

IBM Communications Server para Linux



Guía de iniciación rápida

Versión 64

IBM Communications Server para Linux



Guía de iniciación rápida

Versión 64

Nota:

Antes de utilizar esta información y el producto al que da soporte, asegúrese de leer la información de carácter general que figura en el apéndice "Avisos", en la página 113.

Sexta edición (mayo de 2009)

Esta publicación es la traducción del original inglés *IBM Communications Server for Linux* (GC31-6768-03).

Esta edición se aplica a IBM Communications Server para Linux, versión 6.4 y a todos los releases y modificaciones posteriores hasta que se indique lo contrario en nuevas ediciones o boletines técnicos.

Puede solicitar las publicaciones a través del representante local de IBM o de la sucursal de IBM que preste servicio en su localidad. No hay existencias de publicaciones en la dirección indicada más abajo.

IBM agradece sus comentarios. Puede enviar sus comentarios a la dirección siguiente:

International Business Machines Corporation
Attn: Communications Server for Linux Information Development
Department AKCA, Building 501
P.O. Box 12195, 3039 Cornwallis Road
Research Triangle Park, North Carolina
27709-2195
EE.UU.

Puede enviarnos comentarios por correo electrónico utilizando uno de los métodos siguientes:

- Fax (EE.UU. y Canadá):
 - 1+919-254-4028
 - Envíe el fax a "Attn: Communications Server for Linux Information Development"
- Correo electrónico:
 - comsvrcf@us.ibm.com

Al enviar información a IBM, otorga a IBM un derecho no exclusivo a utilizar o distribuir esa información del modo que IBM considere oportuno, sin incurrir por ello en ninguna obligación con el cliente.

© Copyright International Business Machines Corporation 2000, 2009.

Contenido

Tablas	vii
-------------------------	------------

Figuras	ix
--------------------------	-----------

Bienvenido a IBM Communications Server para Linux xi

Cómo utilizar este manual	xi
Guía de iniciación	xi
Convenios tipográficos	xii
Abreviaturas utilizadas en este manual	xiii
Novedades	xiii
Nuevas funciones	xiv
Funciones que se han eliminado	xiv
Dónde encontrar más información.	xv

Capítulo 1. Acerca de IBM Communications Server para Linux 1

Funciones y empaquetado de IBM Communications Server para Linux	1
IBM Communications Server para Linux	1
Funciones de red avanzadas	6
Funciones y ventajas	11
Una base sólida y versátil.	11
Trabajo en una configuración cliente/servidor	12
Fácil configuración	12
Opciones de interfaces de usuario adicionales para la administración.	13
Mejor rendimiento	13
Opciones de seguridad	14
Flexibilidad de la gestión de la red	14
Fiabilidad, disponibilidad y facilidad de mantenimiento	14
Integración, crecimiento y cambio de la red.	15

Capítulo 2. Planificación de la red e IBM Communications Server para Linux 17

Tareas de planificación de la red	17
Identificación de las necesidades funcionales de la red	17
Determinación de la configuración de Communications Server para Linux	18
Identificación de las necesidades de recursos para la instalación y el funcionamiento	18
Direccionamiento IPv4 e IPv6	23
Compatibilidad asegurada entre configuraciones de distintas plataformas	25
Convenios de denominación.	25

Capítulo 3. Instalación de Communications Server para Linux en servidores Linux 27

Empaquetado del programa bajo licencia de Communications Server para Linux	27
Preparación de la instalación de Communications Server para Linux	28
Inhabilitación de las funciones de Gestión de energía	28
Instalación de software como requisito previo	28
Visualización de información detallada sobre la instalación del producto	28
Cambio de la variable de entorno de idioma	29
Migración desde niveles anteriores de Communications Server para Linux	29
Consideraciones	29
Proceso de migración	30
Instalación del programa bajo licencia Communications Server para Linux	32
Instalación de Communications Server para Linux	33
Documentación en línea de Communications Server para Linux	34
Bibliotecas de clases de acceso a sistema principal (HACL)	34
Configuración de WebSphere Application Server	34
Configuración del certificado seguro de WebSphere Application Server	34
Configuración de WebSphere Application Server	35
Instalación del archivo de configuración del servidor	35
Procedimientos posteriores a la instalación	36
Trabajo en una configuración cliente/servidor	36
Visualización de manuales en PDF	36
Revisión de información de release actual	36
Configuración de SSL para su uso con el servidor TN o el redirector TN	36
Copia de seguridad de los archivos de configuración de Communications Server para Linux	37
Restauración de una copia de seguridad de los archivos de configuración de Communications Server para Linux	38
Reinicialización de los archivos de configuración	38
Desinstalación de Communications Server para Linux	39

Capítulo 4. Instalación de clientes IBM Remote API Client en Linux. 41

Requisitos de hardware y software	41
Requisitos de hardware	41
Versión del sistema operativo Linux	42
Java	42
GSKIT	42
Visualización de información detallada sobre la instalación del producto	42
Configuración de la variable de entorno de idioma	43

Instalación del cliente Remote API Client de Linux	43
Configuración de certificados de seguridad de HTTPS utilizando GSKIT	44
Desinstalación del cliente Remote API Client de Linux	46

Capítulo 5. Instalación de clientes IBM Remote API en Linux para System z . . . 47

Requisitos de hardware y software	47
Requisitos de hardware	47
Versión del sistema operativo Linux	47
Java	47
GSKIT	48
Visualización de información detallada sobre la instalación del producto	48
Configuración de la variable de entorno de idioma	48
Instalación del cliente Remote API Client de Linux para System z	49
Configuración de certificados de seguridad de HTTPS utilizando GSKIT	50
Desinstalación del cliente Remote API Client de Linux para System z	51

Capítulo 6. Instalación de clientes IBM Remote API Client en AIX. 53

Requisitos de hardware y software	53
Requisitos de hardware	53
Versión del sistema operativo	53
Java	53
GSKIT	53
Cambio de la variable de entorno de idioma	54
Instalación del cliente Remote API Client de AIX	54
Instalación del cliente Remote API Client mediante la copia de archivos en la estación de trabajo AIX	54
Instalación del cliente Remote API Client desde el CD	55
Configuración de certificados de seguridad de HTTPS utilizando GSKIT	56
Desinstalación del cliente Remote API Client de AIX	56

Capítulo 7. Planificación e instalación del cliente Remote API Client de Windows 59

Requisitos de hardware y software	59
Acceso al programa Setup	60
Instalación del cliente Remote API Client para Windows utilizando el programa Setup	61
Opciones avanzadas para la configuración del cliente Remote API Client	64
Instalación del software del cliente Remote API Client desde la línea de mandatos	65
Configuración de certificados de seguridad de HTTPS utilizando GSKIT	67
Personalización del software del cliente Remote API Client después de la instalación	68
Reinstalación del software del cliente Remote API Client	69

Desinstalación del software del cliente Remote API Client	69
Desinstalación del software del cliente Remote API Client desde la línea de mandatos	70
Ayuda	70

Capítulo 8. Configuración y utilización de Communications Server para Linux . 71

Planificación de la configuración de Communications Server para Linux	72
Hojas de trabajo de planificación	73
Hojas de tareas	73
Utilización del programa de administración de Motif	73
Especificación de la vía de acceso de los programas de Communications Server para Linux	73
Habilitación de Communications Server para Linux	74
Gestión de Communications Server para Linux con el programa de administración de Motif	74
Configuración de las funciones de cliente/servidor	79
Configuración del nodo	80
Configuración de la conectividad	82
Configuración de un enlace SDLC para tráfico dependiente	82
Configuración de un enlace Ethernet para tráfico dependiente e independiente	83
Configuración de un enlace Enterprise Extender	84
Configuración de las LU de tipo 0-3	85
Definición de las LU de tipo 0-3	86
Definición de una agrupación de LU	86
Configuración de la comunicación APPC	87
Configuración de una red APPN sencilla	88
Configuración de APPC dependiente	93
Configuración de CPI-C	93
Configuración de LUA	94
Definición de una agrupación de LU	94
Configuración de la pasarela SNA	95
Soporte para LU implícitas en sentido descendente	97
Definición de LU en sentido descendente	98
Configuración del DLUR	98
Configuración de soporte para el DLUR en el nodo local	100
Configuración de soporte para el DLUR de paso a través para nodos en sentido descendente	100
Configuración del servidor TN	101
Definición de LU 3270	103
Definición de una agrupación de LU	104
Configuración del servidor TN3270	105
Configuración del redirector TN	106
Configuración del redirector TN	106
Inhabilitación de Communications Server para Linux	107
Inicio automático de Communications Server para Linux	108
Habilitación de Communications Server para Linux	108
Inicialización del nodo SNA	108
Activación de puertos y estaciones de enlace	108

Inicio de Communications Server para Linux durante el arranque	109	Publicaciones de Communications Server para Linux versión 6.4	117
Capítulo 9. Recursos de información sobre Communications Server para Linux y SNA	111	Publicaciones de SNA (arquitectura de red de sistemas)	118
Biblioteca de SNA	111	Publicaciones de configuración de sistema principal	119
Información accesible en red	111	Publicaciones de z/OS Communications Server	119
Lectura recomendada	112	Publicaciones sobre TCP/IP	119
Apéndice. Avisos.	113	Publicaciones sobre X.25	119
Marcas registradas	115	Publicaciones de APPC	119
Bibliografía	117	Publicaciones sobre programación	119
		Otras publicaciones de redes de IBM	120
		Índice.	121

Tablas

1. Guía de iniciación	xii	2. Convenios tipográficos.	xii
---------------------------------	-----	------------------------------------	-----

Figuras

1. Pasarela SNA que enlaza varios sistemas Linux en sentido descendente con un sistema principal 7
2. Branch Extender 8
3. Servidor TN 10
4. Ventana Nodo. 76
5. Barra de herramientas de Communications Server para Linux 78
6. Nodo Communications Server para Linux que se comunica directamente con un sistema principal 80
7. Nodos Communications Server para Linux en una red APPN 81
8. Pasarela SNA 96
9. Nodo de Communications Server para Linux que proporciona DLUR 99
10. Nodo de Communications Server para Linux configurado para el servidor TN 102
11. Servidor TN 103

Bienvenido a IBM Communications Server para Linux

Este manual ofrece una introducción a IBM Communications Server para Linux, un producto de software de IBM que permite a un sistema que ejecute Linux intercambiar información con otros nodos de una red SNA (Arquitectura de red de sistemas).

