela Opções Avançadas, que contém definições avançadas para a configuração de cliente Windows. A maioria dos usuários pode utilizar as definições padrão para estes parâmetros, portanto você provavelmente não precise alterar as definições na caixa de diálogo.

Para obter mais informações sobre estes parâmetros, consulte “Opções Avançadas da Configuração do Remote API Client” na página 62.

Para obter mais informações sobre qualquer um dos parâmetros (ou definições) de configuração, clique em **Ajuda**.

Instalando o Remote API Client no Windows Utilizando o Programa de Instalação

11. Quando você tiver completado a janela Configuração, clique em **OK**. O programa de **Configuração** exibe uma mensagem se você não completou essa tela de maneira adequada.
12. Quando a instalação tiver sido concluída com êxito, a janela Concluir será exibida. Você pode selecionar uma ou as duas ações a seguir para serem executadas depois que sair do programa de instalação:

Visualizar o arquivo LEIA-ME

Visualize o arquivo **LEIA-ME**.

Iniciar cliente

Inicie a execução desse cliente do Communications Server para Linux. Escolha **Concluir** para sair do programa de instalação.

Opções Avançadas da Configuração do Remote API Client

A janela Opções Avançadas permite configurar alguns parâmetros avançados do Remote API Client. A maioria dos usuários não precisa alterar esses parâmetros, mas podem ajustar as definições padrão, se necessário.

Tempo limite de acesso à LAN

Especifique o tempo em segundos em que a conexão do cliente a um servidor poderá ficar inativa antes de ser fechada. Quando essa caixa de opções está vazia, nenhum tempo limite de acesso à rede local foi especificado (e, dessa forma, um tempo limite infinito será utilizado). Se você marcar essa caixa, poderá digitar um valor de tempo limite em segundos no campo adjacente. O valor mínimo é 60 (para 60 segundos); se você deixar a caixa vazia ou especificar um valor inferior a 60, o Remote API Client assumirá o valor mínimo igual a 60.

Número Máx. de tentativas de difusão

Especifique o número máximo de vezes que o cliente tenta se conectar a um servidor por difusão. Quando a janela Opções Avançadas é aberta, o valor padrão 5 é exibido. O valor nessa caixa será utilizado somente se a caixa de opções Difusões UDP estiver marcada na janela Configuração principal.

Tempo limite para Reconectar

Especifique o tempo, em segundos, que o cliente aguarda antes de tentar reconectar a um servidor depois que o servidor parou de funcionar. Quando a janela Opções Avançadas está aberta, o valor padrão 200 é exibido.

Para obter mais informações sobre estes parâmetros, pressione **Ajuda**.

Quando você tiver completado a janela Opções Avançadas, clique em **OK**. Se tiver completado a janela corretamente, o programa de **Configuração** retornará para a janela Configuração. Se estiver instalando um novo Remote API Client, retorne à Etapa 11. Do contrário, clique no botão **OK** na caixa de diálogo Configuração para concluir a configuração.

Instalando o Software Remote API Client a partir da Linha de Comandos

Nota: Para instalar o SDK, utilize o programa de **Instalação**, conforme descrito em “Instalando o Remote API Client no Windows Utilizando o Programa de Instalação” na página 59. Não é possível instalar o SDK a partir da linha de comandos.

Depois de extrair a imagem de instalação do Remote API Client para um diretório temporário, será possível instalar o software Remote API Client a partir da linha de comandos em vez de utilizar o programa de **Instalação** para Windows. Na linha de comandos, digite o comando **setup** com uma ou mais opções. Essas opções podem ser digitadas em maiúscula ou minúscula e podem ser precedidas por uma / (barra) ou um - (hífen). Se um parâmetro, como *folder*, for uma cadeia que contém um espaço, você deverá colocar a cadeia entre aspas duplas.

Após a digitação do comando **setup**, o programa de **Configuração** solicitará que você forneça qualquer informação que não tenha incluído na linha de comandos, e exibe mensagens de confirmação em vários estágios da configuração. Se não desejar que o programa de **Configuração** avise você, utilize a opção **-accept -s** para executar o programa em modo silencioso, aceitando os termos do Software License Agreement.

As opções do comando **setup** são descritas a seguir:

-? Exibe uma lista das opções da linha de comandos. É igual à opção **-h**.

-h Exibe uma lista das opções da linha de comandos. É igual à opção **-?**.

-accept -s

Executa a instalação em modo silencioso, aceitando os termos do Software License Agreement. Esse acordo pode ser encontrado no subdiretório **license** da imagem de instalação do Windows.

A opção **-s** deve ser a última na linha de comandos e você deve ter certeza de que tenha especificado o nome do domínio (utilizando a opção **-i**) e qualquer outro parâmetro que deseja especificar. Quando a instalação é executada em modo silencioso, ela não solicita que você especifique quaisquer parâmetros ou mensagens de confirmação da exibição. Todos os argumentos da linha de comandos após **-s** são ignorados.

-f2 Especifique o nome de caminho completo do arquivo de log de instalação criado durante a instalação do modo silencioso (utilizando a opção **-s**).

Se você não especificar esta opção, o arquivo será criado como **setup.log** no diretório a partir do qual executa o programa de instalação. Se estiver instalando em modo silencioso a partir da unidade de CD, você deverá especificar essa opção para garantir que o arquivo esteja criado em seu computador (porque ele não pode ser criado na unidade de CD).

-kfolder

Especifique a pasta Program.

-pdirectory

Especifique o diretório de instalação.

-idomain

Especifique um nome de domínio para este cliente. Este parâmetro é requerido; não há valor padrão.

Instalando o Software Remote API Client a partir da Linha de Comandos

-wdirectory

Especifique o diretório de origem que contém os arquivos do software cliente do Communications Server para Linux se a origem estiver localizada num disco ou CD. Do contrário, utilize a opção *-v*.

-vserver

Especifique o servidor a partir do qual os arquivos de software do cliente devem ser transferidos por download. Você pode especificar o nome do servidor ou o endereço TCP/IP. Se você estiver copiando os arquivos de origem de um disco ou CD, utilize a opção *-w*, em vez da opção *-v*.

-lserver

Especifique um servidor a ser incluído na lista de servidores que um cliente pode acessar.

Se o cliente estiver na mesma rede privada que os servidores e acessá-los via TCP/IP, cada servidor será identificado simplesmente pelo nome do servidor.

Se o cliente utilizar HTTPS para acessar os servidores, identifique cada um deles especificando o nome do servidor WebSphere que fornece suporte para HTTPS e o nome do servidor Communications Server para Linux, no seguinte formato:

webservername : servername1

Esse parte da premissa que o WebSphere está configurado para utilizar a porta 443, a porta padrão para conexões HTTPS. Se o administrador da rede configurou o WebSphere para utilizar um número de porta diferente, inclua o número da porta no seguinte formato:

webservername : portnumber : servername1

Para obter mais detalhes sobre como configurar o WebSphere para dar suporte a conexões do HTTPS, consulte "Configurando o WebSphere Application Server" na página 34.

-o Sobrescreva os arquivos **.DLL** existentes. Se os arquivos **.DLL** do Remote API Client já estiverem presentes, eles serão sobrescritos pelo programa de **Instalação**, mesmo se tiverem um número de versão mas elevado do que o número de versão dos arquivos **.DLL** do programa de **Instalação**.

-y Salve os arquivos **.DLL** existentes. Se os arquivos **.DLL** do Remote API Client já existirem nos diretórios requeridos, o programa de **Instalação** copiará os arquivos **.DLL** existentes para um subdiretório do diretório de instalação e instalará os arquivos **.DLL** do Remote API Client. As cópias no subdiretório asseguram que, se o software Remote API Client for desinstalado, o processo de desinstalação será concluído.

-n Cancele a instalação se encontrar arquivos **.DLL** existentes do Remote API Client.

-atimeout

Especifique o tempo limite de acesso à rede local em segundos. Esse é o intervalo de tempo da conexão do cliente em que um servidor pode ficar inativo antes de ser fechado. O valor 0 indica nenhum tempo limite.

-bmax-broadcast

Especifique o número máximo de tentativas de difusão UDP. Uma difusão UDP é uma tentativa do cliente de se conectar a qualquer servidor no domínio, em vez de a um servidor específico. O valor 0 indica que nenhuma tentativa de difusão foi feita.

Instalando o Software Remote API Client a partir da Linha de Comandos

`-jreconnect-timeout`

Especifique o tempo, em segundos, que o cliente aguarda antes de tentar reconectar a um servidor depois que o servidor parou de funcionar.

Configurando Certificados de Segurança HTTPS Utilizando GSKIT

Antes que o IBM Remote API Client possa se conectar aos servidores via HTTPS, utilize o programa do gerenciador de chaves GSKIT para definir a configuração do certificado de segurança no cliente. Execute as seguintes etapas.

1. Execute o programa do gerenciador de chaves GSKIT, `installdir\snakeyman.exe`. `installdir` representa o diretório no qual você instalou o software cliente, que é `C:\IBMCS\w32cli` (cliente de 32 bits) ou `C:\IBMCS\w64cli` (cliente de 64 bits), a menos que tenha especificado um local diferente durante a instalação do cliente.

Na interface com o usuário do gerenciador de chaves, abra o arquivo do banco de dados de chaves `installdir\ibmcs.kdb`, que está no formato CMS.

2. A senha inicial do banco de dados de chaves é `ibmcs`. Antes de configurar os certificados de segurança, você **deve** alterá-la para manter a segurança da configuração. No diálogo para alterar a senha, marque a caixa de opções "Fazer stash da senha para um arquivo?" a fim de garantir que a nova senha seja salva quando o banco de dados de chaves for aberto.
3. Obtenha uma cópia do certificado da Autoridade de Certificação (CA) utilizado para subscrever o certificado de segurança do Web Server, e instale no banco de dados de chaves. Para fazer isso, selecione os Certificados Signatários da interface com o usuário do gerenciador de chaves, e clique em Incluir.
4. Se o servidor WebSphere estiver configurado para solicitar certificados de segurança do cliente, este deverá possuir um certificado emitido por uma CA cujo certificado esteja presente no banco de dados de certificados de segurança do Servidor da Web. Para solicitar um novo certificado:
 - a. Selecione Criar, Novo Pedido de Certificado na interface com o usuário do gerenciador de chaves, e preencha os detalhes solicitados.
 - b. Salve e, em seguida, extraia o certificado para um arquivo, e envie-o para a CA.
 - c. Quando o certificado for emitido, armazene-o no banco de dados do Servidor da Web. Para fazer isso, selecione os Certificados Pessoais da interface com o usuário do gerenciador de chaves, e clique em Receber.

Como medida temporária para seu teste interno, é possível criar um certificado cliente auto-assinado em vez de obter um certificado da CA. Contudo, tal certificado não provê o nível de segurança necessário e não deve ser utilizado num sistema de trabalho. Para criar um certificado auto-assinado:

- a. Selecione Criar, Novo Certificado Auto-assinado, na interface com o usuário do gerenciador de chaves, e preencha os detalhes solicitados.
 - b. Salve e, em seguida, extraia o certificado para um arquivo.
 - c. Armazene o arquivo de certificados no banco de dados do Servidor da Web. Para fazer isso, selecione os Certificados Pessoais da interface com o usuário do gerenciador de chaves, e clique em Receber.
5. Saia do gerenciador de chaves GSKIT ao concluir a configuração dos certificados.

Personalizando o Software Remote API Client Depois da Instalação

Você pode alterar quaisquer definições personalizadas a qualquer momento após a instalação inicial, executando o programa **Configuration Utility**, localizado no grupo de programas do Communications Server para Linux. O programa exibe a mesma janela Configuração exibida no processo de instalação inicial. Você pode alterar as informações em qualquer campo, seguindo o procedimento em “Instalando o Remote API Client no Windows Utilizando o Programa de Instalação” na página 59.

Se você não instalou os arquivos do SDK durante a instalação inicial e quiser incluí-los agora, execute o programa de Instalação novamente e escolha **Desenvolvedor** para o tipo de instalação.

Reinstalando o Software Remote API Client

É possível reinstalar o software Remote API Client em qualquer momento, por exemplo, para fazer upgrade do software.

Para fazer isso, execute o programa de Instalação como antes, utilizando as instruções fornecidas em “Instalando o Remote API Client no Windows Utilizando o Programa de Instalação” na página 59 ou “Instalando o Software Remote API Client a partir da Linha de Comandos” na página 63. O programa de **Instalação** exibe o local do qual os arquivos do software do cliente foram copiados durante a instalação inicial. Clique em **OK** para obter novas cópias dos arquivos desse mesmo local. Ao clicar em **OK**, o programa de **Instalação** copiará os arquivos e retornará para a tela Opções.

Nota: Se estiver reinstalando o software Remote API Client no modo silencioso (conforme descrito em “Instalando o Software Remote API Client a partir da Linha de Comandos” na página 63), poderá reiniciar o computador para concluir a instalação. Isso pode ser preciso se alguns arquivos do programa estiverem em uso durante o processo de instalação (por exemplo, se o Remote API Client estiver em execução) e, portanto, não puderem ser substituídos pelos arquivos novos. Nesse caso, os novos arquivos são copiados para um diretório temporário e serão movidos automaticamente para o local apropriado a próxima vez que o computador for reiniciado.

Para verificar se é necessário reiniciar o computador, utilize um editor de texto, como o **Bloco de notas**, para visualizar o conteúdo do arquivo de log de instalação quando o processo de instalação for concluído. O arquivo de log de instalação é chamado **setup.log** e é criado no diretório a partir do qual você executa o programa de Instalação, a menos que você utilize a opção de linha de comandos **-f2** para especificar um caminho e um nome de arquivo diferentes.

No final do arquivo, sob o título **Response Result**, o texto **Result Code** deve ser seguido por um dos dois valores 0 (zero) ou -12. Se o valor for 0, não há necessidade de reiniciar o computador. Se o valor for -12, reinicie o computador antes de tentar utilizar o Cliente Windows.

Desinstalando o Software Remote API Client

Você pode desinstalar o software Remote API Client a qualquer momento, utilizando a opção **Incluir/Remover Programas** do Painel de Controle do Windows. Depois que o processo de desinstalação é confirmado, o Windows faz o seguinte:

- Exclui todos os arquivos instalados.
- Se quaisquer arquivos **.DLL** foram salvos em um subdiretório durante a instalação inicial, restaura os arquivos para seus locais originais.
- Exclui o subdiretório no qual os arquivos **.DLL** salvos foram armazenados, contanto que o subdiretório esteja vazio.
- Remove a pasta Program e o diretório criado, se estiverem vazios.
- Se a desinstalação for bem-sucedida, exclui o arquivo **setup.log**, o qual contém todas as transferências e exclusões de arquivos.
- Exibe uma mensagem informando que a desinstalação foi bem-sucedida ou que o usuário deve verificar o arquivo **setup.log**, pois houve falha em alguma parte da instalação.

O botão **Sair** retorna ao Windows.

Ajuda

Você pode acessar a Ajuda a qualquer momento, pressionando a tecla **F1**. As janelas Configuração e Opções Avançadas também têm botões **Ajuda**.

Capítulo 8. Configurando e Utilizando o Communications Server para Linux

O modo mais fácil de definir e modificar a configuração do Communications Server para Linux é utilizar o programa de administração Motif (`xsnaadmin`). Esse programa fornece uma interface gráfica com o usuário a partir da qual você pode visualizar e gerenciar recursos do SNA no nó local. Você também pode utilizar outras ferramentas de administração, como a administração da linha de comandos, mas o programa Motif é o mais recomendado.

O programa de administração Motif inclui telas de ajuda que fornecem informações gerais para o SNA e o Communications Server para Linux, informações de referência para diálogos do Communications Server para Linux e orientação para executar tarefas específicas. Em cada tarefa (por exemplo, configurar o nó) ou tipo de comunicação (por exemplo, TN3270 ou APPC), o programa fornece orientações sobre como configurar os recursos obrigatórios.

O programa de administração Motif permite configurar todos os parâmetros obrigatórios para configurações padrão do Communications Server para Linux. Em relação aos parâmetros avançados, o Motif fornece os valores padrão. Você precisa fornecer somente as informações essenciais da configuração, que permitem instalar a comunicação do SNA de modo rápido e fácil.

Também é possível utilizar o programa de administração Motif para gerenciar o sistema Communications Server para Linux em execução. O programa de administração permite fazer e aplicar alterações na configuração enquanto o Communications Server para Linux está ativo e fornece acesso fácil às informações de status dos recursos do nó.

O programa de administração Motif exibe automaticamente as informações de status para recursos do Communications Server para Linux. A maior parte dessas informações é mostrada na janela Nó (consulte “Gerenciando o Communications Server para Linux com o Programa de Administração Motif” na página 72). Além disso, você pode controlar determinados recursos—como nós e estações de link—usando os botões **Iniciar** e **Parar** na janela Nó. Outros recursos são sempre iniciados e parados de forma automática; portanto, não há necessidade de controlá-los manualmente.

Nota:

1. Você deve ser um membro do grupo de login `sna` para definir ou modificar recursos do Communications Server para Linux.
2. Para utilizar o programa de administração Motif, você deve ter um X-terminal.
3. Para obter informações adicionais sobre a interface com o usuário do programa de administração Motif, incluindo os botões e ícones que aparecem em suas janelas, consulte as telas de ajuda do programa ou o *Communications Server for Linux Administration Guide*.
4. As janelas e diálogos no programa de administração Motif podem diferenciar daquelas mostradas neste manual, dependendo das opções que você fez em um determinado diálogo.

Configurando e Utilizando o Communications Server para Linux

Para obter informações sobre outras ferramentas de administração do Communications Server para Linux, incluindo a administração da linha de comandos e programas aplicativos NOF, consulte *Communications Server for Linux Administration Guide*, *Communications Server Linux Administration Command Reference* ou *Communications Server for Linux NOF Programmer's Guide*.

Planejando a Configuração do Communications Server para Linux

Antes de fazer alterações na configuração é muito importante planejá-las completamente. As alterações feitas podem causar interrupção, não somente para os usuários do nó local, mas possivelmente para os usuários de toda a rede.

Talvez você ache útil desenhar um diagrama das alterações que está fazendo na topologia da rede. Caso esteja incluindo ou removendo conexões a outros nós, desenhe uma figura mostrando seu nó e os demais. Você pode usar o Motif para coletar informações de configuração sobre todas as conexões existentes e incluir essas informações no seu diagrama.