Existen dos variantes de instalación de IBM Communications Server para Linux en función del hardware en el que funciona:

Communications Server para Linux

Communications Server para Linux, número de producto del programa 5724-i33, funciona en los siguientes sistemas:

- Estaciones de trabajo Intel de 32 bits que ejecuten Linux (i686)
- Estaciones de trabajo AMD64/Intel EM64T de 64 bits que ejecuten Linux (x86_64)
- Sistemas IBM pSeries que ejecuten Linux (ppc64)

Communications Server para Linux en System z

Communications Server para Linux en System z, número de producto de programa 5724-i34, funciona en sistemas principales System z que ejecuten Linux para System z (s390 o s390x).

Existen dos copias diferentes del manual *IBM Communications Server para Linux, Guía de iniciación rápida*, una para cada una de estas dos variantes de instalación. Asegúrese de que dispone de la copia correcta del manual para la instalación de Communications Server para Linux. Este manual es aplicable a Communications Server para Linux en las plataformas i686, x86_64 y ppc64.

Communications Server para Linux ofrece elementos esenciales para una amplia gama de necesidades y soluciones de gestión de redes. Pueden utilizarse para intercambiar información con nodos de redes SNA, o para ofrecer acceso de sistema principal para programas Telnet que se comunican a través de Transmission Control Protocol/Internet Protocol (TCP/IP).

Cómo utilizar este manual

Este apartado describe cómo se organiza y presenta la información de este manual.

Guía de iniciación

Este manual está dirigido al personal técnico y de gestión que participa en la planificación de redes y a toda persona interesada en Communications Server para el sistema operativo Linux.

Para buscar la información que necesita para empezar a utilizar Communications Server para Linux, consulte la Tabla 1 en la página xii.

Cómo utilizar este manual

Tabla 1. Guía de iniciación

Si desea...	Consulte...
Leer acerca de Communications Server para Linux	Capítulo 1, “Acerca de IBM Communications Server para Linux”, en la página 1
Planificar la forma de utilización de Communications Server para Linux en la red	Capítulo 2, “Planificación de la red e IBM Communications Server para Linux”, en la página 17
Instalar Communications Server para Linux en servidores Linux	Capítulo 3, “Instalación de Communications Server para Linux en servidores Linux”, en la página 27
Instalar clientes Remote API en Linux (de 32 bits, Intel/AMD de 64 bits o pSeries)	Capítulo 4, “Instalación de clientes IBM Remote API Client en Linux”, en la página 41
Instalar clientes Remote API en Linux para System z	Capítulo 5, “Instalación de clientes IBM Remote API en Linux para System z”, en la página 47
Instalar clientes Remote API en AIX	Capítulo 6, “Instalación de clientes IBM Remote API Client en AIX”, en la página 53
Instalar clientes Remote API en Windows	Capítulo 7, “Planificación e instalación del cliente Remote API Client de Windows”, en la página 59
Configurar Communications Server para Linux	Capítulo 8, “Configuración y utilización de Communications Server para Linux”, en la página 71
Buscar información acerca de la documentación de Communications Server para Linux y otras publicaciones, incluida la información en línea	Capítulo 9, “Recursos de información sobre Communications Server para Linux y SNA”, en la página 111
Leer avisos e información sobre marcas registradas	“Avisos”, en la página 113

Convenios tipográficos

En la Tabla 2 se muestran los estilos tipográficos utilizados en esta publicación.

Tabla 2. Convenios tipográficos

Elemento especial	Ejemplo de tipografía
Palabras enfatizadas	Realice una copia de seguridad de los archivos antes de suprimirlos
Título de publicación	<i>IBM Communications Server para Linux, Guía de administración</i>
Nombre de vía de acceso o de archivo	<code>/usr/spool/uucp/miarch.bkp</code>
Programa o aplicación	<code>snaadmin</code>
Datos entrados por el usuario	<code>0p1</code>
Salida de la máquina	<code>CLOSE</code>

Abreviaturas utilizadas en este manual

En este manual se utilizan las abreviaturas siguientes:

AIX	Advanced Interactive Executive
API	Interfaz de programas de aplicación
APPC	Comunicación avanzada programa a programa
APPN	Red avanzada de igual a igual
BrNN	Nodo de red de ramificación
COS	Clase de servicio
CPI-C	Interfaz común de programación para comunicaciones
CSV	Common Service Verb
DDDLU	Definición dinámica de LU dependientes
DES	Estándar de cifrado de datos
DLC	Control de enlace de datos
DLUR	Peticionario de LU dependiente
DLUS	Servidor de LU dependiente
FTP	Protocolo de transferencia de archivos
HPR	Direccionamiento de alto rendimiento
IETF	Internet Engineering Task Force
ISO	International Organization for Standards
ISR	Direccionamiento de sesiones intermedias
LAN	Red de área local
LDAP	Lightweight Directory Access Protocol
LEN	Low-Entry Networking
LLC2	Control de enlace lógico 2
LU	Unidad lógica
LUA	Interfaz de programas de aplicación de LU convencional
MDS-NMVT	Soporte de dominio múltiple—transporte de vectores de gestión de la red
MPC	Canal multivía
MS	Management Services
NMVT	Transporte de vectores de gestión de redes
NOF	Node Operator Facility
OSI	Open Systems Interconnection
PU	Unidad física
RFC	Solicitud de comentarios
RLE	Codificación de longitud de ejecución
SAA	Arquitectura de aplicación de sistemas
SAP	Punto de acceso a servicio
SNA	Arquitectura de red de sistemas
SSL	Secure Sockets Layer
TCP/IP	Protocolo de control de transmisión/protocolo de Internet
TN	Telnet
TP	Programa de transacciones
VT	Terminal virtual
WAN	Red de área amplia

Novedades

Communications Server para Linux versión 6.4 sustituye a Communications Server para Linux versión 6.2.3, Communications Server para Linux versión 6.2.2, Communications Server para Linux versión 6.2.1 y Communications Server para Linux versión 6.2.

Novedades

Los releases de este producto que todavía están soportados son:

- Communications Server para Linux versión 6.2.3
- Communications Server para Linux versión 6.2.2
- Communications Server para Linux versión 6.2.1

Los releases siguientes de este producto ya no están soportados:

- Communications Server para Linux versión 6.2
- Communications Server para Linux versión 6.0.1 (V6.0.1), que estaba disponible como PRPQ 5799-RQA o 5799-RXL.

Communications Server para Linux versión 6.4 funciona con IBM Remote API Client versión 6.4.0, 6.3.1 ó 6.3.0.

Nuevas funciones

En este release se han añadido las siguientes funciones a Communications Server para Linux:

- Puede especificar una correlación entre tipos de dispositivos TN3270 y los modelos de LU que Communications Server para Linux debería solicitar del host cuando dichos dispositivos conectan con el servidor TN a través de Communications Server para Linux utilizando la DDDL (Definición dinámica de unidades lógicas dependientes). Esto le permite utilizar el modelo de LU que más apropiado sea para cada tipo de dispositivo.
- El HPR (Direccionamiento de alto rendimiento) incluye ahora otras opciones de configuración:
 - La funcionalidad de la modalidad progresiva ARB (también conocida como ARB-P), que mejora el control del flujo de HPR cuando trabaja con variaciones del tiempo de respuesta en sistemas virtuales y remotos.
 - Un temporizador de retardo de conmutación de vía de acceso configurable, el cual ayuda a evitar conmutaciones de vía de acceso innecesarias causadas por retrasos transitorios en el tráfico de la red.
- La interfaz APPC incluye un nuevo verbo CANCEL_CONVERSATION, que permite cancelar un suceso de conversación si hay aún otros verbos pendientes. Este verbo funciona de manera similar a la llamada CPI-C Cancel_Conversation (cmcanc) y está disponible en AIX, Linux y Windows.
- En un cliente IBM Remote API Client para Windows, ahora es posible ejecutar programas de utilidades (el de utilidad de configuración de cliente **sxclconf**, el de supervisión de cliente **sxclappl** y el de utilidad de línea de mandatos **tpinst32** para configurar un TP que se pueda invocar) en las lenguas soportadas; no está limitado a la lengua utilizada al instalar el cliente.
- En un cliente IBM Remote API Client para Windows, la utilidad de configuración de cliente **sxclconf** permite ahora habilitar o inhabilitar el registro de excepciones, el registro de auditorías y rastreo (rastreo de API en todas las API y rastreo de cliente/servidor en los mensajes entre el cliente y el servidor).
- Las aplicaciones Java CPI-C están soportadas en el cliente IBM Remote API Client para Windows, AIX y Linux.

Funciones que se han eliminado

No se han eliminado funciones en este release.

Dónde encontrar más información

La bibliografía proporciona otros manuales de la biblioteca de Communications Server para Linux, así como otros manuales que contienen información adicional sobre SNA y otros productos relacionados.

Capítulo 1. Acerca de IBM Communications Server para Linux

Este capítulo explica cómo está empaquetado Communications Server para Linux y describe sus funciones, características y ventajas.

Funciones y empaquetado de IBM Communications Server para Linux

Communications Server para Linux es un software de comunicación que se ejecuta en el sistema operativo de Linux. Consta de las funciones descritas en “IBM Communications Server para Linux” y “Funciones de red avanzadas” en la página 6.

IBM Communications Server para Linux

IBM Communications Server para Linux conecta aplicaciones en las redes SNA y TCP/IP. Convierte un sistema de Linux en un nodo SNA equipándolo con recursos y protocolos SNA, lo que permite al sistema de Linux comunicarse con otros sistemas en una red SNA, incluyendo sistemas principales. También ofrece funciones TCP/IP que permiten utilizar IBM Communications Server para Linux en la red TCP/IP o en el límite entre las redes TCP/IP y SNA.

Communications Server para Linux ofrece los siguientes servicios:

Soporte de red

Communications Server para Linux proporciona soporte a las redes de subárea y de igual a igual:

Redes de subárea SNA

Estas redes (también conocidas como redes moderadas por sistema principal) están organizadas jerárquicamente; uno o varios sistemas principales controlan la comunicación entre los sistemas, gestionan la red y proporcionan servicios de proceso y almacenamiento de datos de alta capacidad. Todos los demás nodos de la red dependen del control de un sistema principal.

Los sistemas Linux pueden participar en una red de subárea si se configuran como nodos dependientes de sistema principal.

Redes de igual a igual

Para los entornos de proceso distribuido, Communications Server para Linux da soporte a redes APPN. En estas redes de igual a igual, los sistemas Linux conservan las funciones de proceso y se comunican entre sí directamente como iguales. Las redes de igual a igual utilizan las posibilidades del sistema Linux, que actualmente compite con costosos sistemas principales.

Una red APPN consta de nodos iguales de los tipos siguientes:

- Nodo de red APPN (que proporciona control del tráfico, servicios de cálculo y selección de rutas dinámicas y servicios de gestión de red)
- Nodo final APPN (que utiliza servicios de nodo de red APPN para comunicarse con nodos iguales)
- Nodo LEN (que se comunica directamente con los nodos adyacentes o con los nodos configurados de modo que parezcan adyacentes)

Funciones y empaquetado de IBM Communications Server para Linux

Nota: Los sistemas principales pueden funcionar como nodos de igual en una red APPN utilizando una LU 6.2 independiente para comunicarse con los sistemas Linux y otros sistemas principales en la red.

Cómo proporcionar funciones de subárea en una red APPN

La función del petionario de LU dependientes (DLUR) hace posible el tráfico entre sistemas principales y nodos dependientes de sistemas principales a través de una red APPN.

Opciones de control de enlace de datos

En el nivel de enlace, Communications Server para Linux ofrece distintas opciones de conectividad que ayudan a satisfacer las consideraciones de tamaño, velocidad, seguridad y coste de la red. (Para ver una lista detallada de los tipos de enlace soportados, consulte "Requisitos de instalación" en la página 20.) CS/AIX soporta enlaces de datos para diferentes tipos de red, que se detallan a continuación:

Redes de área local

Para la conectividad LAN, puede instalar los enlaces adecuados a fin de que la comunicación se efectúe mediante los protocolos Token Ring, Ethernet estándar y Ethernet 802.3.

Redes de área amplia

Communications Server para Linux da soporte a la conectividad SDLC y X.25 (QLLC). Depende del adaptador OEM al que se proporcione soporte en cada plataforma.

Conexión local

Communications Server para Linux da soporte a la conectividad Canal multivía de canal a canal (CTCMPC) en la conexión local (sólo Communications Server para Linux en System z).

Integración de IP

Si la red troncal corporativa se basa en IP, puede utilizar la función Enterprise Extender (HPR/IP) de Communications Server para Linux para integrarla en SNA y permitir así que las aplicaciones SNA se comuniquen a través de la red IP.

Soporte de LU

Las unidades lógicas (LU) son recursos de red específicos de aplicaciones que residen en cada uno de los nodos de la red SNA. Cada una de las LU actúa como una interfaz que las aplicaciones utilizan para acceder a los enlaces a fin de comunicarse a través de la red con las aplicaciones asociadas de otros nodos.

Communications Server para Linux da soporte a diferentes tipos de LU para distintas clases de aplicaciones.

- En una red de subárea, Communications Server para Linux da soporte a LU independientes, que pueden ser de cualquiera de los tipos siguientes:
 - LU 0
 - LU 1
 - LU 2
 - LU 3
 - LU 6.2

LU 0 da soporte a la comunicación básica programa a programa, que se utiliza normalmente en las transacciones de punto de venta de los sectores de venta al por menor y banca. LU 2 da soporte a aplicaciones

de emulación que permiten al sistema Linux emular un terminal de la familia IBM 3270. Los demás tipos de LU permiten a las aplicaciones participar en procesos distribuidos o comunicarse con diferentes impresoras o terminales de pantalla interactivos.

Communications Server para Linux da soporte a sistemas principales que utilizan la definición dinámica de LU independientes (DDDLU) una función del sistema principal que permite añadir LU dependientes del sistema SNA a la configuración del sistema principal cuando se establece el enlace de comunicación desde el sistema SNA hasta el sistema principal. Con DDDLU, no es necesario que las LU estén configuradas estáticamente en el sistema principal. (Sigue siendo necesario definir las LU dependientes en el nodo Communications Server para Linux). De este modo se reduce la configuración inicial necesaria en el sistema principal y se facilita una posible ampliación posterior.

Communications Server para Linux puede comunicarse con sistemas principales con posibilidad de DDDLU y con sistemas principales sin esta posibilidad, sin que existan diferencias en la configuración necesaria. Cuando se establece el enlace de comunicaciones desde el nodo Communications Server para Linux con el sistema principal, el sistema principal con posibilidad de DDDLU informa al nodo de que da soporte a DDDLU; a continuación, el nodo envía la información necesaria para definir las LU dependientes que utilizan el enlace. Si el sistema principal no tiene posibilidad de DDDLU, Communications Server para Linux no envía esta información y supone que ya se han definido estáticamente las LU en el sistema principal.

- La LU 6.2 independiente da soporte al tráfico independiente en las redes APPN. También da soporte a la comunicación autónoma y a la gestión de red, así como al proceso distribuido.

Además, la función DLUR de Communications Server para Linux permite que el tráfico de LU dependientes fluya a través de una red APPN.

- El soporte de la RUI primaria proporciona la capacidad de que una aplicación de Communications Server para Linux gestione dispositivos LU dependientes conectados por LAN/WAN como si fueran un sistema central. Esta función tiene algunas restricciones respecto a la conectividad, pero permite que las aplicaciones transfieran datos entre dispositivos de LU dependiente sin necesidad de una aplicación completa de sistema central.

Soporte de sesión

Una sesión es un canal lógico temporal entre LU asociadas. Normalmente, las aplicaciones asociadas que están asociadas con cada una de las LU se comunican por medio de la sesión. Communications Server para Linux puede dar soporte a miles de sesiones. Communications Server para Linux puede también dar soporte a sesiones en forma de U (lo que también se denomina "transparencia local/remota"), en las que las LU primarias y secundarias residen en el mismo sistema Linux. Estas sesiones permiten desarrollar y probar un par de programas de transacciones de origen y destino en un mismo sistema, sin necesidad de una conexión de enlace.

Los datos que fluyen en una sesión entre dos LU asociadas pueden comprimirse, para reducir el ancho de banda necesario.

- Para el tipo de LU 6.2, Communications Server para Linux permite especificar el uso de la compresión en la configuración de la modalidad que la sesión utiliza. Puede especificar diferentes algoritmos de

Funciones y empaquetado de IBM Communications Server para Linux

compresión para utilizar y que cada uno de ellos proporcione un nivel de compresión diferente (RLE, LZ9 o LZ10). También puede especificar diferentes niveles de compresión para los datos que fluyan en direcciones distintas de la sesión o especificar la compresión en una dirección pero no en la otra.

- Para los tipos de LU 0–3, Communications Server para Linux permite especificar la utilización de la compresión en la configuración de la estación de enlace o PU que utiliza la sesión. La compresión RLE se utiliza para la dirección de entrada y LZ9 para la dirección de salida.

Soporte de API

Communications Server para Linux incluye interfaces de programación de aplicaciones (API) para desarrollar aplicaciones de determinados tipos de LU, para el proceso distribuido, para la gestión de la red y para la administración del propio Communications Server para Linux.

Communications Server para Linux ofrece un conjunto de API que son compatibles con las API proporcionadas por los miembros de la familia Communications Server que se ejecutan en otros sistemas operativos.

Una API es una interfaz que permite que un programa de transacciones (TP) se comunique con su LU de soporte. Consiste en una biblioteca de verbos (también denominados funciones, llamadas y subrutinas) de la que el TP selecciona aquellos que necesita para pasarlos a su LU a fin de solicitar una acción, como SEND_DATA. La LU, a su vez, procesa los verbos y genera una corriente de datos de acuerdo con el protocolo adecuado, añade una cabecera que indica la dirección de destino y envía los datos por el enlace a las LU asociadas.

CPI-C (interfaz común de programación para comunicaciones) es una de las API más potentes debido a su portabilidad. CPI-C se introdujo para dar soporte a las LU 6.2 dependientes e independientes y se adecua a SSA (Arquitectura de aplicación de sistemas) para unificar las diferentes plataformas y los distintos sistemas operativos. CPI-C utiliza un conjunto de reglas sintácticas común a todos los sistemas. De este modo, se ha convertido en un estándar.

Además de la API CPI-C estándar para el lenguaje C, Communications Server para Linux incluye también una API CPI-C para utilizar con aplicaciones Java. Para obtener más información, consulte la publicación *IBM Communications Server for AIX or Linux CPI-C Programmer's Guide*. En los manuales de Communications Server para Linux, todas las referencias a CPI-C incluyen CPI-C para Java, a menos que se indique lo contrario.

Otras API de Communications Server para Linux incluyen:

- API de APPC para las comunicaciones de igual a igual entre programas de aplicación que utilizan LU 6.2. La API tiene la opción de funcionamiento sin bloqueo. Cuando un TP utiliza verbos sin bloqueo, la API puede devolver el control al TP antes de que haya finalizado la acción solicitada. Más tarde, cuando la acción ha finalizado, se informa de ello al TP.
- API de LUA para las comunicaciones con aplicaciones de sistema principal.
- API de CSV (Common Service Verb) para las funciones de programa de utilidad tales como la conversión de caracteres y el control de rastreo de aplicaciones.

Funciones y empaquetado de IBM Communications Server para Linux

Además, Communications Server para Linux incluye las siguientes interfaces de programación de su propiedad:

- API de MS (Management Services) para las funciones de mensajería de la red.
- API de NOF (Node Operator Facility) para aplicaciones que configuran y gestionan los recursos de Communications Server para Linux resources.