Quando você inclui novos recursos no diagrama, é fácil ver se estão duplicados ou se existe algum conflito de nomes. Da mesma forma, o diagrama pode ajudá-lo a optar pelos recursos que devem ser removidos e ajuda você a evitar a eliminação dos essenciais.

Se estiver configurando um sistema Communications Server para Linux cliente/servidor com mais de um nó, certifique-se de incluir todos os nós Communications Server para Linux e seus recursos de conectividade no diagrama. Em seguida, você pode configurar cada nó sucessivamente, conforme descrito neste capítulo, da mesma maneira que configuraria um nó independente.

Depois que você determinar as alterações que deseja fazer, colete as informações de configuração necessárias. Para obter orientação durante a coleta de informações de configuração para funções específicas do Communications Server para Linux, utilize as planilhas de tarefas fornecidas na ajuda on-line do programa de administração Motif ou as planilhas de planejamento fornecidas no *Communications Server for Linux Administration Guide*.

Este capítulo fornece instruções para configurar as funções mais frequentemente utilizadas, disponíveis no Communications Server para Linux. Para cada tarefa de configuração, este manual também relaciona as informações que você precisa coletar antes de configurar o recurso.

Nota: Este guia não fornece descrições detalhadas sobre as informações de configuração a serem digitadas nos diálogos do Communications Server para Linux. Para obter mais informações sobre os campos de um determinado diálogo, consulte a ajuda on-line do diálogo no programa de administração Motif.

Planilhas de Planejamento

Antes de iniciar a configuração dos recursos do Communications Server para Linux, reúna todos os dados de configuração dos novos recursos. Para registrar todas as informações de uma determinada função ou aplicativo a qual necessite suprir suporte, utilize as planilhas de planejamento fornecidas no *Communications Server for Linux Administration Guide*.

Planejando a Configuração do Communications Server para Linux

Você provavelmente precisará coletar informações de configuração de várias fontes, como administradores de rede e de host, programadores de aplicação e usuários finais.

Se você estiver tentando se conectar a outro nó, o administrador desse nó será um contato-chave. O administrador de um nó pode lhe informar os nomes, endereços e características de todos os recursos nesse nó. Geralmente, você precisará ter certeza de que os parâmetros de configuração correspondentes são digitados no nó local e no nó remoto.

Folhas de Tarefas

As telas da ajuda on-line no programa de administração Motif contêm folhas de tarefas que fornecem orientação ao usuário durante determinadas tarefas de configuração. Essas folhas contêm ponteiros para todas as telas de auxílio dos diálogos que serão usados para o fornecimento de informações de configuração. Você pode usá-las para percorrer o auxílio e ver exatamente quais dados devem ser coletados.

As folhas de tarefas também fazem referência ao auxílio mais detalhado de cada uma das janelas e diálogos que devem ser usados para o fornecimento de informações de configuração. Essas telas de auxílio explicam cada campo a ser preenchido ou selecionado.

Utilizando o Programa de Administração Motif

Antes de usar o programa de administração Motif, talvez você deseje incluir informações de caminho no arquivo `.login` ou `.profile` para permitir que o sistema localize programas executáveis (consulte “Especificando o Caminho para os Programas do Communications Server para Linux”). Além disso, ative o software Communications Server para Linux antes de utilizar o programa de administração (consulte “Ativando o Communications Server para Linux” na página 72).

Para obter informações sobre como chamar o Motif e usar o programa, consulte “Gerenciando o Communications Server para Linux com o Programa de Administração Motif” na página 72.

Especificando o Caminho para os Programas do Communications Server para Linux

Para executar os programas do Communications Server para Linux, especifique o caminho para o diretório que contém os programas executáveis do Communications Server para Linux. Você pode especificar o caminho incluindo o diretório na variável de ambiente `PATH` antes de executar os programas pela primeira vez ou incluindo o nome do diretório sempre que executar os programas.

O programa de administração Motif é armazenado no diretório `/opt/ibm/sna/bin/X11`, e os outros programas são armazenados no diretório `/opt/ibm/sna/bin`. Se incluir esses diretórios na definição da variável de ambiente `PATH` no arquivo `.login` ou `.profile`, o Communications Server para Linux localizará os programas automaticamente. Uma outra opção é especificar o nome do diretório quando executar o programa, como mostrado nos seguintes exemplos:

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

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

Utilizando o Programa de Administração Motif

As linhas de comando de exemplo mostradas neste manual pressupõem que você incluiu os diretórios na variável de ambiente PATH e não incluem nomes de diretórios.

Ativando o Communications Server para Linux

O Communications Server para Linux deve ser ativado no sistema local antes de configurar ou gerenciar o nó local. Da mesma forma que ocorre com qualquer aplicação X/Motif, você também pode precisar instalar a variável de ambiente DISPLAY para indicar um servidor X adequado.

Para ativar o Communications Server para Linux, insira o seguinte comando no prompt de comandos do Linux:

```
sna start
```

Nota: Ao utilizar o comando **sna start**, o software Communications Server para Linux utiliza o diretório a partir do qual você emitiu o comando como seu diretório de trabalho atual e mantém um ou mais descritores de arquivos abertos nesse diretório. Isso significa que você não conseguirá desmontar o sistema de arquivos que contém esse diretório enquanto o software Communications Server para Linux estiver em execução. Para evitar problemas, você deve iniciar o software Communications Server para Linux a partir de um diretório em um sistema de arquivos que não precise ser desmontado; por exemplo, você poderia utilizar `cd /` para alterar o diretório raiz antes de utilizar o comando **sna start**.

Ao instalar o Communications Server para Linux, o utilitário de instalação atualiza automaticamente o arquivo de inicialização `/etc/rc.d/init.d/snastart` para incluir o comando **sna start**. Isso assegura que o Communications Server para Linux seja iniciado automaticamente na inicialização do sistema. Para que o Communications Server para Linux inicie automaticamente, remova a linha ou marque-a como comentário, e siga as instruções nesta seção para ativar o software Communications Server para Linux manualmente.

O Communications Server para Linux registra mensagens para erros padrão (normalmente, na tela do terminal) para indicar que está sendo inicializado e se a inicialização foi concluída com êxito.

Gerenciando o Communications Server para Linux com o Programa de Administração Motif

Para utilizar o programa de administração Motif do Communications Server para Linux, primeiro verifique se o Communications Server para Linux foi inicializado conforme descrito em "Ativando o Communications Server para Linux". (Talvez você também precise instalar a variável de ambiente DISPLAY para indicar um servidor X adequado).

Para iniciar o Motif no segundo plano, emita o seguinte comando:

```
xsnaadmin &
```

O Communications Server para Linux exibe a janela Domínio. Essa janela mostra todos os nós definidos e permite iniciar e parar os nós. Clicar duas vezes em qualquer nó torna visível a janela Nó do nó correspondente, conforme mostrado na Figura 4 na página 74.

A janela Nó mostra informações sobre o nó e seus recursos. Se você ainda não tiver configurado o nó, o programa de administração solicitará que você o configure, conforme descrito em “Configurando o Nó” na página 78.

Nota: Este manual usa a janela de termos para descrever as janelas do Motif que exibem informações sobre os recursos do Communications Server para Linux. Uma janela pode conter uma ou mais seções ou painéis. Um diálogo é uma janela do Motif em que você pode digitar informações.

A janela Nó mostra a maioria das informações necessárias e fornece fácil acesso a tudo. Mostra todos os recursos-chave no nó local.

Se estiver configurando um sistema cliente/servidor Communications Server para Linux com mais de um nó, siga as instruções neste capítulo para configurar cada nó sucessivamente (retornando à janela Domínio para selecionar o próximo nó).

Outras janelas podem ser abertas a partir do menu **Janelas** na janela Nó. Essas janelas incluem o seguinte:

- Janela Conjuntos de LUs
- Janela Nomes dos Destinos CPI-C

O menu **Serviços** na janela Nó fornece uma forma rápida de incluir recursos e fornece auxílio para tarefas de configuração e gerenciamento. O menu **Diagnósticos** conduz aos diálogos Registrando em Log e Rastreado.

Janela Nó (Node)

Uma janela Nó (Node) de exemplo é mostrada na Figura 4 na página 74. A barra de título mostra o nome do sistema Linux.

Utilizando o Programa de Administração Motif

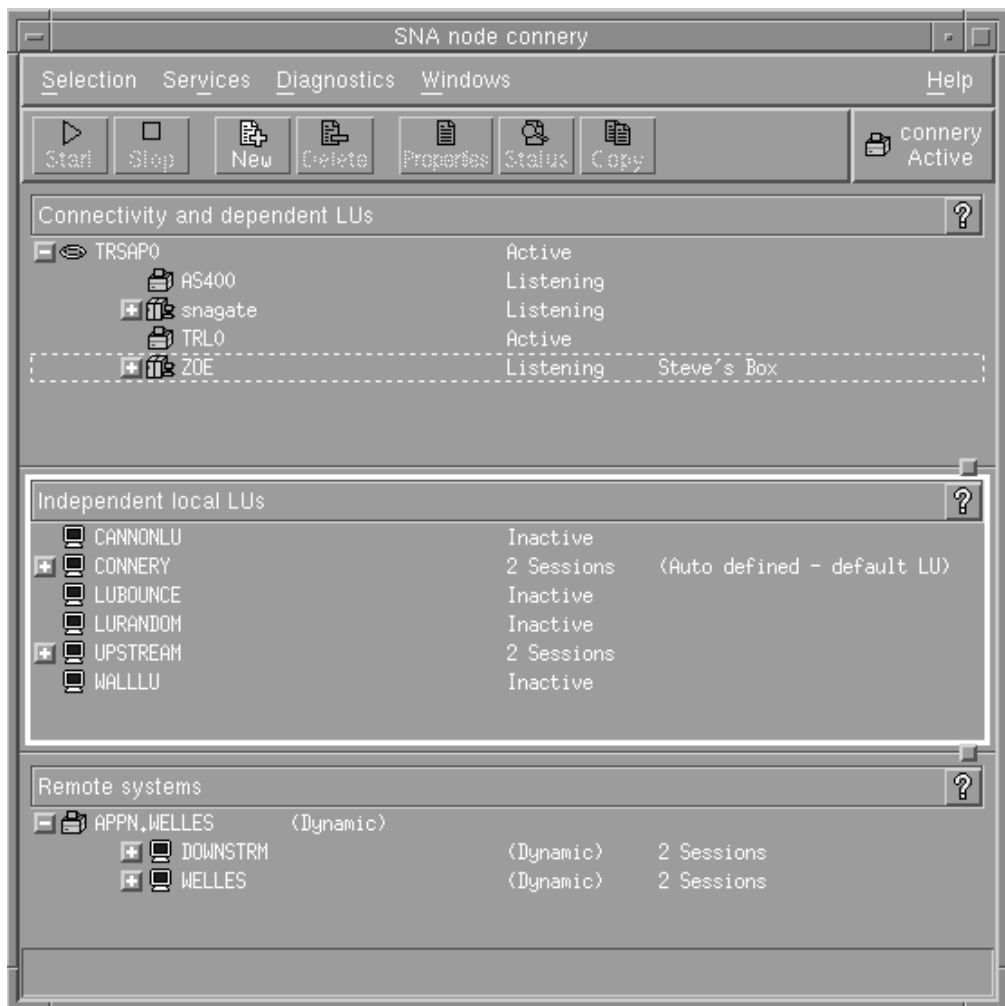


Figura 4. Janela Nó

Na janela Nó, configure e gerencie todos os recursos e componentes do nó Communications Server para Linux.

- Portas
- Estações de link
- LUs do tipo 0-3 e LUs independentes do tipo 6.2
- PUs internas de DLUR
- LUs locais independentes
- Nós remotos
- LUs Associadas

Você pode incluir, excluir, modificar e gerenciar todos esses recursos a partir da janela Nó. O layout dos recursos na janela mostram as relações entre os recursos e permitem que você controle quais recursos são exibidos.

Portas, LUs locais e nós remotos são sempre exibidos. A janela Nó exibe cada estação de link abaixo de sua porta pai, e cada LU dependente abaixo de sua estação de link pai. Também mostra LUs associadas abaixo de LUs locais e de nós remotos.

A janela Nó contém seções separadas para os diferentes tipos de recursos do nó:

- A caixa **Nó** no canto superior direito da janela **Nó** indica se o nó está **Ativo** ou **Inativo**.
- O painel superior da janela **Nó** (o painel **Conectividade**) lista os recursos de conectividade para o nó, inclusive portas, estações de link ou PUs em cada porta, e LUs dependentes em uma determinada estação de link ou PU. Para cada recurso, essa janela mostra as informações de status atuais.
- O painel do meio (LUs Locais Independentes) mostra as LUs independentes definidas no nó local. Essa janela também exibe informações sobre as sessões que usam uma determinada LU e todos os registros que definem a localização de uma LU associada pela estação de link usada para acessá-la.
- O painel inferior (**Sistemas Remotos**) mostra informações sobre nós remotos e LUs associadas. Também mostra informações sobre as sessões de cada nó remoto ou LU associada.

Você pode selecionar qualquer um desses painéis dando um clique sobre eles. Também pode selecionar recursos específicos em um painel dando um clique sobre a linha do recurso. Para exibir ou modificar a configuração de um item, dê um clique duplo sobre ele. (Você pode usar os botões e menus nessa janela para acessar informações de configuração de determinados recursos).

Para cada item listado, os recursos que pertencem a esse item são encadeados nas informações desse item. Por exemplo, as estações de link são agrupadas pela porta à qual pertencem. Você pode clicar no botão **Expandir (Expand)** (+) ao lado de um item para mostrar os recursos desse item, caso ainda não estejam exibidos, ou pode clicar no botão **Contrair (Contract)** (-) para ocultá-los.

Você pode executar as seguintes tarefas de administração na janela **Nó**:

Iniciar ou interromper um recurso

Selecione o recurso e clique no botão **Iniciar (Start)** ou **Parar (Stop)**. (Uma outra opção é selecionar **Iniciar Item (Start item)** ou **Parar Item (Stop item)** no menu **Seleção (Selection)**).

Incluir um recurso para um item

Selecione o item e clique no botão **Novo (New)** (ou selecione **Novo (New)** no menu **Seleção (Selection)**). Por exemplo, para incluir uma estação de link em uma porta, selecione a porta e clique no botão **Novo (New)**.

Excluir um Recurso

Selecione o recurso e clique no botão **Excluir (Delete)** (ou selecione **Excluir (Delete)** no menu **Seleção (Selecionar)**).

Exibir ou modificar a configuração de um recurso

Selecione o recurso e clique no botão **Propriedades (Properties)** (ou selecione **Propriedades (Properties)** no menu **Seleção (Selection)**).

Obter informações de status para qualquer recurso

Selecione o recurso e clique no botão **Status** (ou selecione **Status** no menu **Seleção (Selection)**).

Copie a configuração dos recursos

Selecione o recurso e clique no botão **Copiar (Copy)** (ou selecione **Copiar (Copy)** no menu **Seleção (Select)**).

Além disso, você pode selecionar determinadas tarefas de configuração para o nó no menu **Serviços (Services)**, controlar o registro (do domínio) e rastreamento (do nó) no menu **Diagnósticos (Diagnostics)** e exibir ou modificar recursos de domínio selecionando um dos itens no menu **Janelas (Windows)**.

Itens de Recurso

O layout dos recursos em uma janela mostra os relacionamentos entre eles.

Se um item possui um ou mais itens filhos associados a ele, um símbolo **Expandir (Expand)** (+) ou um símbolo **Contraír (Contract)** (–) aparece perto dele:

- Um símbolo **Expandir (Expand)** indica que os itens filho associados estão ocultos. Você clica no símbolo **Expandir (Expand)**, ou pressiona a tecla + no teclado numérico, para mostrá-los.
- Um símbolo **Contraír (Contract)** indica que os itens filho estão exibidos. Você pode clicar no símbolo de **Contraír (Contract)** ou pressionar a tecla – no teclado numérico para ocultá-los.
- Se um item não tiver nenhum dos dois símbolos ao seu lado, isso significa que o item não tem itens filho associados a ele.

Por exemplo, uma estação de link está associada a uma determinada porta. No painel Conectividade da janela Nó, a estação de trabalho é exibida abaixo de sua porta pai juntamente com todas as outras estações de link associadas a essa porta. A porta é sempre exibida, mas você pode optar por exibir ou ocultar a lista de estações de link associadas. Da mesma forma, as estações de link com uma lista de LUs associadas podem ser expandidas para exibir as LUs ou contraídas para ocultá-las.

Um recurso pai deve ser sempre configurado antes de seus recursos filho. A eliminação do recurso pai fará com que todos os seus recursos filho também sejam eliminados.

Botões da Barra de Ferramentas

As janelas de recursos incluem botões da barra de ferramentas para facilitar a execução de funções comuns. Uma barra de ferramentas do Communications Server para Linux é mostrada na Figura 5.



Figura 5. Barra de Ferramentas do Communications Server para Linux

Nem todos os botões são exibidos nas barras de ferramentas de cada janela de recursos. Se a operação de um botão não for válida para o item selecionado no momento (ou uma operação exigir que um item seja selecionado, mas não existir nenhum selecionado), a descrição do botão será exibida em cinza e a função não poderá ser selecionada (se você clicar no botão, nada acontecerá). Os seguintes botões podem ser exibidos em janelas de recursos:

Iniciar (Start)

Inicia o item selecionado.

Parar (Stop)

Interrompe o item selecionado.

Novo (New)

Inclui um novo item de recurso.

Excluir

Elimina os recursos selecionados.

Propriedades (Properties)

Abre o diálogo do item selecionado para exibir ou modificar a configuração do item.

Status Exibe o status atual do item selecionado.

Copiar (Copy)

Copia o item selecionado. Ao clicar nesse botão, um diálogo cujos campos duplicam a configuração do item selecionado será aberto. Preencha os campos do diálogo (preenchendo o nome do novo item) para incluir o novo recurso.

Muitos recursos, como portas e estações de link, não podem ser modificados enquanto estão ativos. Você pode, contudo, exibir os parâmetros de um recurso ativo selecionando o recurso e clicando no botão **Propriedades (Properties)** para abrir seu diálogo. Clique no botão **Fechar (Close)** quando tiver concluído.

Configurando Funções de Cliente/Servidor

Esta seção terá relevância apenas se instalou o Communications Server para Linux num ambiente de cliente/servidor (com vários nós Communications Server para Linux na mesma rede).

Em um ambiente de cliente/servidor, um servidor pode ser marcado como um servidor de configuração. Communications Server para Linux mantém uma lista desses servidores de configuração. O primeiro servidor listado é o servidor master e todos os outros servidores listados são servidores de backup. Os servidores são listados em ordem, de forma que o segundo servidor listado (o primeiro servidor de backup) assuma o controle se o servidor master estiver indisponível, o terceiro servidor listado (o segundo servidor de backup) assuma o controle se nem o servidor master nem o primeiro servidor de backup estiver disponível, e assim por diante.

Quando alguns nós no domínio estão ativos, o primeiro servidor de configuração disponível no domínio (o primeiro a ser conectado e com o software Communications Server para Linux em execução) torna-se o servidor master. Se o servidor master atual se tornar indisponível (porque não pode ser contatado, talvez devido a uma falha da rede ou porque o software SNA em execução está parado), o próximo servidor de configuração na lista se tornará o novo servidor master.

O Communications Server para Linux pode executar sem um master. Isso ocorre se nenhum dos servidores na lista de servidores de configuração pode ser contatado. Se isso ocorrer, será possível visualizar e configurar recursos do nó somente nos servidores que podem ser contatados.

Nota: Você não pode indicar diretamente qual nó funciona como o servidor master; o servidor master é selecionado com base na ordem em que os nós são incluídos na lista de servidores de configuração. Se desejar mover um servidor para o início da lista, remova todos os outros nós da lista e, em seguida, inclua-os novamente.

Na janela Domain do programa de configuração Motif, é possível incluir um servidor de configuração selecionando **Fazer Configuração do Servidor** no menu **Seleção**. O servidor é incluído no final da lista; ele se torna o servidor master somente se todos os outros servidores de configuração estão indisponíveis. Para remover um servidor, selecione **Servidor de Configuração Remota** no menu **Seleção**.

Configurando Funções de Cliente/Servidor

Nota: Não poderá excluir um servidor se ele for o único servidor listado no qual o software Communications Server para Linux está em execução, porque, nesse caso, não haverá nenhum outro servidor que possa assumir o controle como o servidor master. Pelo menos um servidor master ativado é necessário em uma configuração de cliente/servidor.

Para obter informações adicionais sobre como configurar e gerenciar um sistema cliente/servidor Communications Server para Linux, consulte o *Communications Server for Linux Administration Guide*. Este manual também fornece informações sobre a configuração avançada de cliente/servidor, inclusive como mover clientes e servidores para domínios diferentes do Communications Server para Linux, e como configurar os detalhes da operação do cliente.

Configurando o Nó

A primeira etapa na configuração do Communications Server para Linux em um sistema é configurar o nó local. A configuração do nó fornece as informações básicas de que o nó precisa para comunicar-se em uma rede SNA. Configure o nó para que possa definir a conectividade ou outros recursos para o nó.

Se o nó já tiver sido configurado, você poderá usar os procedimentos descritos nesta seção para modificar a configuração do nó; mas, interrompa o nó antes de fazer alterações na configuração.

Antes de configurar o nó, decida se deseja configurar o nó como um nó APPN ou como um nó não-APPN. Essa decisão depende dos recursos dos outros nós SNA com os quais você está se comunicando.

Um nó Communications Server para Linux que se comunica diretamente com um computador é mostrado na Figura 6.

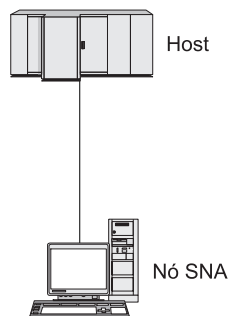


Figura 6. Nó Communications Server para Linux que se Comunica Diretamente com um Host

Se o host não suportar APPN, configure o nó Communications Server para Linux como um nó LEN. Se o host suportar APPN, o nó Communications Server para Linux poderá ser configurado como um nó de rede ou de extremidade APPN (se o Communications Server para Linux utilizar SNA apenas para comunicação com o host, provavelmente será necessário configurar o nó Communications Server para Linux como um nó de extremidade ou nó de rede derivado).

Vários nós Communications Server para Linux em uma rede APPN são mostrados na Figura 7 na página 79.

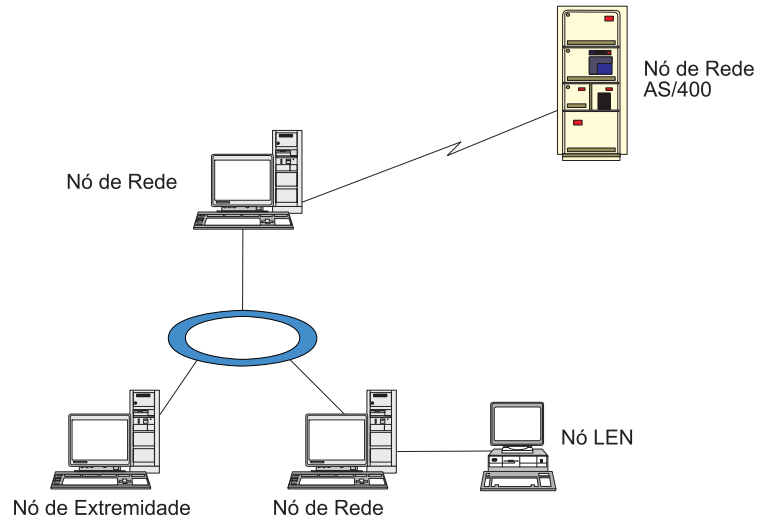


Figura 7. Nós Communications Server para Linux numa Rede APPN

Quando o nó local fizer parte de uma rede APPN, configure-o como um nó de rede APPN se o nó fornecer serviços de percurso APPN para outros nós. Se outros nós fornecerem serviços de percurso, configure o nó local como um nó de extremidade APPN. Se o nó local se comunica apenas com um nó conectado diretamente (que pode ser de qualquer tipo) configure o nó como um nó LEN.

Antes de começar a configuração do nó, obtenha as seguintes informações:

- Tipo do suporte APPN (nó de rede, nó de rede de ramificação, nó de extremidade ou nó LEN).
- Nome do ponto de controle (e alias, se for diferente). Consulte o planejador de rede para determinar esse nome.
- ID do Nó padrão. (Você pode substituir esse padrão ao configurar um link de comunicação individual.)

Para configurar o nó, siga estas etapas na janela Nó:

1. Selecione **Configure os Parâmetros do Nó** no menu **Serviços** ou clique duas vezes na caixa **Nó**, no canto superior direito da janela **Nó**. O Communications Server para Linux exibe o diálogo **Parâmetros do Nó**.
2. Especifique o nível do suporte APPN, o nome do ponto de controle e (se necessário) o ID do nó padrão.
3. Clique no botão **OK** para definir o nó. Ao definir o nó, o Communications Server para Linux definirá automaticamente uma LU padrão com o mesmo nome que o ponto de controle.

Para sair sem salvar os valores digitados, clique no botão **Cancelar**.

Configurando a Conectividade

Para que um nó do Communications Server para Linux se comunique com outros nós, configure a conectividade com pelo menos um nó adjacente. Um link de conexão pode ser configurado para executar tráfego dependente, independente ou ambos.

Você pode ter placas para um ou mais protocolos de link instalados no computador. Muitas informações que precisam ser digitadas para configurar a conectividade dependem do protocolo de link que você está usando. Para obter

Configurando a Conectividade

uma lista dos protocolos de link suportados pelo Communications Server para Linux, consulte “Requisitos de Instalação” na página 19.

Para configurar um link, você precisa definir uma porta e (na maioria dos casos) uma estação de link. Quando o programa de administração Motif é usado, um DLC (controle de link de dados) é automaticamente configurado como parte da configuração da porta. Além disso, você tem a opção de definir a porta como parte de uma rede de conexão.

Os links necessários para a configuração dependem até onde você quer chegar e se a rede é APPN. As informações necessárias dependem do protocolo de link e do fato de o link ser de tráfego dependente, independente ou ambos.

Como exemplos, esta seção explica como configurar os seguintes tipos de link:

- Link suportando o tráfego dependente com um sistema host por meio de uma linha SDLC.
- Ligar tráfegos dependente e independente suportado em uma rede APPN usando o protocolo de link Ethernet. Esse exemplo também define uma rede de conexão na porta Ethernet.
- Link do Enterprise Extender em uma rede APPN (observe que os links Enterprise Extender suportam apenas tráfego independente).

Para outros protocolos de link, consulte o *Communications Server for Linux Administration Guide* ou a ajuda on-line do programa de administração Motif.

Configurando um Link SDLC para Tráfego Dependente

Para uma porta SDLC (Synchronous Data Link Control), as seguintes informações são necessárias:

- O nome da porta SNA (geralmente o padrão pode ser usado). Também é preciso especificar o número de dispositivo do SDLC.
- Se a porta deve ser ativada automaticamente quando o nó for iniciado.
- Tipo de Linha (de envio chaveada, de recebimento chaveada ou linha dedicada).
- Função do Link (primário, secundário, negociável, multidrop primário ou multi-PU secundário).
- Endereço do Poll (apenas para linha de recebimento chaveada numa porta não primária). Para outros tipos de portas, configure o endereço de poll na estação de link.

Para uma estação de link SDLC, as seguintes informações adicionais são necessárias:

- Método de ativação (pelo administrador, na inicialização por nó ou por demanda).
- Digite o tráfego suportado (neste exemplo, dependente apenas).
- Função do nó remoto (neste exemplo, host).

Para configurar o link SDLC, execute as seguintes etapas na janela Nó:

1. Configure a porta:
 - a. Selecione o painel Conectividade da janela.
 - b. Selecione **Nova Porta** no submenu **Conectividade** no menu **Serviços** (ou clique no botão **Novo** na barra de botões).
 - c. No diálogo resultante, selecione o tipo de protocolo no menu de opções e escolha para definir uma porta.

Ao clicar no botão **OK**, o Communications Server para Linux exibe o diálogo Porta SDLC.

- d. Digite os valores apropriados nos campos do diálogo.
- e. Clique no botão **OK** para definir a porta.

A porta é exibida no painel Conectividade da janela Nó.

2. Defina uma estação de link na porta:

- a. Certifique-se de que selecionou a porta na qual a estação de link está sendo incluída no painel Conectividade da janela Nó.
- b. Selecione **Nova Estação de Link** no submenu **Conectividade** no menu **Serviços** (ou clique no botão **Novo** na barra de botões).
- c. Clique no botão **OK**.

O Communications Server para Linux exibe o diálogo Estação de Link SDLC.

- d. Digite os valores apropriados nos campos do diálogo.
- e. Clique no botão **OK** para definir uma estação de link.

A estação de link é exibida abaixo da porta à qual pertence no painel Conectividade da janela Nó.

Configurando um Link Ethernet para Suportar Tráfego Dependente e Independente

Este exemplo mostra como configurar um link Ethernet que suporte os tráfegos dependente e independente em uma rede APPN. Além disso, define uma rede de conexão na porta Ethernet.

Para uma porta Ethernet, você precisa das seguintes informações:

- O nome da porta SNA (geralmente o padrão pode ser usado). Se você tiver várias placas de rede Ethernet, também precisará fornecer o número da placa Ethernet. Também é preciso especificar o número de SAP (service access point) (normalmente 04 para adaptadores Intel e OSA2). Para um adaptador OSA-Express, o número SAP local deve corresponder àquele definido no OSA/SF para os endereços de dispositivo de E/S que correspondem à interface ethX nesta imagem do Linux.
- Se a porta deve ser ativada automaticamente quando o nó for iniciado.
- O nome da rede de conexão (deve ser igual em todas as portas na mesma rede de conexão).

Para uma estação de link Ethernet, você precisa das seguintes informações adicionais:

- Método de ativação (pelo administrador, na inicialização por nó ou por demanda).
- Tipo de tráfego suportado (nesse exemplo, dependente e independente).
- Nome do ponto de controle do nó remoto (só é necessário para um nó LEN).
- Tipo do nó remoto (nó de rede, nó de extremidade ou nó de descoberta).
- Função do nó remoto (nesse exemplo, gateway SNA de recebimento de dados ou DLUR de passagem).
- Para configurar uma estação de link seletiva, você precisa do endereço MAC (Medium Access Control) e do número de SAP (normalmente 04) para a estação remota. Se não fornecer informações de endereço e especificar Por Administração no campo *Ativação*, a estação de link será uma estação de link de monitoramento não seletivo.

Configurando a Conectividade

Para configurar o link Ethernet, siga estas etapas na janela Nó:

1. Configure a porta:
 - a. Selecione o painel Conectividade da janela.
 - b. Selecione **Nova Porta** no submenu **Conectividade** no menu **Serviços** (ou clique no botão **Novo** na barra de botões).
 - c. No diálogo resultante, selecione o tipo de protocolo no menu de opções e escolha para definir uma porta.
Ao clicar no botão **OK**, o Communications Server para Linux exibe o diálogo SAP Ethernet.
 - d. Digite os valores apropriados nos campos do diálogo.
 - e. Clique no botão **OK** para definir a porta.
A porta é exibida no painel Conectividade da janela Nó.
2. Defina uma estação de link na porta:
 - a. Certifique-se de que selecionou a porta na qual a estação de link está sendo incluída no painel Conectividade da janela Nó.
 - b. Selecione **Nova Estação de Link** no submenu **Conectividade** no menu **Serviços** (ou clique no botão **Novo** na barra de botões).
 - c. Clique no botão **OK**.
O Communications Server para Linux exibe o diálogo Estação de Link Ethernet.
 - d. Digite os valores apropriados nos campos do diálogo.
 - e. Clique no botão **OK** para definir uma estação de link.
A estação de link é exibida abaixo da porta à qual pertence no painel Conectividade da janela Nó.

Configurando um Link do Enterprise Extender

Este exemplo mostra como configurar um link do Enterprise Extender em uma rede APPN. Observe que os links Enterprise Extender suportam apenas tráfego Independente.

Para uma porta do Enterprise Extender, você precisa das seguintes informações:

- O nome da porta SNA (geralmente o padrão pode ser usado). Se você tiver diversas placas adaptadoras de rede executando IP, também precisará fornecer o nome da interface IP que deseja utilizar (como eth0).
- Se a porta deve ser ativada automaticamente quando o nó for iniciado.

Para uma estação de link do Enterprise Extender, você precisa das seguintes informações adicionais:

- Método de ativação (pelo administrador, na inicialização por nó ou por demanda).
- Tipo do nó remoto (nó de rede, nó de extremidade ou nó de descoberta).
- Para configurar uma estação de link seletiva, você precisa do nome do host IP e do endereço IP da estação remota. Se você não fornecer estas informações e especificar Por Administrador no campo *Ativação*, a estação de link se torna uma estação de link de escuta não acessível.

Para configurar a estação de link do Enterprise Extender, execute as seguintes etapas da janela de nó:

1. Configure a porta:
 - a. Selecione o painel Conectividade da janela.

- b. Selecione **Nova Porta** no submenu **Conectividade** no menu **Serviços** (ou clique no botão **Novo** na barra de botões).
 - c. No diálogo resultante, selecione o tipo de protocolo no menu de opções e escolha para definir uma porta.
Ao clicar no botão **OK**, o Communications Server para Linux exibe o diálogo IP da Porta.
 - d. Digite os valores apropriados nos campos do diálogo.
 - e. Clique no botão **OK** para definir a porta.
A porta é exibida no painel Conectividade da janela Nó.
2. Defina uma estação de link na porta:
- a. Certifique-se de que selecionou a porta na qual a estação de link está sendo incluída no painel Conectividade da janela Nó.
 - b. Selecione **Nova Estação de Link** no submenu **Conectividade** no menu **Serviços** (ou clique no botão **Novo** na barra de botões).
 - c. Clique no botão **OK**.
O Communications Server para Linux exibe o diálogo Estação de Link IP.
 - d. Digite os valores apropriados nos campos do diálogo.
 - e. Clique no botão **OK** para definir uma estação de link.
A estação de link é exibida abaixo da porta à qual pertence no painel Conectividade da janela Nó.

Configurando LUs Tipo 0–3

Para dar suporte a aplicativos de usuário que utilizam LUs tipo 0–3, configure as LUs dependentes. Antes de fazer isso, execute a seguinte configuração:

- Configure o nó, conforme descrito em “Configurando o Nó” na página 78.
- Configure um link para dar suporte ao tráfego de LU dependente, conforme descrito no “Configurando a Conectividade” na página 79.

Não é necessário configurar um link direto para o host se tiver um link de envio de dados para outro nó via gateway SNA, ou caso esteja utilizando DLUR. Para obter informações adicionais, consulte “Configurando o Gateway SNA” na página 93 e “Configurando o DLUR” na página 95.

Configure LUs dependentes tipo 0–3 para dar suporte à comunicação com um sistema host. É possível utilizar as informações nesta seção para definir uma LU a fim de suportar a Concentração PU, DLUR ou LUA. Também é possível definir um intervalo de LUs, para configurar várias LUs do mesmo tipo numa única operação.

Além disso, é possível definir um conjunto de LUs para ser utilizado quando necessário, designando uma LU para um conjunto ao definir a LU ou designando as LUs definidas anteriormente a um conjunto.

Definindo LUs Tipo 0–3

Antes de configurar a LU de 3270, obtenha as seguintes informações:

- Nome da LU. (Este é um identificador local e não precisa corresponder à configuração do host.)
- Número da LU (ou números de uma faixa de LUs).
- Tipo de LU (modelo de tela 3270 ou impressora 3270).
- Nome do conjunto (se você estiver incluindo a LU em um conjunto).

Configurando LUs Tipo 0–3

Para configurar uma LU dos tipos 0–3 para uma estação de link definida anteriormente, siga estas etapas na janela Nó:

1. Selecione a estação de link para o host no painel Conectividade da janela.
2. Clique no botão **Novo**.
3. Selecione o tipo de LU (**Nova LU de Vídeo 3270** ou **Nova LU de Impressora 3270**) no diálogo resultante.

Ao selecionar esse item e clicar em **OK**, o Communications Server para Linux exibirá o diálogo Tipo de LU 0–3.

4. Digite os valores apropriados nos campos do diálogo.
5. Clique no botão **OK** para definir a LU.

A LU é exibida no painel Conectividade da janela Nó, abaixo da estação de link para o host.

Definindo um Conjunto de LUs

Para LU tipo 0–3, é possível definir conjuntos de LUs de modo a simplificar a configuração do usuário e fornecer maior flexibilidade ao estabelecer sessões do host. Por exemplo, você pode definir várias LUs em um único conjunto de LUs e, em seguida, configurar vários usuários utilizando esse conjunto de LUs. Isso facilita a configuração das sessões de usuário e permite que qualquer sessão utilize qualquer LU no conjunto.