Para obtener información más detallada acerca de una API, consulte la guía de programación para la API en cuestión (consulte la bibliografía).

Soporte de cliente/servidor

Los sistemas que ejecutan Communications Server para Linux se pueden configurar para que se comuniquen mediante protocolos de cliente/servidor. Cuando se utilizan protocolos de cliente/servidor en una red, se hace referencia a todos los sistemas que utilizan esos protocolos para comunicarse en la red como “dominio.”

Los sistemas que ejecutan Communications Server para Linux en una configuración de cliente/servidor pueden realizar las funciones siguientes:

- Un servidor contiene un nodo SNA y sus componentes de conectividad asociados. El servidor ofrece conectividad SNA a las aplicaciones del sistema local o de otros sistemas del dominio Communications Server para Linux. Los servidores deben ser sistemas Linux.
- Un cliente Remote API Client no contiene componentes de nodo SNA, sino que accede a ellos a través de un servidor. Un cliente puede acceder a uno o varios servidores a la vez, y puede ejecutar aplicaciones simultáneamente si lo necesita. Los clientes pueden estar ejecutando AIX, Linux, o Windows. (Un sistema Linux puede ser un servidor o un cliente, pero no ambos a la vez; no puede instalar el servidor y el cliente en el mismo sistema).

Los servidores y los clientes se comunican en el dominio Communications Server para Linux utilizando TCP/IP. Como alternativa, servidores y clientes se pueden comunicar utilizando HTTPS a través de un servidor WebSphere, el cual utiliza certificados de seguridad para autenticar las conexiones de los clientes. Normalmente es conveniente utilizar HTTPS si los clientes se conectan utilizando una red pública.

En un dominio con múltiples servidores Communications Server para Linux, un servidor contiene la copia maestra del archivo de configuración del dominio Communications Server para Linux. Este servidor se denomina servidor maestro.. Se pueden definir otros servidores del dominio como servidores de reserva o dejarlos como servidores iguales.. El archivo de configuración del dominio se copia en los servidores de reserva—cuando se inician o cuando se cambia la copia maestra—para que todos los servidores de reserva dispongan de una copia de la información más reciente. Un servidor igual obtiene la información de configuración del dominio cuando la necesita del servidor maestro, pero no actúa como servidor de reserva.

Si el servidor maestro falla, el primer servidor de reserva de la lista de servidores definidos para el dominio pasa a ser el maestro. El archivo de configuración del dominio de este servidor se utiliza como copia maestra y se copia a otros servidores, si es necesario. Cuando se reinicia el servidor maestro, recibe una copia de la configuración del dominio desde el servidor de reserva que actúa actualmente como maestro y, a continuación, pasa a ser el maestro.

Funciones y empaquetado de IBM Communications Server para Linux

Soporte de aplicaciones distribuidas

En un sistema cliente/servidor Communications Server para Linux, las aplicaciones que se ejecutan en los clientes Remote API Client trabajan conjuntamente con los recursos de conectividad de los servidores para ejecutar una sola tarea. Las aplicaciones que se ejecutan en otros sistemas (que no son Communications Server para Linux) también pueden cooperar con las aplicaciones de los sistemas Communications Server para Linux para realizar el proceso distribuido.

Communications Server para Linux da soporte a aplicaciones distribuidas mediante APPC (también conocida como LU 6.2).

Funciones de red avanzadas

En el producto base de Communications Server para Linux se incluye un conjunto de funciones que añaden posibilidades de red avanzadas. Estas funciones son las siguientes:

- La pasarela SNA conecta redes LAN a redes SNA de subárea.
- El soporte a la LU primaria proporciona soporte para controlar los dispositivos LU dependientes en sentido descendente de la misma forma que una aplicación de sistema principal.
- Branch Extender simplifica las redes APPN de grandes dimensiones separando los recursos en distintas ubicaciones (por ejemplo, en distintas sucursales de una organización grande). Esto reduce la cantidad de información sobre topología que debe mantenerse, sin dejar de permitir la ubicación eficiente de los recursos.
- APPC Application Suite proporciona aplicaciones seleccionadas para su uso en redes APPN.
- Enterprise Extender (EE, también denominado HPR/IP) permite transportar el tráfico SNA de forma nativa a través de redes IP.
- El servidor TN proporciona acceso al sistema principal sobre SNA a clientes TN3270 y TN3270E, denominados de forma global clientes TN3270.
- La función del redirector TN proporciona acceso de sistema principal TCP/IP de paso a través a clientes TN3270, TN3270E, TN5250 y VT, denominados de forma genérica clientes Telnet.

Pasarela SNA

Una pasarela es un dispositivo transparente para el usuario que conecta redes o sistemas informáticos distintos, dando soporte a los dos entornos que conecta. Los usuarios finales se perciben como residentes en la misma red.

Funciones y empaquetado de IBM Communications Server para Linux

La pasarela SNA permite a un sistema Communications Server para Linux actuar como pasarela de enlace entre varios sistemas en sentido descendente en una red SNA para una o varias unidades físicas del sistema principal (PU), tal como se ilustra en la Figura 1. Para simplificar la conectividad del sistema principal y eliminar los enlaces sobrantes, la pasarela SNA actúa como concentrador de PU—considera los diversos sistemas como una sola PU (que parece residir en el nodo de pasarela SNA) y se comunica con el sistema principal a través de una única conexión física.

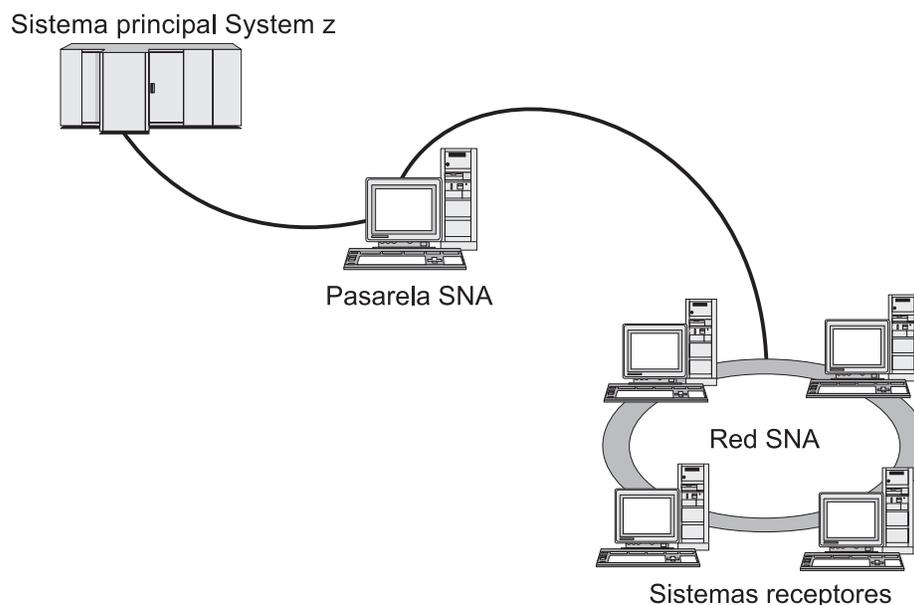


Figura 1. Pasarela SNA que enlaza varios sistemas Linux en sentido descendente con un sistema principal

Soporte a la LU primaria

El soporte de la LU primaria permite que una aplicación Linux controle dispositivos LU dependientes en sentido descendente como si se tratara de una aplicación de sistema principal.

Las aplicaciones LUA suelen conectarse a los sistemas principales como LU secundarias, por lo que la aplicación del sistema principal controla la definición de las sesiones y es responsable del envío de BIND para iniciar una sesión. Communications Server para Linux también incluye la posibilidad de actuar como LU primaria con dispositivos SNA dependientes en sentido descendente a través de una LAN, utilizando la interfaz de RUI primaria. Utilizando esta interfaz, una aplicación puede conectarse con sesiones de LU dependientes de sentido descendente sin necesidad de un sistema principal.

Para utilizar aplicaciones de LU primaria, el nodo debe estar configurado con LU en sentido descendente (o una plantilla de PU en sentido descendente) utilizando el nombre de LU de sistema principal #PRIRUI#. Esto indica al servidor que las aplicaciones que utilizan la RUI primaria controlarán estas PU y los recursos LU asignados a las mismas. Las PU se pueden utilizar tanto en puertos LAN como WAN. Consulte la publicación *IBM Communications Server for AIX or Linux LUA Programmer's Guide* para obtener más información sobre las aplicaciones de programación para utilizar RUI primarias.

Branch Extender

Los nodos de red de una red APPN necesitan mantener la información sobre topología (acerca de la ubicación de otros nodos en la red y los enlaces de comunicación entre ellos) y reenviar esta información por la red cuando la topología cambia. A medida que el tamaño de la red crece, la cantidad de información almacenada y el tráfico de red relacionado con la topología pueden convertirse en demasiado elevados y difíciles de gestionar.

Es posible evitar estos problemas dividiendo la red en subredes, de modo que cada nodo sólo necesite mantener la información sobre topología de los nodos de su propia subred. Sin embargo, esto tiene como resultado un mayor tráfico de red al intentar localizar recursos en otras subredes.

La función Branch Extender de APPN, ilustrada en la Figura 2, proporciona una solución a estos problemas.