Nota: Você pode atribuir uma sessão de usuário a uma LU específica ou a um conjunto de LUs.

- Se você atribuir a sessão do usuário a uma LU específica que está em um conjunto, a sessão utilizará essa LU se ela estiver disponível; do contrário, ela utilizará qualquer LU disponível do conjunto, embora você a tenha atribuído ao conjunto de LUs, em vez de uma LU específica.
- Se você desejar que o usuário utilize apenas uma LU especificada, de forma que a sessão do usuário não poderá ser estabelecida se a LU já estiver em uso, assegure-se de que a LU não esteja em um conjunto.

É possível visualizar os conjuntos de LUs para o nó local do Communications Server para Linux, utilizando a janela Conjunto de LUs. Essa janela lista os conjuntos de LUs configurados no sistema local e permite que você selecione LUs a serem incluídas em um conjunto de LUs.

Os seguintes tipos de LUs podem ser incluídos num conjunto (não misture LUs de tipos diferentes no mesmo conjunto):

- LU de tela 3270
- LU sem restrição

Para que você possa incluir LUs em um conjunto, as LUs devem ser definidas no nó local.

Para configurar um conjunto de LUs, siga estas etapas na janela Nó:

1. Selecione **Conjuntos de LUs** no menu **Janelas**.
O Communications Server para Linux exibe a janela Conjuntos de LUs.
2. Clique no botão **Novo**.
O Communications Server para Linux exibe o diálogo Configuração do Conjunto de LUs.

A caixa à direita lista as LUs que ainda não estão alocadas para um conjunto. Qualquer uma delas pode ser incluída no novo conjunto.

3. Selecione a LU ou LUs a serem incluídas no conjunto e clique no botão **Novo** para mover as LUs selecionadas para a caixa à esquerda.

Para remover uma LU da caixa à esquerda, selecione-a e clique no botão **Remover**.

4. Clique no botão **OK** para definir o conjunto de LUs.

Todas as LUs na caixa à esquerda são incluídas no conjunto de LUs.

O conjunto é exibido na janela Conjuntos de LUs.

Configurando a Comunicação APPC

As aplicações APPC e CPI-C exigem que você configure primeiro a APPC. Uma aplicação APPC usa os recursos da LU do tipo 6.2 do nó para comunicar-se com outra aplicação APPC ou CPI-C em um host ou computador não-hierarquizado, através de um modo especificado.

Para que você possa configurar a comunicação APPC, execute a seguinte configuração:

1. Configure o nó, conforme descrito em “Configurando o Nó” na página 78.
2. Configure a conectividade, conforme descrito em “Configurando a Conectividade” na página 79.

As etapas de configuração restantes dependem do fato de a configuração suportar tráfego dependente, independente ou ambos:

APPC Independente

A APPC independente usa LUs independentes. Cada sessão LU-LU envolve uma LU local e uma LU associada.

Para a LU local, você pode usar a LU padrão predefinida associada ao ponto de controle do nó, ou pode configurar novas LUs locais.

A LU associada não precisará ser configurada se o nó Communications Server para Linux for um nó de extremidade ou um nó de uma rede APPN, porque o APPN pode localizar as LUs associadas dinamicamente. No entanto, você precisará configurar a LU associada se a rede não for APPN ou se for um nó LEN. Nesse caso, você deve configurar o nó remoto no local onde se encontra a LU associada e, em seguida, definir a LU associada no nó remoto.

APPC Dependente

Se o nó remoto for um host que não suporta LU 6.2 independente, configure para tráfego dependente. Para APPC dependente, configure uma LU local.

Se as aplicações usarem CPI-C, talvez você precise fazer uma configuração adicional de CPI-C depois de configurar a APPC (consulte “Configurando o CPI Communications” na página 90). Uma aplicação CPI-C usa os recursos da LU do tipo 6.2 do nó e os recursos do modo para comunicar-se com outra aplicação APPC ou CPI-C em um host ou computador não-hierarquizado. Defina os mesmos recursos para uma aplicação CPI-C que foram definidos para uma aplicação APPC. Além disso, se o TP no computador Communications Server para Linux for o TP de chamada, também conhecido como o TP de origem (o TP que inicia a conversação), pode ser necessário definir uma ou mais entradas de informações secundárias para ele, conforme descrito em “Configurando o CPI

Configurando a Comunicação APPC

Communications” na página 90. Cada uma dessas entradas fornece informações sobre o TP associado, a LU e recursos de modo usados para acessá-lo e todas as informações de segurança necessárias.

Esta seção explica como configurar uma rede APPN simples (usando a LU 6.2 independente), que consiste em um nó de rede, um nó de extremidade e um nó LEN, conforme descrito em “Configurando uma Rede APPN Simples”. (Esse exemplo também mostra como obter informações de status para sessões CP-CP entre dois nós).

Além disso, explica como configurar a comunicação de APPC dependente, conforme descrito em “Configurando o APPC Dependente” na página 90.

Os dois exemplos pressupõem que as sessões APPC usam um modo e classe de serviço (COS) padrão.

Para obter informações sobre como configurar informações adicionais de APPC, por exemplo, modos, segurança e TPs disponíveis para chamada (de destino), consulte o *Communications Server for Linux Administration Guide*.

Configurando uma Rede APPN Simples

A rede APPN mais simples que pode ser configurada inclui apenas dois nós: um nó de rede APPN e um nó de extremidade APPN. O nó de rede cuida do percurso da sessão até o nó de extremidade.

Configurando um Nó de Rede

Este cenário presume que você esteja utilizando a LU de ponto de controle e um modo padrão, e esteja utilizando um tipo de link de rede local (Token Ring, Ethernet). Nesse caso, você pode configurar o nó de rede simplesmente seguindo estas tarefas de configuração:

1. Configure o nó, conforme descrito em “Configurando o Nó” na página 78. Para o campo *Suporte do APPN*, selecione o valor *Nó de Rede*. Anote o nome do ponto de controle.
2. Configure a conectividade, conforme descrito em “Configurando a Conectividade” na página 79. Configure o link para suportar tráfego independente.

Para entrar em contato com esse nó de rede a partir de um nó de extremidade adjacente, você precisará saber o endereço MAC e número de SAP da porta no nó de rede. Você pode utilizar o seguinte procedimento para obter o endereço MAC em um nó do Communications Server para Linux:

1. Selecione a porta na janela *Nó*.
2. Clique no botão **Iniciar** para iniciar a porta.
3. Clique no botão **Status** para obter informações de status sobre a porta. O diálogo *Status da Porta* exibe o endereço MAC e o número de SAP.
4. Anote-os para que possa digitar esses valores no diálogo de configuração de estação de link para o nó de extremidade.

Configurando um Nó de Extremidade

Este cenário presume que você esteja utilizando a LU de ponto de controle e um modo padrão, e esteja utilizando um tipo de link de rede local (Token Ring, Ethernet). Nesse caso, você pode configurar o nó de rede simplesmente seguindo estas tarefas de configuração:

1. Configure o nó, conforme descrito em “Configurando o Nó” na página 78. No campo *Suporte do APPN*, selecione o valor *Nó de Extremidade*.
2. Configure a conectividade, conforme descrito em “Configurando a Conectividade” na página 79. Configure o link para suportar o tráfego independente e forneça as seguintes informações para a estação de link:
 - Digite o nome do nó de rede (consulte “Configurando um Nó de Rede” na página 86) como o valor do campo *Nó Remoto*.
 - Digite o endereço MAC e o número de SAP para a porta no nó de rede no painel *Informações de Contatos* no diálogo de configuração da estação de link.

Em uma rede APPN, uma única estação de link conectada a um nó de rede adjacente pode ser usada para que você se comunique com qualquer nó remoto na rede; portanto, você não precisa configurar uma estação de link separada para cada nó remoto.

Verificando a Conectividade entre Dois Nós

Esse exemplo pressupõe que você configurou um nó de rede, conforme descrito em “Configurando um Nó de Rede” na página 86, e um nó de extremidade, conforme descrito em “Configurando um Nó de Extremidade” na página 86. Você pode executar o seguinte procedimento para um nó de extremidade:

1. Na janela *Nó*, selecione a estação de link que se conecta ao nó de rede adjacente.
2. Clique no botão **Iniciar** para iniciar a estação de link.

Quando a estação de link é iniciada, as sessões CP-CP entre os dois nós são estabelecidas automaticamente. Essas sessões são exibidas no painel *LUs Locais Independentes* da janela *Nó*.
3. Para obter informações de status para uma sessão, selecione a sessão na janela *Nó* e clique no botão **Status**.

Configurando uma LU APPC Independente

Em muitos casos, as aplicações podem usar a LU de ponto de controle do nó local, que é automaticamente definida quando você configura o nó. Essa é a LU padrão—se a aplicação não especificar uma determinada LU, essa será usada. Se a aplicação usar a LU padrão, você não precisará definir uma LU local. Verifique a documentação da aplicação APPN ou entre em contato com o programador da aplicação.

Para configurar uma LU 6.2 independente, você precisa das seguintes informações:

- Nome da LU local.
- Alias da LU local (se um alias for usado em um TP suportado por essa LU).

Para configurar uma LU local independente, siga estas etapas na janela *Nó*:

1. Selecione o painel *LUs Locais Independentes* da janela.
2. Selecione **Nova LU Local Independente** no submenu **APPC** no menu **Serviços** (ou clique no botão **Novo**).

O Communications Server para Linux exibe o diálogo *LU Local*.

3. Digite os valores apropriados nos campos do diálogo.
4. Clique no botão **OK** para definir uma LU local. A LU independente é exibida no painel *LUs Locais Independentes* da janela *Nó*.

Configurando LUs Associadas para um Nó LEN

Defina um nó remoto (e as LUs associadas no nó) nas seguintes situações:

Configurando a Comunicação APPC

- Se o nó local for um nó LEN, defina todos os nós remotos e LUs associadas no nó remoto com os quais ele se comunica usando a APPC. Um nó LEN não pode localizar LUs associadas de forma dinâmica; a definição do nó remoto permite que isso seja feito.
- Se o nó local não fizer parte de uma rede APPN (por exemplo, se você tiver dois nós de extremidade diretamente conectados, sem nenhum servidor de nó de rede), as LUs não poderão ser localizadas dinamicamente. Nesse caso, configure cada LU associada.
- Se o nó remoto for um nó LEN e o nó local for um nó de rede que funciona como o servidor de nó de rede do nó LEN, defina o nó LEN (e suas LUs associadas) como um nó remoto no servidor de nó de rede. Essa definição permite que os nós no restante da rede APPN localizem LUs no nó LEN.
- Se o nó remoto estiver em uma rede APPN diferente, defina o nó remoto porque ele não pode ser dinamicamente localizado.

Não defina LUs associadas se os nós local e remoto fizerem parte da mesma rede APPN.

Quando você inclui uma definição de nó remoto, uma LU associada com o mesmo nome do nó remoto é automaticamente incluída; essa é a LU de ponto de controle para o nó remoto. Se a aplicação usar essa LU associada, você não precisará incluir outra LU associada, apesar de talvez desejar incluir um alias de LU para a LU associada. Para incluir um alias, dê um clique duplo na LU associada e digite o alias no diálogo Configuração da LU Associada.

Se a aplicação usar um alias de LU para referir-se à sua LU associada, inclua uma definição de alias de LU associada.

Se o nó remoto ou local for um nó LEN, defina a LU associada como um filho do nó remoto, pois o nó LEN não pode participar na localização dinâmica de LUs. Se a aplicação usar a LU de ponto de controle do nó remoto como sua LU associada, isso significa que a LU de ponto de controle foi definida automaticamente quando o nó remoto foi definido.

Você pode usar o programa de administração Motif para incluir um alias de LU associada (consulte “Definindo um Alias de LU Associada” na página 89), incluir uma definição de uma LU associada em um nó remoto específico (consulte “Definindo uma LU Associada em um Nó Remoto” na página 89) ou definir várias LUs associadas usando curingas (consulte “Definindo Várias LUs Associadas Usando Curingas” na página 89).

Definindo um Nó Remoto: Antes de configurar um nó remoto, você precisa das seguintes informações:

- O nome qualificado da rede SNA do nó.

Para configurar um nó remoto, siga estas etapas na janela Nó:

1. Selecione o painel Sistemas Remotos da janela.
2. Selecione **Novo Nó Remoto** no submenu **APPC** no menu **Serviços** (ou clique no botão **Novo** na barra de botões, em seguida seleciona **Definir Nó Remoto**). O Communications Server para Linux exibe o diálogo Configuração de Nó Remoto.
3. Digite os valores apropriados nos campos do diálogo.
4. Clique no botão **OK** para definir o nó remoto. O nó remoto é exibido no painel Sistemas Remotos da janela Nó.

Ao definir um sistema remoto, o Communications Server para Linux define automaticamente a LU de ponto de controle no nó remoto como uma LU associada no nó local.

Definindo um Alias de LU Associada: Para definir um alias de LU associada, você precisa das seguintes informações:

- Nome qualificado de LU associada (nome de rede SNA e nome de LU)
- Alias de LU associada usado por um TP local

Para incluir um alias de LU associada, siga estas etapas na janela Nó:

1. Selecione o painel Sistemas Remotos da janela.
2. Selecione **APPC, Novas LUs Associadas e Alias da LU Associada** no menu **Serviços** (ou clique no botão **Novo** na barra de botões e selecione **Definir Alias da LU Associada**).

O Communications Server para Linux exibe o diálogo Configuração do Alias da LU Associada.

3. Digite o nome e alias da LU associada no diálogo.
4. Clique no botão **OK** para definir o alias de LU associada. Esse alias é exibido no painel Sistemas Remotos da janela Nó (como parte da definição Network).

Definindo uma LU Associada em um Nó Remoto: Para definir uma LU associada em um nó remoto específico, você precisa das seguintes informações:

- Nome qualificado de LU associada
- Alias da LU associada (se um alias for usado por um TP local)
- Nome qualificado do nó que contém informações de diretório para a LU associada.

Para incluir uma definição de LU associada de um nó remoto específico, siga estas etapas na janela Nó:

1. Selecione o nó remoto.
2. Selecione **APPC, Novas LUs Associadas e LU Associada no Nó Remoto**, no menu **Serviços** (ou clique no botão **Novo** na barra de botões e selecione **Definir LU Associada no Nó Remoto**).

O Communications Server para Linux exibe o diálogo Configuração da LU Associada.

3. Digite os valores apropriados nos campos do diálogo.
4. Clique no botão **OK** para definir a LU associada. Esse alias é exibido no painel Sistemas Remotos da janela Nó, abaixo do sistema remoto ao qual ele pertence.

Definindo Várias LUs Associadas Usando Curingas: Você pode usar curingas para configurar a localização de um conjunto de LUs associadas que estão localizadas no mesmo nó remoto e cujos nomes são iniciados pelos mesmos caracteres. Se você usar curingas, não precisará configurar cada LU associada individualmente.

Quando você definir LUs associadas usando curingas, forneça as seguintes informações:

- Nome qualificado da LU associada. O nome da LU associada curinga consiste em duas cadeias EBCDIC de tipo A, cada uma com 1–8 caracteres, que correspondem aos nomes qualificados de LU de várias LUs associadas.

A primeira cadeia pode ser um nome de rede SNA completo que corresponda exatamente ao nome de rede das LUs associadas ou um prefixo curinga que

Configurando a Comunicação APPC

corresponda ao início do nome da rede. Se você digitar um prefixo curinga para o nome da rede, deixe a segunda cadeia em branco.

Se você fornecer um nome de rede SNA completo para a primeira cadeia, também poderá digitar um valor para a segunda cadeia. (Não é permitido digitar a segunda cadeia, a menos que você tenha fornecido um nome de rede SNA válido para a primeira cadeia). A segunda cadeia é tratada como um prefixo de caractere curinga, que deve corresponder ao início da segunda parte dos nomes qualificados de LU associadas.

- Nome do nó onde as LUs associadas estão localizadas.

Para incluir várias LUs associadas, siga estas etapas na janela Nó:

1. Selecione o nó remoto para o qual você está definindo as LUs associadas.
2. Selecione **APPC, Novas LUs Associadas e LUs Associadas Curingas no Nó Remoto**, no menu **Serviços** (ou clique no botão **Novo**, na barra de botões, e selecione **Definir LUs Associadas Curingas no Nó Remoto**).
O Communications Server para Linux exibe o diálogo Configuração da LU Associada Curinga.
3. Digite as informações apropriadas nos campos do diálogo.
4. Clique no botão **OK** para definir as LUs associadas. Essas LUs são exibidas no painel Sistemas Remotos da janela Nó, abaixo do nó remoto ao qual pertencem.

Configurando o APPC Dependente

Para configurar uma LU 6.2 dependente, você precisa das seguintes informações:

- Nome da LU local.
- Alias da LU local (se um alias for usado em um TP suportado por essa LU).
- Nome da estação de link que fornece a conexão ao host.
- Número da LU.
- Se a LU deve ser atribuída ao conjunto padrão para LUs 6.2 dependentes.

Se você estiver configurando LUs dependentes do tipo 6.2 para serem usadas com aplicações APPC ou CPI-C, talvez deseje defini-las como membros do conjunto padrão. Uma LU não usada do conjunto de LUs definidas como LUs padrão é atribuída a uma aplicação que não especifica uma LU local específica.

Para configurar uma LU local dependente, siga estas etapas na janela Nó:

1. Selecione uma estação de link no painel Conectividade da janela.
2. Selecione **Nova LU Local Dependente** no submenu **APPC** no menu **Serviços** (ou clique no botão **Novo** na barra de botões, e selecione **Nova LU Local Dependente**).
O Communications Server para Linux exibe o diálogo LU Local.
3. Digite os valores apropriados nos campos do diálogo.
4. Clique no botão **OK** para definir uma LU local. A LU dependente é exibida no painel Conectividade, abaixo da estação de link à qual pertence.

Configurando o CPI Communications

Se você suportar uma aplicação CPI-C que use nomes de destino simbólicos de CPI-C, será preciso definir as informações adicionais de CPI-C. Essas informações associam o nome de destino simbólico às informações sobre o TP associado, a LU associada, o modo e a segurança para a conversação.

Para determinar o nome de destino simbólico para o CPI-C, consulte o desenvolvedor da aplicação (se a aplicação for de outro fabricante, consulte a documentação do produto).

Para configurar informações adicionais do CPI-C, você precisa das seguintes informações:

- Nome de destino simbólico usado pelo TP
- Nome do TP associado
- Nome ou alias da LU associada
- Nome do Modo

Para configurar informações adicionais de CPI-C, siga estas etapas na janela Nó:

1. Selecione o **CPI-C** no submenu **APPC** no menu **Serviços**.
O Communications Server para Linux exibe a janela Nomes de Destinos CPI-C.
2. Clique no botão **Novo**.
O Communications Server para Linux exibe o diálogo Configuração do Destino CPI-C.
3. Digite os valores apropriados nos campos do diálogo.
4. Clique no botão **OK** para definir informações adicionais de CPI-C.

Configurando a LUA

A API LUA pode ser utilizada para aplicações que utilizam tipos de LU 0–3 para se comunicar com um computador do host. (Para obter informações detalhadas sobre a API LUA, consulte o *Communications Server for Linux LUA Programmer's Guide*.)

Antes de configurar a LUA, siga estas etapas de configuração:

1. Configure o nó, conforme descrito em “Configurando o Nó” na página 78.
2. Configure a conectividade para tráfego dependente, conforme descrito em “Configurando a Conectividade” na página 79. (Se você estiver utilizando o gateway SNA de envio de dados ou DLUR, configure o link para nó de envio de dados no lugar de link direto ao host).

Para configurar a LUA, você precisa das seguintes informações:

- Nome da LU ou nome do conjunto de LUs.
- Número de cada LU. O número da LU deve corresponder ao número de LU configurado no host.

Para configurar a LUA, defina a LU usando o seguinte procedimento:

1. Selecione a estação de link para o host no painel Conectividade da janela Nó.
2. Clique no botão **Novo**.
3. No diálogo resultante, selecione **Nova LU para LUA**.
4. Digite os valores apropriados nos campos do diálogo. Especifique um tipo de LU como Irrestrito.
5. Clique no botão **OK**. A LU é exibida no painel Conectividade da janela Nó, abaixo da estação de link para o host.
6. Se você for usar algum grupo de LU, defina-o conforme descrito em “Definindo um Conjunto de LUs” na página 92.

Definindo um Conjunto de LUs

Você pode definir conjuntos de LUs para simplificar a configuração do usuário e fornecer maior flexibilidade no estabelecimento de sessões do host. Por exemplo, você pode definir várias LUs em um único conjunto de LUs e, em seguida, configurar vários aplicativos LUA utilizando esse conjunto. Isso facilita a configuração dos aplicativos e permite que todos os aplicativos utilizem qualquer LU no conjunto.

Nota: Você pode atribuir uma sessão de usuário a uma LU específica ou a um conjunto de LUs.

- Se você atribuir a sessão do usuário a uma LU específica que está em um conjunto, a sessão utilizará essa LU se ela estiver disponível; do contrário, ela utilizará qualquer LU disponível do conjunto, embora você a tenha atribuído ao conjunto de LUs, em vez de uma LU específica.
- Se você desejar que o usuário utilize apenas uma LU especificada, de forma que a sessão do usuário não poderá ser estabelecida se a LU já estiver em uso, assegure-se de que a LU não esteja em um conjunto.

É possível visualizar os conjuntos de LUs para o nó local do Communications Server para Linux, utilizando a janela Conjunto de LUs. Essa janela lista os conjuntos de LUs configurados no sistema local e permite que você selecione LUs a serem incluídas em um conjunto de LUs.

Você pode incluir os seguintes tipos de LU em um conjunto a ser usado pelo 3270 (não misture LUs de tipos diferentes no mesmo conjunto):

- LU de tela 3270
- LU sem restrição

Para que você possa incluir LUs em um conjunto, as LUs devem ser definidas no nó local.

Para configurar um conjunto de LUs, siga estas etapas na janela Nó:

1. Selecione **Conjuntos de LUs** no menu **Janelas**.
O Communications Server para Linux exibe a janela Conjuntos de LUs.
2. Clique no botão **Novo**.
O Communications Server para Linux exibe o diálogo Configuração do Conjunto de LUs.
A caixa à direita lista as LUs que ainda não estão alocadas para um conjunto. Qualquer uma dessas LUs com tipo LU Irrestrita pode ser incluída no novo conjunto para LUA.
3. Selecione a LU ou LUs a serem incluídas no conjunto e clique no botão **Novo** para mover as LUs selecionadas para a caixa à esquerda.
Para remover uma LU da caixa à esquerda, selecione-a e clique no botão **Remover**.
4. Clique no botão **OK** para definir o conjunto de LUs.
Todas as LUs na caixa à esquerda são incluídas no conjunto de LUs.
O conjunto é exibido na janela Conjuntos de LUs.

Configurando o Gateway SNA

Além de fornecer acesso direto a um computador host, o Communications Server para Linux pode fornecer recursos do gateway SNA. Esse recurso permite que outros computadores acessem um computador host por meio de um nó do Communications Server para Linux, em vez de exigir uma conexão separada para o host a partir de cada computador.

O recurso de gateway SNA é mostrado na Figura 8.

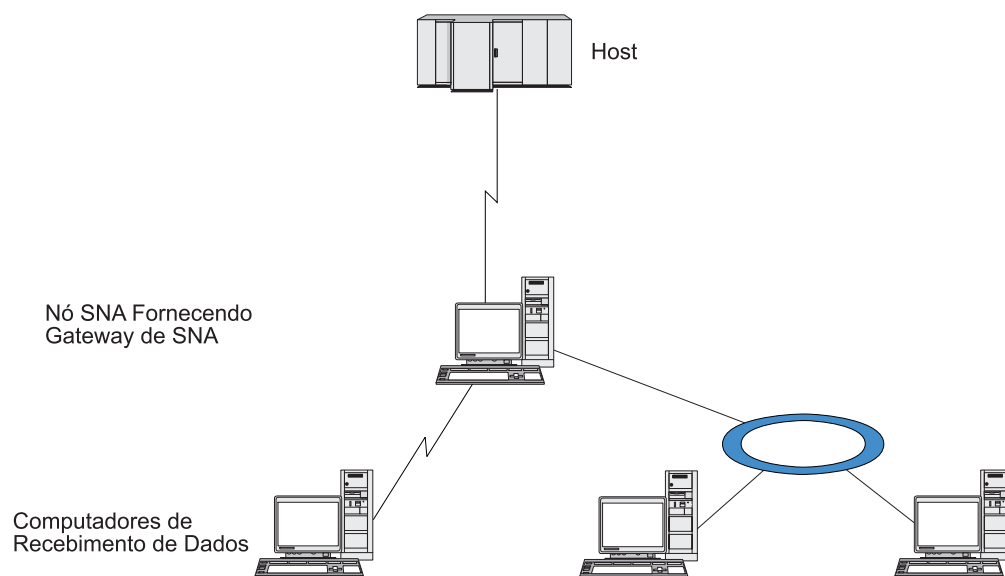


Figura 8. Gateway SNA

O computador de recebimento de dados deve conter uma PU SNA do tipo 2.0 ou 2.1 para suportar LUs dependentes. Por exemplo, o computador de recebimento de dados poderia ser outro computador Communications Server para Linux ou um PC executando o Communications Server para Windows.

Quando o nó local do Communications Server para Linux utiliza o recurso de gateway SNA, todos os dados transferidos entre o host e o computador de recebimento de dados são roteados por meio do nó local. Isso permite que um computador de recebimento de dados compartilhe uma conexão de host com o Communications Server para Linux ou com outros computadores de recebimento de dados, em vez de exigir um link direto. Por exemplo, você poderia configurar vários computadores de recebimento de dados conectados ao Communications Server para Linux por meio de uma rede Token Ring local, de modo a permitir acesso total à mesma linha dedicada do Communications Server para Linux para o host.

O uso do gateway SNA também simplifica a configuração no host, pois você não precisa definir os computadores de recebimento de dados e a linha de comunicação para eles. A configuração do host precisa incluir somente o computador Communications Server para Linux e seu link de comunicação do host; as LUs nos computadores de recebimento de dados são configuradas como parte dos recursos do computador Communications Server para Linux. O host não sabe que o gateway SNA está sendo usado.

Para que você possa configurar o gateway SNA, execute a seguinte configuração:

Configurando o Gateway SNA

- Defina o nó local, conforme descrito em “Configurando o Nó” na página 78.
- Configure uma porta e estação de link para tráfego dependente entre o nó local e o host, conforme descrito em “Configurando a Conectividade” na página 79. Além disso, configure portas e estações de link para tráfego dependente entre o nó local e os nós de recebimento de dados. Se você precisar suportar LUs de recebimento de dados que ainda não foram definidas, poderá definir um gabarito na porta para suportar PUs implícitas e LUs de recebimento de dados (consulte “Suportando LUs Implícitas de Recebimento de Dados”).
- Defina, no nó local, as LUs usadas para a comunicação com o host (LUs de envio de dados). Defina as LUs de envio de dados como LUs do tipo 0–3 com um tipo de LU Irrestrito (desconhecido). (As LUs nos nós de recebimento de dados podem ser de qualquer tipo).
- Se você for usar algum grupo de LU, defina-o conforme descrito em “Definindo um Conjunto de LUs” na página 92.

Suportando LUs Implícitas de Recebimento de Dados

Para dar suporte a LUs de recebimento de dados que não sejam predefinidas para o Communications Server para Linux, defina um gabarito na porta para PUs e LUs implícitas de recebimento de dados (com respeito à configuração da porta, consulte “Configurando a Conectividade” na página 79). Esses gabaritos fornecem suporte a LUs de recebimento de dados sem exigir que você configure uma LU no nó local para suportar todas as LUs em um nó de recebimento de dados.

Para configurar uma LU de recebimento de dados para o gateway SNA, você precisa das seguintes informações:

- Uma faixa de números de LU para suportar LUs de recebimento de dados.
- Nome da LU do host.

Para definir um gabarito para LUs implícitas de recebimento de dados, siga estas etapas:

1. Se você já tiver configurado a porta, clique duas vezes na definição da porta no painel Conectividade da janela Nó. O Communications Server para Linux exibe o diálogo da configuração da porta.

Se você ainda não tiver configurado a porta, faça isso agora:

- a. Selecione o painel Conectividade na janela Nó.
- b. Clique no botão **Novo**.
- c. No diálogo resultante, selecione para definir a porta e escolha o tipo de protocolo de link.

O Communications Server para Linux exibe o diálogo de configuração da porta.

- d. Digite os parâmetros básicos da porta, conforme descrito em “Configurando a Conectividade” na página 79.

2. Clique no botão **Avançado** na parte inferior do diálogo.

O Communications Server para Linux exibe o diálogo Parâmetros da Porta. O painel inferior mostra as definições que afetam gabaritos de LU de recebimento de dados.

3. Selecione a opção *Configurar LUs de Recebimento de Dados para Acesso Implícito à PU*.

4. Clique em **OK**.

O Communications Server para Linux exibe o diálogo Configuração do Gabarito da LU de Recebimento de Dados.

5. Digite os valores apropriados nos campos do diálogo.
6. Clique em **OK** para definir o gabarito de LU implícita de recebimento de dados.

Definindo LUs de Recebimento de Dados

Para configurar uma LU de recebimento de dados para o gateway SNA, você precisa das seguintes informações:

- Nome de cada LU de recebimento de dados. (Este é um identificador local e não precisa corresponder à configuração do sistema de recebimento de dados.)
- Número de cada LU de recebimento de dados.
- Estação de link para o nó de recebimento de dados.
- Nome de LU de envio de dados (para a LU de host).

Para configurar uma LU de recebimento de dados para o gateway SNA, siga estas etapas:

1. Selecione a estação de link para o nó de recebimento de dados no painel Conectividade da janela Nó.
2. Clique no botão **Novo**.
3. Selecione **Nova LU de Recebimento de Dados** e clique em **OK**.

O Communications Server para Linux exibe o diálogo LU de Recebimento de Dados.

4. Digite os valores apropriados nos campos do diálogo.
5. Clique em **OK** para definir a LU de recebimento de dados.

A definição da LU é exibida no painel Conectividade da janela Nó, abaixo da estação de link para o nó de recebimento de dados.

Configurando o DLUR

Além de fornecer acesso direto a um computador host, o Communications Server para Linux pode fornecer recursos de DLUR (Dependent LU Requester). Esse recurso permite que as sessões de LUs dependentes expandam vários nós em uma rede APPN em vez de exigir uma conexão direta ao host.

Normalmente, uma sessão de LU dependente exige um link de comunicação direto ao host. Se muitos nós (inclusive um nó de host) estiverem conectados juntos em uma rede APPN, alguns deles poderão não ter uma conexão direta ao host, mas somente uma conexão indireta através de outro nó. Não é possível estabelecer sessões de LU dependente com o host a partir de LUs nesses nós indiretamente conectados.

O solicitador de LU dependente (DLUR) é um recurso de APPN criado para superar essa limitação.

O DLUR em um nó APPN (por exemplo, um nó do Communications Server para Linux) trabalha em conjunto com o DLUS (Dependent LU Server) (DLUS) no host para direcionar sessões de LUs dependentes no nó DLUR através da rede APPN até o host DLUS. O percurso para o host pode expandir vários nós e tirar proveito do gerenciamento de rede, localização dinâmica de recursos e recursos de cálculo de percurso da APPN. O DLUR deve estar disponível no nó onde as LUs estão localizadas e o DLUS deve estar disponível no nó do host. Observe que o DLUR não é necessário em nenhum nó intermediário no percurso de sessão.

Configurando o DLUR

Se o nó DLUR do Communications Server para Linux for um nó de rede ou um Nó de Rede Derivado, também será possível fornecer recursos de DLUR de passagem para LUs dependentes nos computadores de recebimento de dados conectados ao nó Communications Server para Linux. Essas LUs podem utilizar o DLUR no nó do Communications Server para Linux para acessar o host por meio da rede, da mesma maneira que para LUs internas para o nó. Os computadores de recebimento de dados não precisam executar DLUR, e de fato não precisam estar cientes de que o DLUR está sendo utilizado.

A Figura 9 mostra um servidor Communications Server para Linux configurado como um nó de rede APPN, implementando o DLUR de passagem para dar suporte a sessões entre LUs no host (o nó de envio de dados) e as LUs nos nós na rede APPN (nós de recebimento de dados).

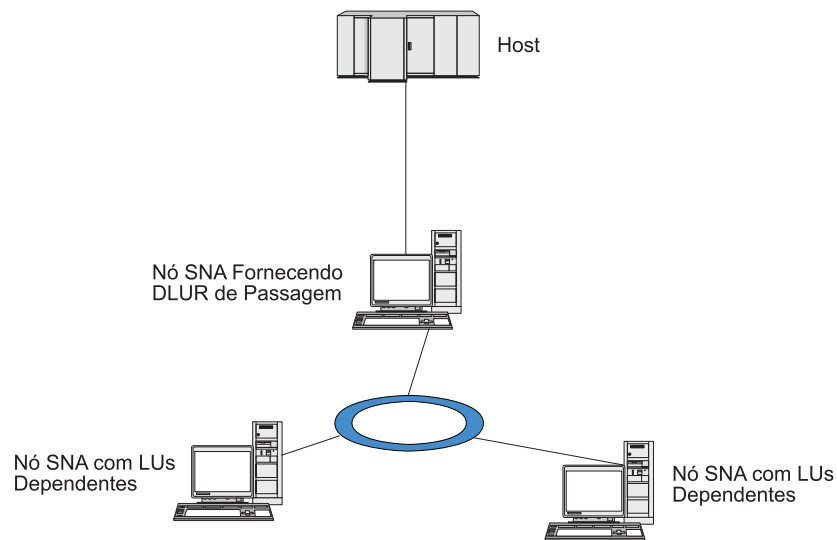


Figura 9. Nó Communications Server para Linux Fornecendo DLUR

Nota:

1. Você não pode configurar o DLUR em um nó LEN.
2. Você pode configurar o DLUR de passagem apenas em um nó de rede ou Nó de Rede de Ramificação.
3. Se estiver utilizando um Branch Extender, você não pode configurar o DLUR em um nó de extremidade na ramificação (com um Nós de Rede de Ramificação como seu servidor de nó de rede). Contudo, você pode suportar aplicações LU dependentes a partir deste nó configurando o DLUR de passagem no Nó de Rede de Ramificação (de forma que o nó de extremidade na ramificação não executa DLUR, mas utiliza o DLUR de passagem no Nó de Rede de Ramificação).

As tarefas que precisam ser executadas para configurar o DLUR dependem do fato de as LUs dependentes estarem no nó local ou em nós de recebimento de dados.

Configurando o Suporte DLUR no Nó Local

Você precisa das seguintes informações para essa tarefa:

- ID de PU para a PU no nó local.
- Nome da PU. (Este é um identificador local e não precisa corresponder à configuração do host.)

- Nome do DLUS no host (e o nome do DLUS de backup, se houver um).
- Nome, número e tipo da LU para cada LU de recebimento de dados. O número da LU deve corresponder ao número configurado no host.

Para configurar o suporte ao DLUR no nó local, execute estas tarefas de configuração:

1. Defina o nó local, conforme descrito em “Configurando o Nó” na página 78. Se você estiver fornecendo o suporte ao DLUR de passagem para nós de recebimento de dados, defina o nó como um nó de rede APPN ou um nó de rede de ramificação.
2. Configure a conectividade à rede APPN. A conectividade à APPN requer pelo menos uma porta e estação de link para tráfego independente entre o nó local e o nó de rede APPN adjacente, conforme descrito em “Configurando a Conectividade” na página 79.
3. Defina uma PU do DLUR no nó local (a PU do DLUR suporta conectividade ao host).

Para configurar a PU do DLUR, siga estas etapas na janela Nó:

- a. Selecione o menu **Serviços**, em seguida o submenu **Conectividade** e **Nova PU do DLUR** (ou clique no botão **Novo** na barra de botões, então selecione **PU do DLUR**).

Ao clicar no botão **OK**, o Communications Server para Linux exibe o diálogo Configuração da PU do DLUR.

- b. Digite os valores apropriados nos campos do diálogo.
- c. Clique no botão **OK** para definir a LU do DLUR.

A PU do DLUR é exibida no painel Conectividade abaixo do item DLUR.