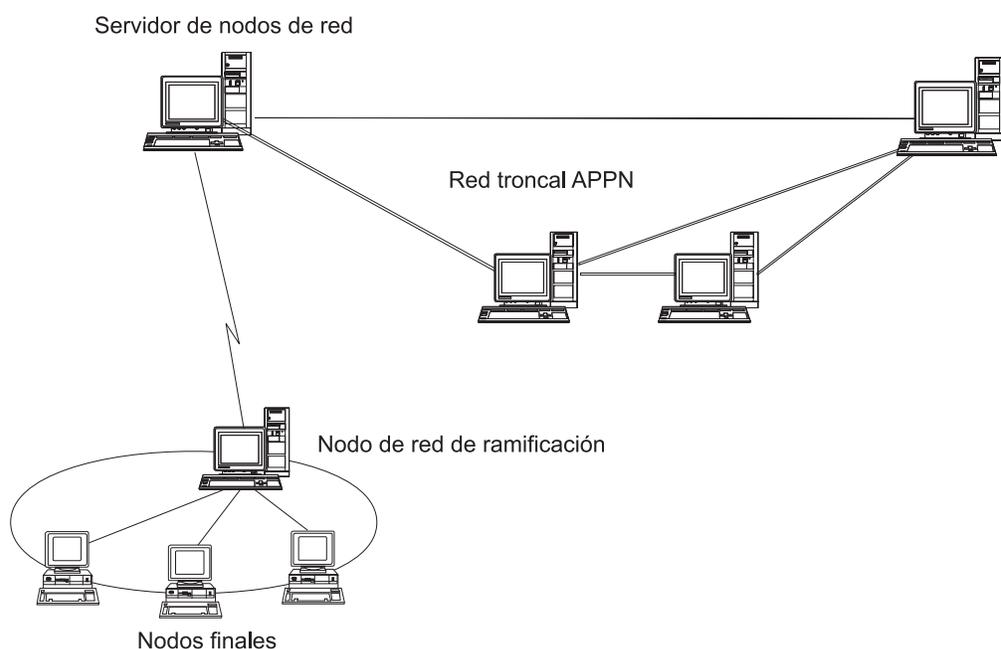


Figura 2. Branch Extender

Como indica su nombre en inglés, Branch Extender está diseñado para las redes que pueden dividirse en áreas diferenciadas, como sucursales independientes de una gran organización. Funciona separando ramas de la red troncal APPN principal (por ejemplo, la red de la sede de la organización).

Cada rama contiene un nodo de un tipo nuevo llamado nodo de red de ramificación (BrNN), que se conecta a un nodo de red en la red troncal APPN principal. El nodo BrNN combina las funciones de un nodo de red APPN y un nodo final APPN.

- El nodo BrNN aparece a la vista de la red troncal como un nodo final conectado a su servidor de nodos de red (NNS) en la red troncal:
 - Los nodos de la red troncal no son conscientes de los nodos existentes en la rama, con lo que se reduce así la cantidad de información sobre topología que debe almacenarse.

Funciones y empaquetado de IBM Communications Server para Linux

- Puesto que el nodo BrNN aparece como un nodo final, no recibe información sobre topología de la red troncal (la información sobre topología se transmite sólo entre nodos de red).
- El nodo BrNN registra todos los recursos de la rama en su NNS, como si estuvieran ubicados en el nodo BrNN. Esto significa que los nodos de la red troncal pueden localizar recursos en la rama sin tener que ser conscientes de los distintos nodos de la rama.
- El nodo BrNN aparece a la vista de la red de ramificación como un nodo de red que actúa como NNS para los nodos finales de la rama. Cada nodo de la rama ve el resto de la red como si se conectara a por medio de su NNS, del mismo modo que en el caso de un NNS estándar.

APPC Application Suite

APPC Application Suite es un conjunto de aplicaciones que demuestra las posibilidades de proceso distribuido de las redes APPN y que puede ser útil en la verificación de la configuración y en la determinación de problemas. APPC Application Suite puede utilizarse para proporcionar soporte para operaciones (como, por ejemplo, la transferencia de archivos) que se realizan con frecuencia en una red.

APPC Application Suite contiene las aplicaciones siguientes:

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

Se puede acceder a estas aplicaciones desde un servidor o desde un cliente Linux o Windows.

Enterprise Extender

Enterprise Extender (también denominado HPR/IP) proporciona un mecanismo para integrar aplicaciones SNA en una red IP.

Las aplicaciones SNA están diseñadas para utilizar protocolos SNA para comunicarse por redes SNA con otras aplicaciones SNA. Al instalarse en una red TCP/IP utilizando Enterprise Extender, las aplicaciones SNA todavía pueden comunicarse; la función Enterprise Extender proporciona un mecanismo para transportar los protocolos SNA a través de la red IP. Concretamente, proporciona la función de direccionamiento de alto rendimiento (HPR) de APPN, que aporta a las aplicaciones las ventajas de la conectividad APPN e IP.

Enterprise Extender en Communications Server para Linux se implementa simplemente como un enlace de comunicaciones. Para conectar dos aplicaciones SNA a través de IP, debe definir un enlace Enterprise Extender, del mismo modo que para cualquier otro tipo de enlace, tal como SDLC o Ethernet.

Servidor TN

Los programas de emulación 3270 que se comunican por TCP/IP (y no por una red SNA) se denominan “programas TN3270” (programas de emulación Telnet 3270).

Funciones y empaquetado de IBM Communications Server para Linux

Los programas TN3270 también pueden incluir soporte para TN3270E (extensiones estándar de Telnet 3270). TN3270E soporta la emulación de dispositivos 3270 (terminales e impresoras) mediante Telnet. Permite que un cliente Telnet seleccione un dispositivo determinado (especificando el nombre de LU o el nombre de una agrupación de LU), y proporciona soporte ampliado para varias funciones, incluidas las teclas ATTN y SYSREQ y el manejo de respuestas SNA.

Nota: en esta publicación se utiliza el término TN3270 para la información que es válida para los protocolos TN3270, TN3287 y TN3270E.

El servidor TN de Communications Server para Linux proporciona acceso a sistemas principales 3270 para usuarios TN3270 en otros sistemas. El servidor TN permite a los usuarios TN3270 compartir una conexión de sistema principal con usuarios Communications Server para Linux o con otros usuarios TN3270, en lugar de requerir un enlace directo. Además, el servidor TN permite a los usuarios TN3270 acceder a sistemas principales que no ejecutan TCP/IP.

La función de servidor TN de Communications Server para Linux TN se ilustra en la Figura 3.

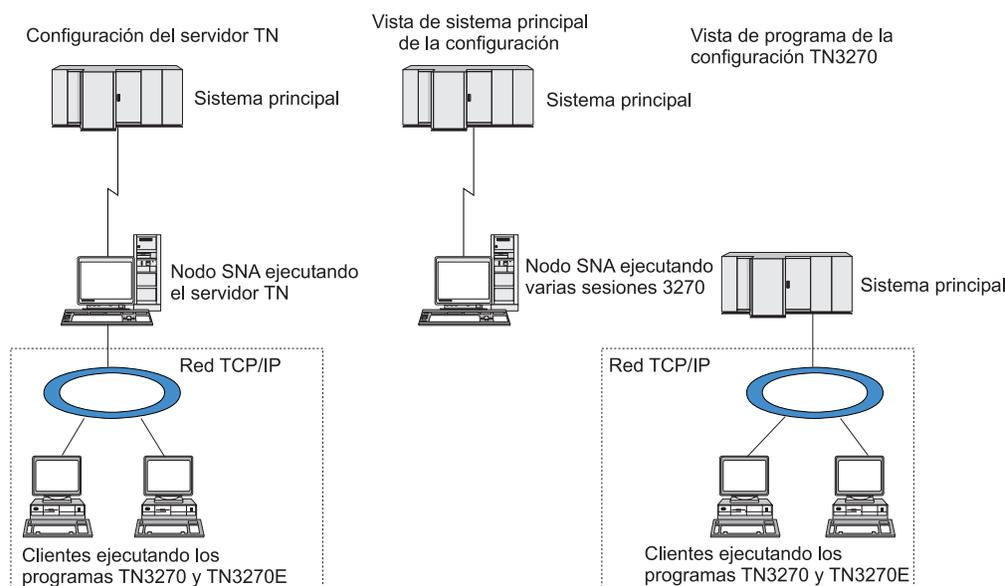


Figura 3. Servidor TN

La función de servidor TN de Communications Server para Linux proporciona una asociación entre un usuario TN3270 y una LU 3270 de Communications Server para Linux. Todos los datos del usuario TN3270 se dirigen a la LU. Esto significa que el sistema principal y el usuario TN3270 están configurados como si estuvieran conectados directamente; ninguno de ellos precisa saber que los datos se dirigen a través del servidor TN.

El servidor TN de Communications Server para Linux TN da soporte a todos los programas de emulación de cliente TN3270 que implementan correctamente los protocolos definidos en los REC de la IETF 1123, 1576, 1646, 1647 y 2355.

Funciones de seguridad: El servidor TN de Communications Server para Linux da soporte al cifrado de datos, la autenticación de servidor, la autenticación de cliente y al inicio de sesión rápido, utilizando el software Secure Sockets Layer (SSL):

Funciones y empaquetado de IBM Communications Server para Linux

- El cifrado de datos significa que los datos que fluyen entre el servidor TN y el emulador TN3270 están cifrados.
- La autenticación de servidor permite a un cliente TN3270 verificar que el servidor TN al que está conectado es el que espera que sea.
- La autenticación de cliente permite a un servidor TN verificar si el cliente TN3270 que se conecta a él es el correcto. El servidor TN también puede comprobar una lista de revocación en un servidor de directorios externo para asegurarse de que la autorización del cliente no ha sido revocada.
- El inicio de sesión rápido conjuntamente con la autenticación de cliente eliminan el requisito que tienen los clientes TN3270 de facilitar un ID de usuario y una contraseña al conectarse al sistema principal. En su lugar, se utiliza el certificado de seguridad del cliente para recuperar la información necesaria de ID de usuario y contraseña.

Redirector TN

La función redirector TN de Communications Server para Linux ofrece servicio de paso para sesiones 3270, 5250 o VT en TCP/IP. El usuario Telnet se comunica con Communications Server para Linux a través de una conexión TCP/IP; Communications Server para Linux se comunica entonces con el sistema principal a través de otra conexión TCP/IP.

El redirector TN de Communications Server para Linux da soporte al cifrado de datos, la autenticación de servidor y la autenticación de cliente mediante el software Secure Sockets Layer (SSL), del mismo modo que el servidor TN para 3270. Esto permite utilizar la comprobación de seguridad de SSL (Secure Sockets Layer) donde sea necesario, y no en la conexión completa entre usuario y sistema principal. Por ejemplo:

- Si los clientes se conectan a Communications Server para Linux a través de una LAN TCP/IP en la que no se requiera ninguna comprobación, pero se conectan a un sistema principal remoto que requiere SSL, puede utilizar SSL en la conexión TCP/IP entre Communications Server para Linux y el sistema principal. Esto significa que la seguridad se comprueba una sola vez para todos los clientes y que los clientes individuales no tienen que proporcionar información de seguridad.
- Si Communications Server para Linux está instalado en la misma ubicación que el sistema principal, pero los clientes se conectan desde ubicaciones externas, puede utilizar SSL en las conexiones del cliente con Communications Server para Linux sin tener que instalar el software SSL en el sistema principal.