4. Para configurar o DLUR para suportar LUs no nó local, inclua as LUs no nó local. As LUs devem ser configuradas para dar suporte ao LUA, conforme descrito em “Configurando a LUA” na página 91. Dependendo dos requisitos dos aplicativos do usuário suportados pelas LUs, pode ser necessário executar configuração adicional.

Configurando o Suporte DLUR de Passagem para Nós de Recebimento de Dados

Você precisa das seguintes informações para essa tarefa:

- Nome da PU de recebimento de dados para cada nó de recebimento de dados ou para cada PU no nó de recebimento de dados. (Este é um identificador local e não precisa corresponder à configuração do host.)
- Nome do DLUS no host.

Para configurar o suporte ao DLUR de passagem para nós de recebimento de dados, execute estas tarefas de configuração:

1. Defina o nó local como um nó de rede APPN (consulte “Configurando o Nó” na página 78).
2. Configure a conectividade aos nós de recebimento de dados. Configure portas e estações de link para o tráfego dependente entre o nó local e cada nó de recebimento de dados, conforme descrito em “Configurando a Conectividade” na página 79. (Você não precisa definir uma PU do DLUR para suportar DLUR de passagem para nós de recebimento de dados).
3. Um nó de recebimento de dados pode suportar várias PUs. Nesse caso, cada PU de recebimento de dados será associada a um link diferente, portanto, você

Configurando o DLUR

precisará de vários links entre o nó DLUR do Communications Server para Linux e o nó de recebimento de dados, além de conhecer o nome da PU de recebimento de dados de cada link.

Configurando o Servidor TN

Os programas de emulação do 3270 que se comunicam em TCP/IP (em vez de em uma rede SNA) são chamados de programas TN3270 (programas de emulação do Telnet 3270).

Os programas TN3270 também podem incluir suporte ao TN3270E (extensões padrão do Telnet 3270). O TN3270E é um protocolo aberto que suporta a emulação de dispositivos 3270 (inclusive terminais e impressoras) usando Telnet. Permite que um cliente de Telnet selecione um determinado dispositivo (especificando o nome da LU) e fornece suporte avançado para várias funções, inclusive as chaves ATTN e SYSREQ e o tratamento de respostas do SNA.

Nota: Este manual usa o termo TN3270 para informações que se aplicam aos protocolos TN3270, TN3287 e TN3270E.

O servidor TN do Communications Server para Linux fornece acesso a computadores host 3270 para usuários TN3270 em outros computadores. O servidor TN permite que usuários TN3270 compartilhem uma conexão de host com o Communications Server para Linux ou com outros usuários TN3270, em vez de requerer um link direto. O Servidor TN também permite que usuários do TN3270 acessem hosts que não estejam executando o TCP/IP.

Um nó Communications Server para Linux que fornece suporte ao Servidor TN para clientes TN3270 é mostrado na Figura 10. O nó do Servidor TN e os clientes se comunicam através da rede TCP/IP.

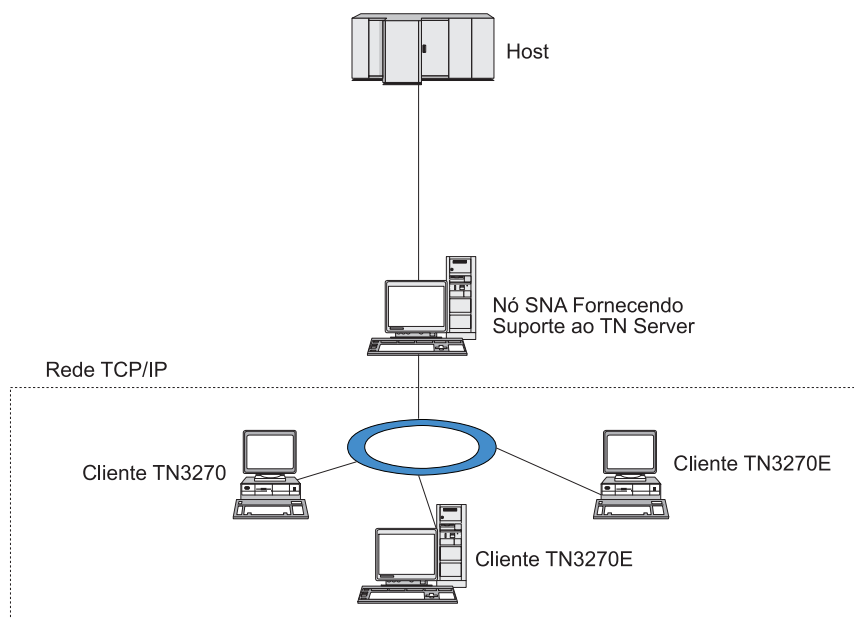


Figura 10. Nó Communications Server para Linux Configurado para Servidor TN

O recurso do servidor TN do Communications Server para Linux fornece uma associação entre um usuário TN e a LU 3270 do Communications Server para

Linux. Todos os dados do usuário de TN3270 são direcionados para a LU. Isso significa que a configuração do host e do usuário de TN3270 é feita como se eles fossem conectados diretamente; nenhum dos dois precisa saber que os dados estão sendo direcionados através do Servidor TN.

O servidor TN do Communications Server para Linux suporta todos os programas da emulação cliente TN3270 que implementam corretamente os protocolos definidos nos RFCs 1123, 1576, 1646, 1647 e 2355 do IETF.

Quando um programa TN3270 se comunica com o Servidor TN, o Communications Server para Linux identifica o programa pelo endereço TCP/IP do computador no qual o programa TN3270 está sendo executado. O Communications Server para Linux não pode distinguir entre dois programas TN3270 diferentes que estejam sendo utilizados por usuários diferentes no mesmo computador. Nos manuais do Communications Server para Linux, o termo usuário do Servidor TN refere-se ao computador em que um programa TN3270 está sendo executado, e não a um usuário individual desse programa.

Conforme mostrado na Figura 11, o host e o usuário do Servidor TN exibem a configuração do Servidor TN diferentemente.

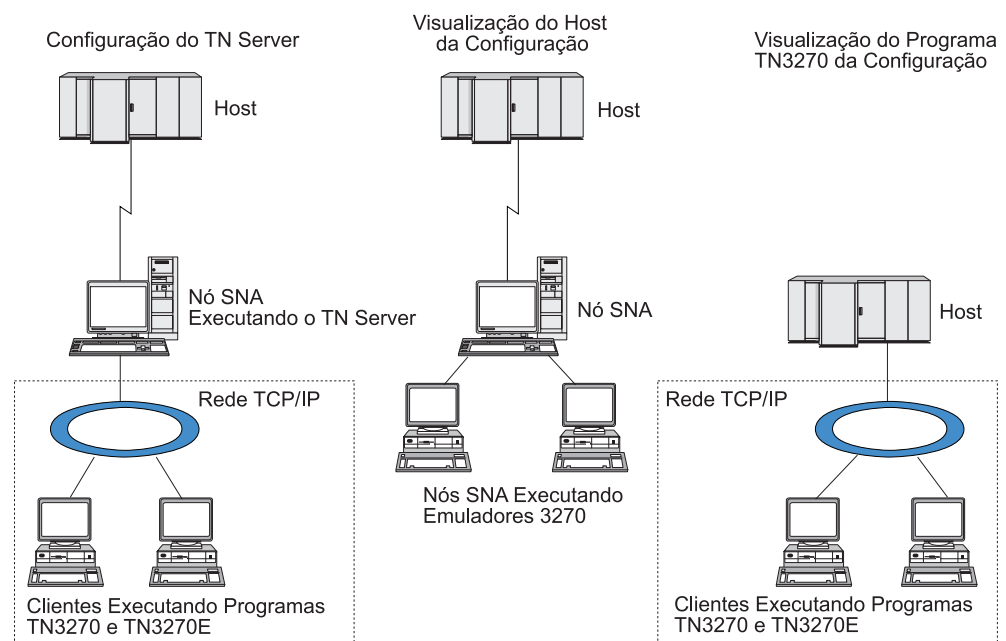


Figura 11. Servidor TN

Cada usuário do Servidor TN conectado ao Communications Server para Linux que esteja utilizando o recurso TN3270 Server está configurado, normalmente, para acessar uma única LU 3270 e, portanto, restrito a uma única sessão do host por vez. No entanto, você também pode configurar um usuário do Servidor TN para acessar um conjunto de LUs 3270, em vez de ter uma única LU 3270 dedicada para cada usuário. Isso permite que os usuários acessem o mesmo número de sessões que o número de LUs disponíveis no conjunto.

Para configurar o acesso ao Servidor TN, execute estas tarefas de configuração:

- Defina o nó local, conforme descrito em “Configurando o Nó” na página 78.

Configurando o Servidor TN

- Configure uma porta e estação de link para tráfego dependente entre o nó local e o host, conforme descrito em “Configurando a Conectividade” na página 79.

Para configurar o acesso do Servidor TN, execute as seguintes tarefas de configuração:

- Defina as LUs 3270 no nó local, usadas para a comunicação com o host. Para incluir LUs, consulte “Definindo LUs 3270”.
- Se você for usar algum grupo de LU, defina-o conforme descrito em “Definindo um Conjunto de LUs”.

Definindo LUs 3270

Antes de configurar a LU de 3270, obtenha as seguintes informações:

- Nome da LU. (Este é um identificador local e não precisa corresponder à configuração do host.)
- Número da LU (ou números de uma faixa de LUs).
- Tipo de LU (modelo de tela 3270 ou impressora 3270).
- Nome do conjunto (se você estiver incluindo a LU em um conjunto).

Para configurar uma LU dos tipos 0–3 para uma estação de link definida anteriormente, siga estas etapas na janela Nó:

1. Selecione a estação de link para o host no painel Conectividade da janela.
2. Clique no botão **Novo**.
3. Selecione o tipo de LU (**Nova LU de Vídeo 3270** ou **Nova LU de Impressora 3270**) no diálogo resultante.

Ao selecionar esse item e clicar em **OK**, o Communications Server para Linux exibirá o diálogo Tipo de LU 0–3.

4. Digite os valores apropriados nos campos do diálogo.
5. Clique no botão **OK** para definir a LU.

A LU é exibida no painel Conectividade da janela Nó, abaixo da estação de link para o host.

Definindo um Conjunto de LUs

Para o 3270, você pode definir conjuntos de LUs de modo a simplificar a configuração do usuário e fornecer maior flexibilidade no estabelecimento de sessões do host. Por exemplo, você pode definir várias LUs 3270 em um único conjunto de LUs e, em seguida, configurar vários clientes TN3270 que utilizam esse conjunto de LUs. Isso facilita a configuração das sessões de 3270 e permite que qualquer cliente utilize qualquer LU no conjunto.

Nota: Você pode atribuir um cliente TN3270 a uma LU específica ou a um conjunto de LUs.

- Se você atribuir o cliente a uma LU específica que está em um conjunto, o cliente utilizará essa LU se ela estiver disponível; do contrário, ele utilizará qualquer LU disponível do conjunto, embora você o tenha atribuído ao conjunto de LUs, em vez de a uma LU específica.
- Se você desejar que o cliente utilize apenas uma LU especificada, de forma que a sessão do cliente não poderá ser estabelecida se a LU já estiver em uso, assegure-se de que a LU não esteja em um conjunto.

É possível visualizar os conjuntos de LUs para o nó local do Communications Server para Linux, utilizando a janela Conjunto de LUs. Essa janela lista os

conjuntos de LUs configurados no sistema local e permite que você selecione LUs a serem incluídas em um conjunto de LUs.

Você pode incluir os seguintes tipos de LU em um conjunto a ser usado pelo 3270 (não misture LUs de tipos diferentes no mesmo conjunto):

- LU de tela 3270
- LU sem restrição

Para que você possa incluir LUs em um conjunto, as LUs devem ser definidas no nó local.

Para configurar um conjunto de LUs, siga estas etapas na janela Nó:

1. Selecione **Conjuntos de LUs** no menu **Janelas**.
O Communications Server para Linux exibe a janela Conjuntos de LUs.
2. Clique no botão **Novo**.
O Communications Server para Linux exibe o diálogo Configuração do Conjunto de LUs.
A caixa à direita lista as LUs que ainda não estão alocadas para um conjunto. Qualquer uma delas pode ser incluída no novo conjunto.
3. Selecione a LU ou LUs a serem incluídas no conjunto e clique no botão **Novo** para mover as LUs selecionadas para a caixa à esquerda.
Para remover uma LU da caixa à esquerda, selecione-a e clique no botão **Remover**.
4. Clique no botão **OK** para definir o conjunto de LUs.
Todas as LUs na caixa à esquerda são incluídas no conjunto de LUs.
O conjunto é exibido na janela Conjuntos de LUs.

Configurando o TN3270 Server

Antes de configurar o TN3270 Server, você precisa das seguintes informações:

- Se o servidor suporta somente o TN3270 ou também o TN3270E (que inclui suporte ao TN3270).
- Se o cliente do TN3270E pode solicitar uma LU específica.
- Nomes de LUs de tela e de impressora (ou nomes de conjuntos de LUs) de cada cliente. (Os nomes de LU de impressora só serão necessários se o TN3270E for suportado).
- Se apenas determinados clientes forem permitidos ou se desejar limitar certos clientes para LUs específicas, você precisará do nome ou endereço TCP/IP do cliente.
- Número da porta TCP/IP no nó do Servidor TN.
- Se a criptografia de dados SSL, autenticação de cliente e autenticação de servidor são requeridos (esta opção está disponível apenas se você instalou o software adicional requerido para suportá-los).

Para associar uma LU de tela e uma LU de impressora, você também precisa dos nomes dessas LUs. O registro de associação de um Servidor TN define uma associação entre uma LU de impressora e uma LU de tela de modo que o protocolo TN3270E possa conectar as duas. Não é preciso definir um registro de associação se o TN3270E ou as LUs de impressora não estiverem sendo suportados.

Configurando o Servidor TN

O registro de padrões do Servidor TN define os parâmetros usados em todas as sessões de cliente do TN3270. Você pode definir um único registro de padrões para cada servidor.

Para configurar o TN3270 Server, execute as seguintes etapas da janela Nó:

1. Defina o registro de acesso ao Servidor TN:
 - a. Selecione **Servidor TN** no menu **Serviços**.
O Communications Server para Linux exibe a janela Servidor TN, que lista todos os registros configurados de acesso ao Servidor TN na área de janela superior e os registros de associação do Servidor TN na área de janela inferior.
 - b. Selecione o painel que contém os registros de acesso do TN3270 Server e clique no botão **Novo**.
O Communications Server para Linux exibe o diálogo Acesso do Servidor TN.
 - c. Digite os valores apropriados nos campos do diálogo.
 - d. Clique em **OK** para definir o registro de acesso ao Servidor TN. O registro é exibido na janela Servidor TN.
2. Defina o registro de associação do Servidor TN:
 - a. Selecione o painel que contém registros de associação na janela Servidor TN e clique no botão **Novo**.
O Communications Server para Linux exibe o diálogo Registro da Associação do Servidor TN.
 - b. Digite os valores apropriados nos campos do diálogo.
 - c. Clique em **OK** para definir o registro de associação do Servidor TN. O registro é exibido na janela Servidor TN.
3. Para forçar respostas na impressora, especifique um método keep alive para sessões do TN3270, especifique como acessar o servidor LDAP externo que mantém uma lista de revogação utilizada para verificar autorização para clientes TN3270, ou utilize o TN3270 SLP (Service Location Protocol), utilize o diálogo Parâmetros Avançados do Servidor TN para tal.

Para obter mais informações sobre como configurar o suporte a SSL para o Servidor TN, consulte as páginas de Suporte do IBM Communications Server na Web, em <http://www.ibm.com/software/network/commsserver/support/>.

Configurando o Redirecionador TN

O recurso Redirecionador TN do Communications Server para Linux fornece acesso ao host do TCP/IP de passagem para clientes TN3270, TN3270E, TN5250 e VT; chamados coletivamente de clientes Telnet. O usuário da Telnet se comunica com o Communications Server para Linux por uma conexão TCP/IP; o Communications Server para Linux se comunica com o host por outra conexão TCP/IP. Isso permite que você utilize a verificação de segurança SSL (Secure Sockets Layer) quando necessário, não a conexão completa usuário para host. Por exemplo:

- Se os clientes estiverem se conectando ao Communications Server para Linux por uma LAN TCP/IP que não requer verificação, mas se conectarem a um host remoto que requeira SSL, você poderá utilizar o SSL por uma conexão TCP/IP entre o Communications Server para Linux e o host. Isso significa que a segurança é verificada apenas uma vez para cliente, e clientes individuais não precisam fornecer informações de segurança.

- Se o Communications Server para Linux estiver instalado no mesmo site que o host, mas os clientes estiverem se conectando a partir de sites externos, será possível utilizar SSL por meio das conexões do cliente para o Communications Server para Linux sem ser preciso instalar o software SSL no host.

Configurando o Redirecionador TN

Antes que você possa configurar o acesso Redirecionador TN, você deve definir o nó local conforme descrito na seção “Configurando o Nó” na página 78. Você também precisa das seguintes informações:

- Se apenas certos clientes são permitidos, você precisa do nome ou endereço TCP/IP do cliente.
- O número da porta TCP/IP utilizado pelo cliente para conectar o nó do Redirecionador TN.
- Nome ou endereço TCP/IP do host.
- Número da porta TCP/IP utilizado pelo nó Redirecionador TN para conectar ao host.
- Se a criptografia de dados SSL, autenticação de cliente e autenticação de servidor são requeridos entre o cliente e o nó do Redirecionador TN (esta opção está disponível apenas se você instalou o software adicional requerido para suportá-los).
- Se a criptografia de dados SSL é requerida entre o nó Redirecionador TN e o host.

Os registros padrão do Redirecionador TN definem os parâmetros que são utilizados em todas as sessões do cliente Redirecionador TN. Você pode definir um único registro padrão para cada número de porta TCP/IP cliente.

Para configurar o Redirecionador TN, execute as seguintes etapas da janela Nó para definir o registro de acesso do Redirecionador TN:

1. Selecione **Servidor TN** no menu **Serviços**.
O Communications Server para Linux exibe a janela Servidor TN, que lista todos os registros configurados de acesso ao TN3270 Server, os registros de associação do TN3270 Server e registros de acesso ao Redirecionador TN.
2. Selecione o painel que contém os registros de acesso do Redirecionador TN e clique no botão **Novo**.
O Communications Server para Linux exibe o diálogo Acesso do Redirecionador TN.
3. Digite os valores apropriados nos campos do diálogo.
4. Clique em **OK** para definir o registro de acesso ao Redirecionador TN. O registro aparece no painel Redirecionador TN da janela Servidor TN.

Nota: O nó SNA deve estar ativo para utilizar o Redirecionador TN, embora ele não utilize nenhum dos recursos SNA do nó.

Desativando o Communications Server para Linux

A desativação do software Communications Server para Linux pára automaticamente o nó do Communications Server para Linux e seus componentes de conectividade associados. A desativação do Communications Server para Linux também impede quaisquer outros processos (por exemplo, um aplicativo LUA) de utilizar recursos do Communications Server para Linux nesse servidor.

Desativando o Communications Server para Linux

Em geral, os serviços individuais devem ser parados assim que os usuários deixam de utilizá-los, e desativados apenas quando não há nenhuma atividade no Communications Server para Linux.

Para desativar o Communications Server para Linux enquanto os usuários estão ativos, avise-os de que está parando o Communications Server para Linux e conceda-lhes tempo para concluírem suas atividades antes da desativação do software.

Ao desativar o software Communications Server para Linux, os aplicativos que utilizam as APIs APPC, CSV, LUA, NOF ou MS são notificados por um código de retorno COMM_SUBSYSTEM_ABENDED e os aplicativos CPI-C por um código de retorno CM_PRODUCT_SPECIFIC_ERROR.

Para desativar o software Communications Server para Linux, insira o seguinte comando no prompt de comandos do Linux:

```
sna stop
```

Se o Communications Server para Linux for desativado com êxito, o **sna stop** retornará um código de saída igual a 0. Qualquer outro código de saída indicará a ocorrência de um erro e que o software Communications Server para Linux não foi desativado. Consulte o *Communications Server para Linux - Guia de Diagnósticos* para obter informações adicionais sobre os valores de código de saída.

Iniciando o Communications Server para Linux Automaticamente

Colocar o Communications Server para Linux no status pleno de funcionamento envolve várias etapas:

- Ativar o software Communications Server para Linux
- Inicializar o nó SNA
- Ativar as portas e as estações de link configuradas no nó.

Cada uma dessas etapas pode ser gerenciada separadamente, e todas as etapas podem ser executadas no momento da inicialização, se necessário. O restante desta seção descreve essas etapas e explica como controlá-las no momento da inicialização.

Ativando o Communications Server para Linux

Communications Server para Linux requer que vários módulos de kernel sejam carregados para operar. Esses módulos serão carregados ao ativar o software Communications Server para Linux pela primeira vez, e descarregados apenas quando o nível de execução do kernel for alterado.

O Communications Server para Linux também requer a execução de vários daemons (programas). Até que estejam em execução, não será possível configurar ou utilizar o Communications Server para Linux.

- Para iniciar os daemons e ativar o software Communications Server para Linux, emita o comando **sna start**.
- Para parar os daemons e desativar o software Communications Server para Linux, emita o comando **sna stop**.

Inicializando o Nó SNA

Quando o software Communications Server para Linux tiver sido ativado, você poderá configurar o nó SNA e seus recursos, geralmente utilizando o programa de administração Motif `x snaadmin`. No entanto, o nó não está disponível para ser utilizado até o software ser inicializado. Você pode inicializá-lo a partir do programa de administração da linha de comandos, utilizando o comando `snaadmin init_node`, ou a partir do programa de administração Motif `x snaadmin`.

Ativando Portas e Estações de Link

As portas e estações de link podem ser configuradas para iniciar em diferentes circunstâncias:

- Somente por intervenção do operador
- Sob pedido (quando um aplicativo é iniciado utilizando um recurso no link)
- Na inicialização do nó (quando o comando `snaadmin init_node` é emitido ou quando o nó é iniciado a partir do programa de administração Motif).

Iniciar por intervenção do operador é o padrão, mas você pode alterar esta opção para uma porta ou link específico, utilizando o programa de administração de linha de comandos ou o programa de administração Motif.

Nota: A inicialização de uma porta permite que ela receba chamadas de outros computadores, mas não permite que faça chamadas externas. Iniciar uma estação de link significa que o Communications Server para Linux tenta entrar em contato com o computador remoto.

Iniciando o Communications Server para Linux na Reinicialização

Assim como outros serviços do Linux, o Communications Server para Linux é ativado na inicialização. Em outras palavras, por padrão, após uma reinicialização, o comando `sna start` é emitido, mas o nó SNA não é iniciado.

Isso é feito no script de inicialização do Communications Server para Linux, `/etc/rc.d/init.d/snastart`. Como é convencional para scripts de inicialização, isso está vinculado a `/etc/rc?.d/init.d/snastart` para os vários níveis de reinicialização.

Você pode editar `/etc/rc.d/init.d/snastart` para alterar o que ocorre na reinicialização. A alteração mais comum é incluir a inicialização do nó. O comando para isso, `snaadmin init_node`, já está incluído no arquivo, mas há um comentário. Dessa forma, você simplesmente precisa excluir o comentário. Ao incluir esse comando, você também aciona a ativação de quaisquer portas ou estações de link configuradas para serem ativadas na inicialização do nó.

Os aplicativos que utilizam o Communications Server para Linux não devem ser iniciados até que o nó tenha sido inicializado. Se necessário, você pode iniciar esses aplicativos automaticamente no momento da inicialização e incluir todos os outros comandos `snaadmin` que precisa executar no momento da inicialização de uma das duas maneiras:

- Inclua comandos no final de `/etc/rc.d/init.d/snastart`, após o comando `snaadmin init_node`.
- Crie um script `/etc/rc?.d/init.d` com um número maior que 95, garantindo que ele será executado após o início do Communications Server para Linux, e inclua os comandos nesse script.

Iniciando o Communications Server para Linux Automaticamente

Nota: As alterações feitas no arquivo `/etc/rc.d/init.d/snastart` não serão salvas ao fazer upgrade do Communications Server para Linux para uma versão posterior. Sempre guarde uma cópia de suas alterações, para que possa replicá-las após um upgrade.

Capítulo 9. Recursos de Informações do Communications Server para Linux e SNA

Este capítulo descreve os recursos na biblioteca SNA que fornecem informações sobre a tecnologia SNA e os muitos produtos e serviços de rede que a IBM oferece. Também descreve informações que estão disponíveis nos fóruns de rede.

Biblioteca SNA

A biblioteca SNA inclui folhetos de marketing, manuais, manuais do usuário e tutoriais que fornecem informações introdutórias e mais aprofundadas sobre os seguintes tópicos:

- Teoria do SNA
- Produtos do SNA
- Implementação do produto
- Configuração dos sistemas e redes
- Programas aplicativos SNA e APIs
- Planejamento geral, desempenho e ajuste.
- Diagnóstico de problemas
- Gerenciamento de rede
- Segurança da rede

Todas as publicações IBM podem ser solicitadas através de um representante IBM, da assistência técnica autorizada IBM em sua localidade ou ligando para a IBM diretamente no telefone 1-800-879-2755.

Para obter informações sobre publicações adicionais, entre em contato com um representante IBM.

Informações Acessíveis pela Rede

Para promover a troca de informações, a IBM patrocina fóruns eletrônicos e BBS. Ela coloca home pages na Internet e fornece documentação on-line, que também pode ser acessada na World Wide Web.

Suporte ao Produto através do IBMLink

O fórum IBMLink é mantido em redes pertencentes à IBM. É projetado para ajudar os clientes que possuem produtos IBM licenciados a resolverem problemas técnicos e outros problemas relacionados ao sistema e à rede. A equipe da IBM responde perguntas e media discussões on-line entre clientes IBM.

Para obter mais informações sobre o IBMLink, utilize <http://www.ibm.com>.

Informações nas Home Pages da IBM

Na Internet, várias home pages IBM fornecem acesso a fóruns. Para obter ajuda abrangente, a home page principal da IBM pode ser utilizada para navegar para os centros de informações na Internet e na World Wide Web. A home page principal pode ser acessada pelo endereço <http://www.ibm.com>.

Informações Acessíveis pela Rede

É possível acessar informações sobre o software de rede da IBM, incluindo o Communications Server para Linux, em <http://www.ibm.com/software/network>. Informações sobre o Communications Server para Linux estão localizadas em <http://www.ibm.com/software/network/commsserver>.

A fim de obter informações mais detalhadas sobre o suporte para o Communications Server para Linux, visite <http://www.ibm.com/software/network/commsserver/support>.

Informações para Download

Na World Wide Web, os usuários podem fazer download de publicações Redbook utilizando o endereço <http://www.redbooks.ibm.com>.

Informações sobre o software IBM podem ser acessadas em <http://www.ibm.com/software>; nesse site é possível acessar links para páginas sobre o Communications Server para Linux e para todos os outros Servidores de Software IBM.

Leitura Sugerida

Para aqueles que desejam reforçar seu entendimento sobre SNA, os manuais a seguir abordam a teoria do SNA e a utilização do Communications Server para Linux na prática. Os manuais são úteis tanto para pessoas inexperientes como para o pessoal bem treinado, que podem começar a se familiarizarem com o SNA ou obter um conhecimento mais profundo sobre o assunto.

- *Systems Network Architecture: Technical Overview* (GC30-3073)
- *IBM Communications Server for Administration Guide*

Se você tiver interesses mais específicos, entre em contato com o representante IBM local.

Apêndice. Avisos

Esta informações foram desenvolvidas para produtos e serviços oferecidos nos Estados Unidos. É possível que a IBM não ofereça os produtos, serviços ou recursos discutidos nesta publicação em outros países. Consulte um representante IBM local para obter informações sobre produtos e serviços disponíveis atualmente em sua área. Qualquer referência a produtos, programas ou serviços IBM não significa que apenas produtos, programas ou serviços IBM possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM ou quaisquer outros direitos da IBM, poderá ser utilizado em substituição a este produto, programa ou serviço. Entretanto, a avaliação e verificação da operação de qualquer produto, programa ou serviço não-IBM são de responsabilidade do Cliente.

A IBM pode ter patentes ou solicitações de patentes pendentes relativas a assuntos relativas a assuntos tratados nesta publicação. O fornecimento desta publicação não garante ao Cliente nenhum direito sobre tais patentes. Pedidos de licença devem ser enviados, por escrito, para:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
Botafogo
Rio de Janeiro, RJ
CEP: 22290-240

Para pedidos de licenças com relação a informações sobre DBCS (Conjunto de Caracteres de Byte Duplo), entre em contato com o Departamento de Propriedade Intelectual da IBM em seu país ou envie pedidos, por escrito, para:

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

O parágrafo a seguir não se aplica a nenhum país em que tais disposições não estejam de acordo com a legislação local: A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO “NO ESTADO EM QUE SE ENCONTRA” SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS NÃO SE LIMITANDO ÀS GARANTIAS IMPLÍCITAS DE MERCADO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns países não permitem a exclusão de garantias expressas ou implícitas em certas transações; portanto, essa disposição pode não se aplicar ao Cliente.

Esta publicação pode conter imprecisões técnicas ou erros tipográficos. Periodicamente, são feitas alterações nas informações aqui contidas; tais alterações serão incorporadas em novas edições da publicação. A IBM pode, a qualquer momento, aperfeiçoar e/ou alterar os produtos e/ou programas descritos nesta publicação, sem aviso prévio.

Referências nestas informações a Web sites não-IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a esses Web sites. Os materiais contidos nesses Web sites não fazem parte dos materiais deste produto IBM e a utilização desses sites da Web é de inteira responsabilidade do Cliente.

A IBM pode utilizar ou distribuir as informações fornecidas da forma que julgar apropriada sem incorrer em qualquer obrigação para com o Cliente.

Licenciados deste programa que desejam obter informações sobre este assunto com objetivo de permitir: (i) a troca de informações entre programas criados independentemente e outros programas (incluindo este) e (ii) a utilização mútua das informações trocadas, devem entrar em contato com:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
Botafogo
Rio de Janeiro, RJ
CEP: 22290-240

Tais informações podem estar disponíveis, sujeitas a termos e condições apropriadas, incluindo em alguns casos o pagamento de uma taxa.

O programa licenciado descrito nestas informações e todos os materiais licenciados disponíveis para ele são fornecidos pela IBM sob os termos do Contrato do Cliente IBM, do Contrato de Licença de Programa Internacional IBM ou de qualquer contrato equivalente.

Os dados de desempenho aqui contidos foram determinados em um ambiente controlado. Portanto, os resultados obtidos em outros ambientes operacionais podem variar significativamente. Algumas medidas podem ter sido tomadas em sistemas de nível de desenvolvimento e não há garantia de que estas medidas serão iguais em sistemas geralmente disponíveis. Além disso, algumas medidas podem ter sido estimadas por extrapolação. Os resultados reais podem variar. Os usuários deste documento devem verificar os dados aplicáveis para seu ambiente específico.

As informações relativas a produtos não-IBM foram obtidas junto aos fornecedores dos respectivos produtos, de seus anúncios publicados ou de outras fontes disponíveis publicamente. A IBM não testou estes produtos e não pode confirmar a precisão de desempenho, compatibilidade ou qualquer outra reivindicação relacionada a produtos de terceiros. As dúvidas sobre os recursos dos produtos não-IBM devem ser encaminhadas aos fornecedores desses produtos.

Estas informações contêm exemplos de dados e relatórios utilizados nas operações diárias de negócios. Para ilustrá-los da forma mais completa possível, os exemplos podem incluir nomes de indivíduos, empresas, marcas e produtos. Todos esses nomes são fictícios e qualquer semelhança com os nomes e endereços utilizados por uma empresa real é mera coincidência.

LICENÇA DE COPYRIGHT: Estas informações contêm programas de aplicativos de exemplo na linguagem fonte, ilustrando as técnicas de programação em diversas plataformas operacionais. Você pode copiar, modificar e distribuir estes programas de amostra em qualquer formato sem pagamento a IBM, para fins de desenvolvimento, utilização, marketing ou distribuição de programas aplicativos que estejam de acordo com a interface de programação do aplicativo para a plataforma operacional para qual os programas de amostra foram desenvolvidos. Esses exemplos não foram testados completamente em todas as condições. A IBM, portanto, não pode garantir ou implicar confiabilidade, manutenção, ou função destes programas. O Cliente pode copiar, modificar e distribuir estes programas de amostra de qualquer forma, sem pagamento à IBM, com objetivo de desenvolver, utilizar, fazer marketing ou distribuir programas aplicativos de acordo com as interfaces de programação de aplicativos da IBM.

Cada cópia ou parte destes programas de exemplo ou qualquer trabalho derivado deve incluir um aviso de copyright com os dizeres: ® (nome da empresa) (ano). Partes desse código originam-se dos Programas de Amostra da IBM Corp. ® Copyright International Business Machines Corporation. 1998, 2007. Todos os direitos reservados.

Marcas Registradas

Os seguintes termos são marcas registradas da IBM Corporation nos Estados Unidos e/ou em outros países:

Advanced Peer-to-Peer Networking	OpenPower
AIX	Operating System/2
Application System/400	Operating System/400
AS/400	OS/2
CICS	OS/400
DB2	POWERS
Enterprise System/3090	PowerPC
Enterprise System/4381	PowerPC Architecture
Enterprise System/9000	pSeries
ES/3090	S/390
ES/9000	SAA
eServer	System p5
IBM	System z
IBMLink	System/390
IMS	VSE/ESA
Language Environment	VTAM
MQSeries	WebSphere
MVS	z/OS
MVS/ESA	z9
	zSeries

Os termos a seguir são marcas ou marcas registradas de outras empresas:

Java e todas as marcas registradas baseadas em Java são marcas registradas da Sun Microsystems, Inc., nos Estados Unidos e/ou em outros países.

UNIX é uma marca registrada nos Estados Unidos e em outros países, licenciada exclusivamente pelo The Open Group.

Intel e EM64T são marcas registradas da Intel Corporation.

AMD64 é uma marca registrada da Advanced Micro Devices, Inc.

Linux é uma marca registrada da Linus Torvalds.

RedHat e RPM são marcas registradas da Red Hat, Inc.

SuSE Linux é uma marca registrada da Novell.

Microsoft, Windows, Windows 2003, Windows XP, Windows Vista e o logotipo Windows são marcas registradas da Microsoft Corporation nos Estados Unidos e/ou em outros países.

Outros nomes de empresas, produtos e serviços podem ser marcas registradas ou marcas de serviço de terceiros.

Bibliografia

As seguintes publicações da IBM fornecem informações sobre os tópicos abordados nesta biblioteca. As publicações estão divididas nos seguintes tópicos:

- Communications Server para Linux, Versão 6.2.3
- SNA (Systems Network Architecture)
- Configuração do Host
- z/OS Communications Server
- TCP/IP (Transmission Control Protocol/Internet Protocol)
- X.25
- APPC (Advanced Program-to-Program Communication)
- Programação
- Outros tópicos sobre redes IBM

São fornecidas breves descrições dos manuais na biblioteca do Communications Server para Linux. Para outros manuais, são apresentados aqui apenas títulos, números de pedido e, em alguns casos, o título abreviado utilizado no texto deste manual.

Publicações do Communications Server para Linux Versão 6.2.3

A biblioteca do Communications Server para Linux é composta dos seguintes manuais. Além disso, versões em cópia eletrônica desses documentos são fornecidas no CD-ROM. Consulte *IBM Communications Server for Linux Quick Beginnings* para obter informações sobre como acessar os arquivos de cópia eletrônica no CD-ROM. Para instalar esses manuais em cópia eletrônica no sistema, você precisa de 9–15 MB de espaço em disco (dependendo de qual versão de idioma você instalará).

- *IBM Communications Server para Linux: Iniciação Rápida* ()
Esse manual é uma introdução geral ao Communications Server para Linux e inclui informações sobre as características de rede suportadas, instalação, configuração e operação.
- *IBM Communications Server para Linux: Guia de Administração* ()
Esse manual fornece uma visão geral do SNA e do Communications Server para Linux e informações sobre a configuração e a operação do Communications Server para Linux.
- *IBM Communications Server para Linux: Referência do Comando de Administração* ()
Esse manual fornece informações sobre os comandos do SNA e do Communications Server para Linux.
- *IBM Communications Server para Linux: Guia do Programador de CPI-C* ()
Esse manual fornece informações para programadores experientes em “C” ou Java sobre como gravar programas de transação SNA utilizando a API de Comunicações CPI do Communications Server para Linux.
- *IBM Communications Server para Linux: Guia do Programador de APPC* ()
Esse manual contém as informações necessárias para gravar programas aplicativos utilizando o APPC (Advanced Program-to-Program Communication).
- *IBM Communications Server para Linux: Guia do Programador de LUA* ()

Esse manual contém as informações necessárias para gravar aplicações utilizando a LUA (LU Application Programming Interface) convencional.