Funciones y ventajas

Communications Server para Linux presenta una serie de funciones y ventajas que van desde la simplificación de la configuración a la mejora del diagnóstico de problemas y del rendimiento de la red.

Una base sólida y versátil

Communications Server para Linux da soporte a la mayoría de entornos y funciones de nodo. En cualquier tipo de red, subárea o APPN, permite al sistema Linux funcionar como cualquiera de los siguientes elementos o como una combinación de ellos:

- Nodo dependiente de sistema principal
- Nodo igual (para ver una descripción de los nodos iguales APPN, consulte la descripción de las redes de igual a igual en "IBM Communications Server para Linux" en la página 1)

Funciones y ventajas

- Asociado (fuente o destino) en aplicaciones distribuidas
- Nodo de pasarela que interconecta redes SNA

Gracias a las API de gestión, el sistema Linux se puede configurar también para que funcione como punto de entrada de MS (Management Services) de manera que proporcione soporte para la gestión de red distribuida. En el nivel de enlace, el sistema Linux puede conectarse a varias LAN y WAN a través de cualquiera de los tipos de enlace soportados (descritos en “IBM Communications Server para Linux” en la página 1 y “Requisitos de instalación” en la página 20).

Trabajo en una configuración cliente/servidor

La configuración cliente/servidor proporciona las ventajas siguientes:

- Concentra los recursos SNA de los servidores, lo cual reduce la carga de trabajo de los clientes, mejora su rendimiento y minimiza el espacio de almacenamiento necesario para ofrecer servicios SNA a los clientes.
- Un solo enlace de datos se puede compartir entre múltiples usuarios de distintas máquinas, lo que elimina la necesidad de que cada máquina tenga una conexión de red SNA física.
- Múltiples servidores pueden proporcionar conectividad redundante (por ejemplo, múltiples servidores que ofrecen acceso al mismo sistema principal). Al tener múltiples vías de acceso para un recurso SNA permite el equilibrio de la carga entre los distintos servidores y en caso de que falle un servidor o enlace en particular proporciona inmediatamente uno de reserva.
- Al utilizar agrupaciones de LU en múltiples servidores, el administrador puede configurar y añadir servidores y usuarios con facilidad.
- Al tener menos enlaces y PU para la conectividad de sistema principal se reduce el tamaño de la definición VTAM del sistema principal.
- Los programas de utilidad de administración se pueden utilizar para configurar y gestionar los recursos de nodo (para cualquier sistema del dominio) y los recursos compartidos. El soporte de cliente/servidor proporcionado por las herramientas de administración de Communications Server para Linux permite una administración transparente de todos los recursos del dominio desde cualquier sistema en el dominio.
- Las aplicaciones SNA se pueden conectar mediante protocolos Internet utilizando TCP/IP y HTTPS para atravesar cortafuegos y para la autenticación y seguridad.

Fácil configuración

Communications Server para Linux está diseñado con opciones y posibilidades de configuración que reducen el tiempo de configuración y la complejidad de red. Por ejemplo:

Programa de administración de Motif

La forma más sencilla de definir y modificar la configuración de Communications Server para Linux es utilizar el programa de administración de Motif (**xsnaadmin**). Este programa ofrece una interfaz gráfica de usuario desde la que puede ver y gestionar los recursos de Communications Server para Linux. Este programa, además, simplifica la configuración mostrando sólo aquellos campos cuyos valores varían normalmente de una instalación a otra, utilizando los valores por omisión para los demás campos.

El programa de administración de Motif incluye pantallas de ayuda que ofrecen información general sobre SNA y Communications Server para

Linux, información de referencia para los diálogos de Communications Server para Linux y orientaciones para realizar tarea específicas.

Configuración dinámica en redes APPN

La configuración de un nodo o de una red también se hace más fácil por medio de la configuración dinámica de la red APPN. Por ejemplo, los nodos finales y las aplicaciones APPN registran dinámicamente los datos de configuración para soportar sesiones de LU 6.2, con lo que la configuración de las sesiones es opcional. Además, si el punto de control del nodo actúa como LU local por omisión, puede evitar toda la configuración de LU 6.2.

APPN también soporta la configuración dinámica de estaciones de enlace en ausencia de estaciones de enlace configuradas.

Opciones de interfaces de usuario adicionales para la administración

El programa de administración de Motif es la interfaz recomendada para configurar y gestionar Communications Server para Linux. Sin embargo, dispone de varias interfaces para Communications Server para Linux, que le permiten trabajar con la que mejor se adapte a su equipo, necesidades y preferencias.

Programa de administración de la línea de mandatos

El programa de administración de línea de mandatos (**snaadmin**) se puede utilizar para emitir mandatos con el fin de gestionar recursos individuales de Communications Server para Linux. Puede utilizar **snaadmin** directamente en el indicador de mandatos de Linux o en un script de shell.

API de NOF

La API de NOF de Communications Server para Linux proporciona las mismas funciones de gestión que el programa de administración de línea de mandatos y ofrece una interfaz adecuada para su utilización en un programa (en lugar de en un script de mandatos). Puede utilizar la API de NOF para escribir sus propios programas de aplicación para administrar Communications Server para Linux.

Mejor rendimiento

Communications Server para Linux mejora el alto rendimiento de las redes SNA y utiliza la operación de clase de servicio. Communications Server para Linux utiliza también la velocidad de la red mediante la compresión de datos SNA para los datos de sesión de LU 0–3 y mediante diferentes métodos de gestión del tráfico que equilibran el flujo del tráfico según el tamaño de la red:

- En redes APPN, Communications Server para Linux da soporte al direccionamiento de alto rendimiento (HPR) y el direccionamiento de sesiones intermedias (ISR), y proporciona opciones de red de conexión. Aunque ISR funciona de forma eficiente en redes pequeñas, causa un deterioro en el rendimiento de las redes grandes.
- En redes de gran tamaño que utilizan las opciones de conectividad LAN (por ejemplo, Token Ring o Ethernet) o que utilizan Enterprise Extender, también puede utilizar la opción de red de conexión para mejorar la eficacia de la comunicación. La opción de red de conexión crea una vía de comunicaciones directamente entre los nodos. Esto permite que el tráfico eluda los nodos de red intermedios.
- Otro método de control del tráfico, el de ritmo adaptable a nivel de sesión, ajusta automáticamente la congestión regulando la velocidad a la que las LU envían unidades de mensaje a las LU asociadas.

Opciones de seguridad

A medida que las redes se van haciendo más complejas y avanzan hacia una arquitectura abierta, la seguridad se convierte en una cuestión prioritaria. En la red SNA que ejecutan Communications Server para Linux, puede proteger la información mediante la definición de varios niveles de seguridad a través de la configuración y mediante la implementación de determinados tipos de enlace. Por ejemplo:

- En un sistema cliente/servidor, puede configurar un servidor WebSphere para proporcionar acceso HTTPS desde clientes Remote API Client a los servidores. Esto significa que las conexiones de los clientes se autentican utilizando certificados de seguridad. (Esta función requiere software adicional aparte del producto Communications Server para Linux estándar. Consulte “Requisitos de instalación” en la página 20 para ver más información.)
- Los usuarios de LU 6.2 pueden definir hasta tres niveles de seguridad: de sesión, de recurso y de conversación. El primero garantiza que participen las LU adecuadas en una sesión, el segundo restringe el acceso a todas las aplicaciones asociadas a una LU en particular y el último restringe el acceso a una aplicación en particular. Se puede obtener más seguridad mediante las rutinas de cifrado de datos.
- El servidor TN y el redirector TN de Communications Server para Linux pueden ofrecer cifrado de datos, autenticación de servidor y autenticación de cliente entre el servidor Communications Server para Linux y los clientes TN3270 o Telnet, utilizando el software SSL (Secure Sockets Layer). (Esta función requiere software adicional aparte del producto Communications Server para Linux estándar. Consulte “Requisitos de instalación” en la página 20 para ver más información.)

Flexibilidad de la gestión de la red

Communications Server para Linux da soporte al esquema de gestión de red Soporte de dominio múltiple-transporte de vectores de gestión de la red (MDS-NMVT) que puede funcionar como un esquema de gestión centralizado, distribuido o jerárquico. Se basa en una arquitectura de punto focal/punto de entrada que ofrece un alto grado de flexibilidad.

Los puntos focales son nodos de control que gestionan la red de acuerdo con los datos que recopilan de los puntos de entrada (aplicaciones de gestión que residen en el resto de nodos de la red).

- En la gestión centralizada, un solo punto focal actúa como punto de control para toda la red.
- En la gestión distribuida, varios puntos focales se reparten la gestión de la red.
- En la gestión jerárquica, los puntos focales están anidados según su función.

De este modo, MDS-NMVT puede adaptarse para gestionar redes de subárea, redes APPN estándar y redes APPN de grandes dimensiones.

Fiabilidad, disponibilidad y facilidad de mantenimiento

Para ayudar a mantener un funcionamiento fiable del sistema, Communications Server para Linux proporciona un conjunto de funciones de visualización y herramientas de diagnóstico de problemas.

- El programa de administración de Motif proporciona herramientas de configuración y gestión mejoradas, que incluyen lo siguiente:
 - Actualizaciones inmediatas de información de configuración

- Información de estado para enlaces, sesiones y recursos de nodo
- Los mandatos de consulta y de estado le ofrecen información sobre:
 - Sesiones LU-LU
 - Sesiones intermedias APPN
 - Enlaces activos
 - Bases de datos de topología APPN, que almacenan información sobre enlaces
- Existen diversas herramientas de diagnóstico de problemas disponibles para ayudarle durante las diferentes etapas de configuración y funcionamiento. Entre ellas se incluyen:
 - Herramienta de recopilación de información de diagnóstico (**snagetpd**), que le permite recopilar fácilmente información de servicio.
 - Mensajes de estado y de error, que le ayudan a resolver problemas relacionados con las rutinas de configuración y con el funcionamiento del sistema.
 - Archivos de anotaciones, que le permiten recopilar información de error, anomalía y auditoría de la red.
 - Recursos de rastreo para recopilar información detallada sobre problemas y dar formato a ésta.

Otros programas de utilidad le ayudan a probar la conectividad de enlaces y la comunicación entre aplicaciones.

Communications Server para Linux también incluye la API de Management Services, que se utiliza para desarrollar herramientas para enviar y recibir alertas de red y datos de problemas.

Todas estas herramientas de gestión y diagnóstico de problemas están totalmente integradas en el modelo cliente/servidor de Communications Server para Linux, por lo que puede gestionar todo el dominio de Communications Server para Linux o recopilar información de diagnósticos desde un solo punto de la red.

Integración, crecimiento y cambio de la red

Para dar soporte a la integración, el crecimiento y el cambio de la red, se pueden utilizar las API de Communications Server para Linux para desarrollar aplicaciones para LU, una plataforma o un sistema operativo en particular, según las necesidades de la empresa. CPI-C es una API de especial importancia porque es coherente a través de las diferentes plataformas y de los distintos sistemas operativos. Se utiliza para desarrollar aplicaciones que puedan ejecutarse en cualquier sistema.

Enterprise Extender también proporciona un mecanismo de integración de las redes SNA y TCP/IP.

Capítulo 2. Planificación de la red e IBM Communications Server para Linux

Este capítulo ofrece una visión general de las fases de planificación de una red que ejecuta Communications Server para Linux. También resume las funciones que se pueden configurar para el sistema Linux y presenta las directrices para calcular los recursos necesarios para dar soporte a las funciones.

Tareas de planificación de la red

Este apartado presenta algunas directrices generales para planificar, configurar y gestionar redes a través del uso de varios programas de utilidad de Communications Server para Linux y de Linux.

Planificar una red supone equilibrar las funciones, el rendimiento, los recursos y el coste. Aunque no existe ninguna planificación única ideal para una red, algunas directrices generales pueden serle útiles para asegurarse de que ésta satisface sus necesidades. Para planificar una red, realice las siguientes acciones:

- Determine las funciones que debe proporcionar la red (tales como la transferencia de archivos o la emulación 3270) y sus necesidades de rendimiento.
- Determina cómo puede configurarse Communications Server para Linux de manera que proporcione las funciones que necesita.
- Calcula los recursos necesarios para instalar Communications Server para Linux, dar soporte a los requisitos de rendimiento y de capacidad y dar soporte a las funciones de Communications Server para Linux e identificar los costes asociados.

Identificación de las necesidades funcionales de la red

Para determinar las funciones que debe proporcionar la red, debe plantearse las preguntas siguientes:

- ¿Se debe utilizar una red APPN?
- ¿Communications Server para Linux se ejecutará como un sistema cliente/servidor? Si es así, ¿trabajarán todos los sistemas en un solo dominio Communications Server para Linux o debo definir dos o más dominios separados?
- ¿Necesito más de un servidor en el dominio Communications Server para Linux para proporcionar equilibrio de la carga de trabajo a los recursos de conectividad? Si es así, ¿qué servidor será el servidor de configuración maestro? ¿Debo proporcionar uno o varios servidores de configuración de reserva?
- ¿Necesito dar soporte a clientes Remote API Client que se conecten a servidores Communications Server para Linux utilizando HTTPS?
- ¿Se ejecutarán las aplicaciones de usuario en el servidor o en sistemas cliente Linux?
- ¿Ofrecerá el servidor recursos de conectividad para aplicaciones Windows (como por ejemplo programas de transacciones de API) que se ejecuten en clientes Windows?
- ¿Debe cada servidor ser un punto final para las sesiones o debe ser uno de los tipos de pasarela siguientes?
 - APPN

Tareas de planificación de la red

- LU 0
- LU 2
- Servidor TN o redirector TN
- ¿Qué tipos de enlace físico utilizará la red?
- ¿Communications Server para Linux necesitará dar soporte a IPv4, IPv6 o a ambos tipos de conexiones?

Las respuestas a estas preguntas le ayudarán a determinar las funciones de Communications Server para Linux que necesita la red.

Determinación de la configuración de Communications Server para Linux

Para determinar cómo debe funcionar Communications Server para Linux, debe decidir primero cómo debe fluir el trabajo en la red. Debe plantearse las preguntas siguientes:

- ¿Qué recursos (como, por ejemplo, aplicaciones) debe haber disponibles en la red?
- ¿Cuántos usuarios necesitan acceder a los recursos remotos?
- ¿Con qué frecuencia se accede a cada uno de los recursos?
- ¿Cuántos usuarios tienen acceso a la red?
- ¿Cómo se direccionarán por la red las peticiones de usuario?

Puede configurar Communications Server para Linux de manera que dé soporte a muchas funciones, entre las que se incluyen por ejemplo las siguientes:

- Nodo de red APPN para el direccionamiento de sesiones intermedias (ISR).
- Nodo final APPN (que se comunica de forma autónoma con los nodos adyacentes pero que utiliza servicios de nodo de red APPN para comunicarse con los nodos iguales no adyacentes).
- Nodo LEN (que se comunica directamente con los nodos adyacentes o con los nodos configurados de modo que parezcan adyacentes).
- Uso de LU 0, LU 1, LU 2, LU 3 y LU 6.2 (dependientes e independientes).
- Conexión de pasarela SNA a un sistema principal

Puede configurar una o más funciones para un nodo determinado, según sus necesidades. Por ejemplo, puede configurar Communications Server para Linux como nodo de red APPN para que proporcione servicios de direccionamiento e ISR y utilizar el mismo nodo para que la pasarela SNA dirija las sesiones LU dependientes como, por ejemplo, LU 0 y LU 2. De forma similar, puede configurar Communications Server para Linux para que ejecute el servidor TN y proporcione soporte a una base de datos compartida, así como una conexión de LU 6.2 independiente con MQSeries en el sistema principal.

Identificación de las necesidades de recursos para la instalación y el funcionamiento

Para calcular el soporte para las funciones de Communications Server para Linux, debe responder a las preguntas siguientes:

- ¿Qué aptitudes debe tener el personal?
- ¿Qué medios de transporte tengo previsto utilizar?
- ¿Cuáles son los requisitos de instalación para la configuración escogida?
- ¿Cuánta memoria y cuánto espacio de paginación necesito para trabajar?

Las respuestas a estas preguntas le ayudarán a identificar los tipos de recursos que Communications Server para Linux utiliza cuando se configura para dar soporte a una o varias funciones descritas en el apartado "Identificación de las necesidades funcionales de la red" en la página 17. Responder a las preguntas también le ayudará a comprender la relación entre las funciones de Communications Server para Linux, los recursos de Linux y los recursos de red.

El modo en que asigne los recursos a los nodos determinará el rendimiento de la red.

Requisitos de personal

Para instalar, utilizar y ajustar Communications Server para Linux necesita lo siguiente:

- Administradores de red, que planifican la red, añaden nuevos dispositivos y mantienen o mejoran el rendimiento global de la red.
- Administradores del sistema, que instalan y mantienen Communications Server para Linux y el hardware en el que funciona y configuran los sistemas para la conexión de red.
- Programadores, que desarrollan aplicaciones personalizadas tales como programas de transacciones o rutinas de gestión de red.

Los administradores de la red y del sistema deben estar completamente familiarizados con el hardware en el que Communications Server para Linux funciona y con el sistema operativo de Linux. Deben conocer las redes a las que están conectados diversos sistemas y deben entender los conceptos generales de SNA. También deben tener los conocimientos siguientes:

- La interfaz de Motif
- **rpm**, la herramienta de instalación de Linux
- TCP/IP, si tienen previsto utilizar las funciones de cliente/servidor, servidor TN o Enterprise Extender
- El sistema operativo Windows 2000, Windows XP, Windows 2003 Server, Windows Vista, o Windows Server 2008, si el sistema Communications Server para Linux incluye clientes Remote API Client en Windows
- WebSphere Application Server, si el sistema Communications Server para Linux incluye clientes Remote API Client que se conecten a servidores utilizando HTTPS

Los programadores que desarrollen aplicaciones personalizadas para SNA deben tener experiencia en el manejo del lenguaje C (o Java si utilizan CPI-C de Java) y deben estar familiarizados con las API que están disponibles en Communications Server para Linux.

Medios de transporte

Es posible que Communications Server para Linux necesite compartir el medio de transporte subyacente (como SDLC o Token Ring) con otros protocolos de comunicación. Por tanto, los requisitos de ancho de banda de la capa física deben tener en cuenta la totalidad de protocolos y aplicaciones que comparten el medio de transporte.

Nota: Communications Server para Linux puede compartir los adaptadores de Token Ring y Ethernet con otros protocolos, como por ejemplo TCP/IP. Probablemente necesite especificar las direcciones de punto de acceso a servicio (SAP) exclusivas para cada protocolo que va a utilizar.

Requisitos de instalación

Las funciones que asigne a Communications Server para Linux (del apartado “Identificación de las necesidades funcionales de la red” en la página 17) determinan también los requisitos de instalación. Este apartado ofrece una visión general de los recursos del sistema necesarios para instalar Communications Server para Linux. Para obtener más información, consulte la documentación suministrada con cada producto (consulte la bibliografía para obtener una lista de los manuales).

Hardware

Requisitos de Communications Server para Linux Un sistema soportado por alguna de las siguientes distribuciones de Linux.

Utilice el mandato **uname -m** para verificar la clase de CPU del sistema de destino. La tabla siguiente muestra el hardware adecuado para cada tipo de servidor y la respuesta de **uname -m** para este hardware.