- *IBM Communications Server para Linux: Guia do Programador de CSV* ()
Esse manual contém informações necessárias para gravar programas aplicativos utilizando a API (Application Program Interface) CSSV (Common Service Verbs).
- *IBM Communications Server para Linux: Guia do Programador de MS* ()
Esse manual contém as informações necessárias para gravar aplicações utilizando a API do MS (Management Services).
- *IBM Communications Server para Linux: Guia do Programador de NOF* ()
Esse manual contém as informações necessárias para gravar aplicações utilizando o API do NOF (Node Operator Facility).
- *IBM Communications Server para Linux: Manual de Diagnósticos* ()
Esse manual fornece informações sobre a resolução de problemas em rede SNA.
- *IBM Communications Server para Linux: Guia do Usuário do Conjunto de Aplicativos de APCC* ()
Esse manual fornece informações sobre os aplicativos APPC utilizados com o Communications Server para Linux.
- *IBM IBM Communications Server para Linux: Glossário* ()
Esse manual fornece uma lista abrangente de termos e definições utilizados em toda a biblioteca do IBM IBM Communications Server para Linux.

Publicações do SNA (Systems Network Architecture)

Os manuais a seguir contêm informações sobre redes SNA:

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

Publicações da Configuração do Host

Os manuais a seguir contêm informações sobre a configuração do host:

- *ES/9000, ES/3090 IOCP User's Guide Volume A04* (GC38-0097)
- *3174 Establishment Controller Installation Guide* (GG24-3061)
- *3270 Information Display System 3174 Establishment Controller: Planning Guide* (GA27-3918)
- *OS/390 Hardware Configuration Definition (HCD) User's Guide* (SC28-1848)

Publicações do z/OS Communications Server

Os manuais a seguir contêm informações sobre o z/OS Communications Server:

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

Publicações do TCP/IP

Os manuais a seguir contêm informações sobre o protocolo de rede TCP/IP (Transmission Control Protocol/Internet Protocol):

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

Publicações do X.25

Os manuais a seguir contêm informações sobre o protocolo de rede X.25:

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

Publicações do APPC

Os manuais a seguir contêm informações sobre o APPC (Advanced Program-to-Program Communication):

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

Publicações de Programação

Os manuais a seguir contêm informações sobre programação:

- *Common Programming Interface Communications CPI-C Reference* (SC26-4399)
- *Communications Server para OS/2 Versão 4 Application Programming Guide* (SC31-8152)

Outras Publicações de Rede da IBM

Os manuais a seguir contêm informações sobre outros tópicos relacionados ao Communications Server para Linux:

- *SDLC Concepts* (GA27-3093)
- *Local Area Network Concepts and Products: LAN Architecture* (SG24-4753)
- *Local Area Network Concepts and Products: LAN Adapters, Hubs and ATM* (SG24-4754)
- *Local Area Network Concepts and Products: Routers and Gateways* (SG24-4755)

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

Índice Remissivo

A

- adaptadores de comunicação 20
- Advanced Power Management 28
- alertas 15
- alias, definindo para LU associada 89
- API
 - para Administração do Communications Server para Linux 13
 - suporte 4
 - Tipos do Communications Server para Linux 4
- API NOF 13
- aplicações associadas 6
- APPC
 - configuração 85
 - LU 6.2 dependente 90
 - LU 6.2 independente 87
 - on-line 108
 - suite de aplicação 6, 9
 - suporte a aplicação distribuída 6
- APPC (advanced program-to-program communication) 6
- APPC Application Suite 9
- APPN
 - aplicações para 6, 9
 - configuração 86, 87
 - configuração dinâmica 12
 - funções de subárea 2
 - Nó de extremidade 1
 - nó de rede 1
 - rede de conexão 13
 - roteamento 13
 - segmentação da rede 25
 - suporte de host para 2
 - suporte de LU dependente 3
 - suporte DLUR 2
 - tipo de nó 1
- armazenamento de paginação 22
- armazenamento em disco 22
- armazenamento em disco rígido 21
- armazenamento principal 22
- arquivo de segurança
 - arquivos de configuração 37
 - restauração 38
- arquivo snastart 72, 105
- ativando o Communications Server para Linux
 - no sistema local 72
- ativando o software Communications Server para Linux 104
- ativando portas e estações de link 105
- auxílio
 - programa de administração Motif 12

B

- botões da barra de ferramentas 76
- botões em janelas de recursos 76

C

- caminho dos programas executáveis do Communications Server para Linux 71
- chamadas 4
- cliente 5
- cliente/servidor
 - configuração 77
- comando de consulta 14
- comando start 72
- comando stop 104
- comandos de status 14
- Common Programming Interface for Communications (CPI-C) 4
- compactação, de dados de sessão de LU 3
- computador de recebimento de dados 93
- concentração de PU 93
- concentrador da PU 6
- conectividade
 - configuração 79
 - opções 2
- configuração 18
 - arquivo de segurança 37
 - arquivos 37, 38
 - comunicação APPC 85
 - conectividade 79
 - DLUR 95
 - exemplos 78, 96, 98
 - exibindo 75
 - Informações secundárias de CPI-C 90
 - LU 6.2 87, 90
 - LU implícita de recebimento de dados 94
 - LU tipo 0-3 83
 - LUs associadas para um nó LEN 87
 - LUs de recebimento de dados para gateway SNA 93
 - modificando 75
 - nó 78
 - nó remoto 88
 - Padrão do Redirecionador TN 103
 - padrões do Servidor TN 102
 - planejamento 70
 - porta 80
 - registros da associação do Servidor TN 101
- configuração de LU 6.2 independente 87
- configuração de LU implícita de recebimento de dados 94
- configuração de porta 80, 82
- configuração dinâmica 12
- configurações avançadas, requisitos de memória e de armazenamento 22
- conjunto de LUs
 - configuração 84
 - definindo 84
 - exibindo 84
- convencões de nomenclatura 25
- CPI-C
 - API 4

- CPI-C (*continuação*)
 - configuração 90
 - interoperabilidade 15
- CPI Communications (CPI-C) 4
- curingas 89

D

- DDDLU (Dynamic definition of dependent LUs) 3
- de rede 4
- desativando o Communications Server para Linux 104
- desinstalando o Communications Server para Linux 39
- desinstalando o Remote API Client no Linux para System z 51
- desinstalando um Remote API Client no AIX 56
- desinstalando um Remote API Client no Linux 45
- diálogo 73
- diretório dos programas executáveis do Communications Server para Linux 71
- DLC
 - configuração 82
 - em configuração de porta 80
- DLUR
 - configuração 95
 - configuração de PU 97
 - descrição 2
 - no nó local 96
 - suporte a nós de recebimento de dados 97
- DLUS 95
- documentação, on-line 107
- documentação do Communications Server para Linux 33
- documentação on-line do Communications Server para Linux 33
- domínio 5

E

- eliminando um recurso 75
- Endereço IPv4 23
- Endereço IPv6 23
- Enterprise Extender
 - configuração de link 82
 - porta de diálogo 83
 - visão geral 9
- estação de link
 - ativando 105
 - definindo na porta 81
- Ethernet
 - configuração de link 81
 - diálogo SAP 82
- exibindo a configuração 75
- Extensor de Ramificação 7

F

fazer o backup do servidor master 77
ferramentas de resolução de problemas 15
fluxo de dados 4
folhas de tarefas 71
Formatos de endereço IP 23
fóruns, on-line 107

G

gateway
definição 6
gateway SNA 6
gateway SNA
configuração 93
visão geral 6
gerenciamento de componentes 73
grupos de discussão, on-line 107
GSKIT
Remote API Client no AIX 53, 55
Remote API Client no Linux 42, 44
Remote API Client no Linux para System z 48, 50
Remote API Client no Windows 65

H

HACL 34
hardware
link 20
hardware de link 20
host
em rede APPN 2
em rede de subárea 1
suporte LU 2
Host Access Class Libraries 34
HPR
comparado ao ISR 13
HPR/IP 9
HTTPS
configurando 34
Remote API Client no AIX 55
Remote API Client no Linux 44
Remote API Client no Linux para System z 50
Remote API Client no Windows 65
requisitos 21

I

incluindo um recurso 75
informações sobre release 36
inicializando o nó SNA 105
iniciando automaticamente o Communications Server para Linux 104
iniciando o Communications Server para Linux
automaticamente na inicialização do sistema 72
iniciando o Communications Server para Linux automaticamente 104
ativando o software Communications Server para Linux 104

iniciando o Communications Server para Linux automaticamente (*continuação*)
ativando portas e estações de link 105
inicializando o nó SNA 105
iniciando no momento da inicialização 105
iniciando o Communications Server para Linux na inicialização 105
iniciando um recurso 75
instalação 33
detalhes dos pacotes existentes 28
preparação para a 28
Remote API Client no AIX 54, 55
Remote API Client no Linux 43
Remote API Client no Linux para System z 49
tarefas de manutenção após 35
instalação do cliente/servidor 35
instalando o Communications Server para Linux 33
instalando o Remote API Client no Linux para System z 49
instalando um Remote API Client no AIX 54, 55
instalando um Remote API Client no Linux 43
installibmcs 33
installibmcsdocs 33
interface de programa aplicativo (API) 4
ISO (International Organization for Standards) 25
ISR (intermediate session routing) 13

J

janela 73
janela Configuração, Remote API Client no Windows
parâmetros 60
parâmetros avançados 62
janela Nó 73
Java
Remote API Client no AIX 53
Remote API Client no Linux 42
Remote API Client no Linux para System z 47

L

leitura sugerida 108
LU
associada, definindo 87
configuração 87, 90, 100
conjunto 92, 99, 100, 101
convenções de nomenclatura 25
recebimento de dados 93, 95
suporte 2
LU 3270
definindo 100
para Servidor TN 10, 99
LU 6.2 dependente 90
LU associada
alias 89
configuração 87, 88
definindo com curingas 89

LU associada (*continuação*)
no nó remoto 89
LU de recebimento de dados
configuração 95
exemplos de hardware 93
para gateway SNA 93
LU local, definindo 87
LU tipo 0-3 83

M

MAC (Medium Access Control) 81
MDS-NMVT (Multiple Domain Support-Network Management Vector Transport) 14
Medium Access Control (MAC) 81
memória do kernel 22
memória principal 22
mídia de transporte 19
migrando de níveis anteriores do Communications Server para Linux 29, 30
modificando a configuração 75

N

nó
comunicação com o host 78
configuração 78
em configuração APPN 79
envio de dados 96
inicializando 105
local 96
recebimento de dados 97
remoto 87, 88
nó de envio de dados 96
nó de recebimento de dados 96
Nó de Rede de Ramificação 7
Nó LEN
configuração de LU associada 87
descrição 1
identificação de nó remoto 81
nó LEN (Low-entry Networking) 81
nó remoto
configuração 87, 88
configuração de LU associada 89
Nome do Servidor 60
Número máx. de tentativa de difusão 62

O

on-line
APPC 108
auxílio 12
documentação 107
fóruns 107
grupos de discussão 107
opções de controle de link de dados 2
opções de interface 13
opções de segurança 13
OSI (Open Systems Interconnection) 25

P

- pacing, nível de sessão 13
- pacing a nível de sessão adaptativo 13
- parâmetro Difusões UDP 61
- parâmetro Domínio 60
- parâmetro Tempo limite de acesso à LAN 62
- parâmetro tempo limite para Reconectar 62
- parando um recurso 75
- PDF, visualizando manuais 36
- planejamento de compatibilidade 25
- planilhas, planejando 70
- planilhas de planejamento 70
- ponto
 - rede 1
- ponto de entrada 14
- ponto focal 14
- porta
 - ativando 105
- porta de diálogo IP 83
- Power Management 28
- problema
 - dados 15
 - ferramentas de diagnóstico 15
- procedimentos
 - instalando o Remote API Client no Windows 59, 63
- procedimentos pós-instalação 35
- processamento distribuído
 - ambiente 1
 - suporte a aplicativo 5
- programa de administração
 - API NOF 13
 - linha de comandos 13
 - Motif 12, 14
- programa de administração da linha de comandos 13
- programa de administração Motif
 - auxílio 12
 - capacidades de gerenciamento 14
 - descrição 12
 - utilização 69
- programa de transação (TP) 4
- programa licenciado 32
 - Remote API Client no AIX 54
 - Remote API Client no Linux 43
 - Remote API Client no Linux para System z 48
- programa snaadmin 13
- programa xsnaadmin 12, 69
- programas TN3270 98
- PU (Physical Unit) 6

R

- RAM (Memória de Acesso Aleatório) 22
- recurso
 - definindo 75
 - eliminando 75
 - gerenciamento 73
 - informações 107
 - iniciando 75
 - itens 76
 - parando 75
 - requisitos 18

- recursos Advanced Power Management
 - para PC 28
- recursos de informações 107
- recursos de software 6
- rede
 - alertas 15
 - convenções de nomenclatura 25
 - gerenciamento 14
 - informações disponíveis através 107
 - planejamento 17, 18, 25
 - ponto a ponto 1
 - subárea 1
 - suporte 1
- rede de conexão 13
- rede de conexão, configuração 82
- Rede local (LAN) 2
- Redirecionador TN
 - configuração 102
 - configuração do registro de acesso 103
 - configuração padrão 103
 - visão geral 11
- Remote API Client
 - requisitos de hardware do AIX 53
 - requisitos de hardware do Linux 41
 - requisitos de software AIX 53
 - requisitos de software do Linux para System z 47
 - requisitos de software Linux 42
 - requisitos do hardware do System z 47
- Remote API Client no Linux
 - detalhes dos pacotes existentes 42
- Remote API Client no Linux para System z
 - detalhes dos pacotes existentes 48
- Remote API Client no Windows
 - instalando 58
 - instalando a partir da linha de comandos 63
 - instalando com o programa setup 59
- requisitos
 - HTTPS 21
 - instalação 19
 - memória e armazenamento 21
 - pessoal e habilidade 19
 - sistema operacional 20
 - software 20, 21
 - WebSphere Application Server 21
- requisitos de armazenamento 21
- requisitos de habilidades 19
- requisitos de hardware
 - Remote API Client no AIX 53
 - Remote API Client no Linux 41
 - Remote API Client no Linux para System z 47
 - Remote API Client no Windows 57
- servidor 20
- requisitos de instalação 19
- requisitos de memória 21
 - configurações avançadas 22
 - tipos de armazenamento 22
- requisitos de pessoal 19
- requisitos de sistema operacional 20
- requisitos de software 20, 21
 - Remote API Client no AIX 53
 - Remote API Client no Linux 42

- requisitos de software (*continuação*)
 - Remote API Client no Linux para System z 47
 - Remote API Client no Windows 57
- requisitos funcionais 17
- rpm 19
- RUI Primária 3

S

- SAA (Systems Application Architecture) 4
- SAP (Service Access Point) 19, 81
- SDLC 2
 - configuração 80
 - para tráfego dependente 80
- SDLC (Synchronous Data Link Control) 80
- Service Access Point (SAP) 19, 81
- servidor 5
 - incluindo 77
 - removendo 77
 - requisitos de hardware do Linux 20
- servidor, Telnet 9
- servidor de backup 5
- servidor de configuração 77
 - incluindo 77
 - removendo 77
- servidor de ponto a ponto 5
- Servidor de Unidade Lógica Dependente (DLUS) 95
- servidor master 5
- Servidor TN
 - configuração 98
 - configuração do registro de acesso 102
 - configuração dos registros de associação 101, 102
 - configuração padrão 102
 - suporte a várias sessões 99
 - usuário 99
 - visão geral 9
- sessão
 - em forma de U 3
 - pacing 13
 - roteamento 13
 - suporte 3
- sessões em forma de U 3
- SNA
 - biblioteca 107
- software do cliente
 - desinstalando 67
 - fazendo upgrade 66
 - personalizando 66
 - reinstalando 66
- software SDK
 - Remote API Client no Windows 58
- solicitador de LU dependente (DLUR) 2
- SSL (Secure Sockets Layer)
 - autenticação de cliente 101, 103
 - autenticação do servidor 36, 101, 103
 - criptografia de dados 36, 101, 103
- sub-rotinas 4
- suporte a cliente/servidor 5
- Systems Application Architecture (SAA) 4

T

- tarefas antes da instalação 28
- TN3270
 - programas 9
 - servidor 9
- TP (transaction program) 4
- transparência, local/remota 3
- transparência local/remota 3

U

- unidade física (PU) 6
- unidade lógica (LU) 2, 95
- usuário de TN3270 10, 99

V

- variável de ambiente do idioma 29, 53
 - Remote API Client no Linux 43
 - Remote API Client no Linux para System z 48
- vários servidores em um domínio 5
- verbos 4
- versão, endereço IP 23

W

- WAN (Wide Area Network) 2
- WebSphere Application Server
 - configurando 34
 - requisitos 21

Comunicando Seus Comentários à IBM

Se você gostar ou não gostar especialmente de algo neste documento, utilize o método a seguir para enviar seus comentários à IBM. Envie seu nome, endereço e número de telefone se desejar obter uma resposta.

Sinta-se à vontade para comentar sobre erros ou omissões específicos, precisão, organização, assunto ou totalidade deste documento. No entanto, os comentários enviados devem dizer respeito somente às informações contidas neste manual e à maneira como elas são apresentadas. Para solicitar publicações adicionais ou fazer perguntas ou comentários sobre as funções de produtos ou sistemas IBM, fale com um representante IBM ou com um representante de marketing IBM autorizado.

Ao enviar comentários à IBM, você concede à IBM um direito não-exclusivo para uso ou distribuição desses comentários, da forma que ela achar mais apropriada, sem incorrer em qualquer obrigação para com você.

Envie-nos seus comentários por correio:

- Se preferir enviar seus comentários por fax, utilize este número: 1+919-254-4028
- Se você preferir enviar comentários eletronicamente, utilize este endereço:
 - comsvrcf@us.ibm.com.

- Utilize o seguinte endereço:

IBM Brasil - Centro de Traduções
Rodovia SP 101 km 09
CEP 13185-900
Hortolândia, SP

Inclua o seguinte em sua nota:

- Título e número da publicação deste documento
- Número da página ou tópico ao qual o comentário se aplica.



Número do Programa:

Impresso em Brazil

G517-7999-02