Tipo de servidor	Hardware	Respuesta de uname
Intel de 32	Sistema Intel Pentium II o posterior de 32 bits	i686
x86_64 de 64 bits	Sistema AMD64 o Intel EM64T	x86_64
pSeries	Sistema pSeries POWER5 u OpenPower	ppc64

Sistema operativo Linux

Antes de instalar y utilizar Communications Server para Linux en la estación de trabajo Linux, ésta debe tener instalada la versión adecuada del sistema operativo Linux.

Communications Server para Linux da soporte a las siguientes variantes de Linux. Para obtener información actualizada acerca de los números de versión y las generaciones de kernel a los que se da soporte para cada variante y cualquier requisito adicional para versiones en concreto, consulte el archivo **README** en la imagen del CD de 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)
- SUSE Linux Enterprise Server 11 (SLES11)

Seguridad mejorada de Linux (SE Linux) de las distribuciones de Linux permiten que Linux supervise y controle el acceso a ciertas funciones y bibliotecas de códigos. En función del nivel de la distribución de Linux que se haya instalado, será necesario realizar algunos cambios en la configuración para habilitar Communications Server para Linux y Linux Streams. Para ver cuáles son, consulte la página web de soporte de Communications Server para Linux <http://www.ibm.com/software/network/commserver/support> para obtener información sobre cómo configurar el sistema para SE Linux.

Hardware de enlace

El hardware de enlace sólo se requiere en el servidor no en el cliente.

La instalación de un PC en una o varias redes requiere enlaces adecuados para el protocolo de comunicación de red seleccionado. El hardware de

enlace consiste en un adaptador de comunicaciones que se instala en el sistema y el cable correspondiente para la conexión a la red (también se necesita el software de controlador).

Nota:

1. Los adaptadores de comunicaciones deben instalarse con cables del mismo tipo. Por ejemplo, un adaptador Ethernet necesita un cable Ethernet para que funcione el enlace.
2. Si utiliza Enterprise Extender como único tipo de enlace, no necesitará los adaptadores que se indican en este apartado; pero deberá disponer de uno de los adaptadores que TCP/IP requiere.
3. Si necesita habilitar el adaptador de la interfaz de Linux para una conexión LAN Ethernet o LAN Token-Ring LLC2 y no hay dirección IP asignada al adaptador de la interfaz, consulte el archivo **README** en la imagen de CD de Communications Server para Linux para obtener detalles sobre cómo habilitar la configuración de Linux para que ofrezca esta función.

Communications Server para Linux da soporte a adaptadores de comunicaciones para los siguientes protocolos de enlace:

- Token Ring
- Ethernet (estándar o IEEE 802.3)
- SDLC
- X.25 QLLC

Los siguientes protocolos de enlace necesitan otros productos o funciones que no están incluidos en Communications Server para Linux:

- SDLC o X.25 (necesita un adaptador y un controlador)

Para obtener información sobre los adaptadores que se han probado con Communications Server para Linux, consulte <http://www.ibm.com/software/network/commsserver/linux>. Si desea realizar alguna pregunta sobre el adaptador o hardware adecuado para sus necesidades, póngase en contacto con su representante de ventas de IBM.

Software adicional: Linux

Communications Server para Linux necesita el siguiente software adicional. Consulte el fichero **README** en la imagen de CD de Communications Server para Linux para obtener más detalles de los requisitos de la versión específica (dependiendo de la variante de Linux que tenga) e instrucciones sobre cómo instalar esos paquetes de software.

- LiS Streams. Consulte el archivo **README** para ver los detalles de la versión de LiS Streams requerida y las instrucciones de instalación.
- OpenMotif (sólo se requiere en un servidor no en un cliente). Esto es necesario para utilizar el programa de administración de Motif, que es el método recomendado de configuración y gestión de Communications Server para Linux.
- Java (necesario si desea utilizar CPI-C de Java). Necesitará Java Runtime Environment (JRE). Si necesita compilar nuevas clases de Java para utilizarlas con una aplicación de CPI-C de Java, necesitará el SDK de Java.

WebSphere Application Server (para el acceso de HTTPS)

Si utiliza un sistema cliente/servidor en el que los clientes Remote API Client se conectan con servidores de Communications Server para Linux

Tareas de planificación de la red

utilizando HTTPS, deberá ejecutar WebSphere Application Server para que estos clientes accedan a los servidores mediante HTTPS.

Communications Server para Linux trabaja con WebSphere Application Server versión 5, que se puede instalar en un sistema que ejecute cualquier sistema operativo soportado por WebSphere. (Si es necesario, se puede instalar en el mismo sistema Linux como un servidor de Communications Server para Linux). Consulte la documentación de WebSphere Application Server para obtener más información sobre cómo instalarlo. Necesitará también instalar un plug-in adicional de Communications Server para Linux en el sistema para utilizar WebSphere con Communications Server para Linux, como se describe en “Configuración de WebSphere Application Server” en la página 34.

Memoria y almacenamiento

Para dar soporte a un conjunto completo de configuraciones y servicios, una estación de trabajo que ejecute Communications Server para Linux necesita el mínimo de memoria requerido para la distribución de Linux más 64 MB y 200 MB de espacio en el disco duro. Además, durante la instalación se necesitan 250 MB de almacenamiento temporal.

Si decide instalar la documentación de Communications Server para Linux en formato de copia software (PDF), necesitará almacenamiento de disco fijo adicional. Para instalar todos los manuales en copia software, necesitará 80 MB de espacio de disco.

Nota: Los requisitos de memoria y de disco fijo para otros programas bajo licencia, aplicaciones de usuario y datos no se incluyen en estos requisitos; revise con detenimiento todos los requisitos del sistema, memoria y disco fijo con el representante de IBM o distribuidor del sector autorizado.

Configuraciones avanzadas

Si tiene previsto ejecutar aplicaciones que requieren más que una configuración básica, necesitará planificar recursos informáticos adicionales.

En general, los requisitos de memoria y de almacenamiento para ejecutar Communications Server para Linux dependen de muchos factores distintos que varían según la función de la estación de trabajo Linux y el entorno de la misma. Sin embargo, si aplicamos la regla empírica de que las LU, los enlaces activos y las sesiones activas son los que más recursos informáticos consumen, se puede calcular la cantidad de memoria adicional y de espacio de disco que se necesita para soportar las aplicaciones más exigentes.

Requisitos de memoria y almacenamiento para el funcionamiento

Este apartado describe los requisitos de memoria y almacenamiento de una estación de trabajo que ejecuta Communications Server para Linux.

Memoria de kernel

Linux utiliza memoria de kernel para permitir la comunicación entre los subsistemas de comunicación y los DLC. La memoria de kernel es un recurso compartido que debe gestionarse a nivel del sistema.

Communications Server para Linux utiliza memoria de kernel para enviar y recibir datos a través de la red, pero tan sólo es uno de los subsistemas que utiliza memoria de kernel. La utilización de recursos de memoria de kernel por parte de Communications Server para Linux puede afectar al

rendimiento de otros subsistemas como, por ejemplo, TCP/IP o NFS. Coordine con el administrador de la red la determinación de los requisitos de memoria de kernel.

Almacenamiento en memoria, en disco y de paginación

Communications Server para Linux utiliza almacenamiento principal (también conocido como memoria principal y memoria RAM [memoria de acceso aleatorio]), almacenamiento en disco permanente y almacenamiento en disco de paginación (también conocido como espacio de paginación):

- Los bloques de control para los recursos SNA (como LU, enlaces y sesiones) consumen almacenamiento principal.
- La memoria de kernel sólo consume almacenamiento principal.
- Los archivos ejecutables, los archivos de configuración y las publicaciones con copia software de Communications Server para Linux consumen almacenamiento en disco permanente.
- Los programas de aplicación, las sesiones y los procesos relacionados tienen requisitos de espacio de paginación que consumen almacenamiento en disco permanente.

Los requisitos de memoria y de almacenamiento en disco dependen de varios factores, que difieren ampliamente de un entorno a otro. Los programas de transacciones (TP) y las sesiones SNA son los que más memoria y almacenamiento en disco consumen.

Un TP es un programa que utiliza la interfaz de programas de aplicación (API) SNA para acceder a la red. Una sesión es un canal lógico temporal entre dos LU en nodos asociados. Los TP utilizan este canal para comunicarse entre ellos.

El consumo de memoria y de almacenamiento en disco se ve afectado en gran medida por el número global de sesiones, el número de sesiones asignadas (conversaciones), la intensidad de tráfico de las conversaciones y el número de TP de usuario activos. Los requisitos de memoria dependen principalmente de la intensidad del tráfico de datos y la utilización resultante de memoria de kernel. Los requisitos de almacenamiento en disco se derivan de los requisitos de espacio de paginación de los TP, las sesiones y los procesos relacionados.

Para todos los tipos de LU, se distingue entre una sesión desocupada y una sesión asignada. Una sesión desocupada es una sesión activa que no está siendo utilizada por programas TP. Una sesión asignada es una sesión que soporta una conversación activa. Para calcular la cantidad total de memoria necesaria, debe calcular la intensidad de tráfico y la parte del número global de sesiones que estarán asignadas, como promedio, en un momento dado cualquiera. También puede configurar el sistema de modo que maneje la demanda más elevada. Estos cálculos varían según los entornos.

Si la carga de la sesión supera la capacidad de memoria del sistema, esto supondrá un coste de paginación.

Procesos

Communications Server para Linux requiere un mínimo de 20 procesos.

Direccionamiento IPv4 e IPv6

Los sistemas que ejecutan Communications Server para Linux Versión 6.4 pueden utilizar las direcciones IPv4 o IPv6 con las siguientes restricciones.

Direccionamiento IPv4 e IPv6

- Todos los servidores en un dominio de cliente/servidor deben utilizar el mismo formato de direccionamiento (IPv4 o IPv6).
 - Si los servidores utilizan IPv4, los clientes también deben utilizar IPv4.
 - Si los servidores utilizan IPv6, los clientes pueden utilizar tanto IPv6 como IPv4.
- Para el servidor TN, si Communications Server para Linux utiliza IPv4, los clientes TN que se conectan al servidor TN también deben utilizar IPv4. Si Communications Server para Linux utiliza IPv6, los clientes TN pueden utilizar tanto IPv6 como IPv4. De forma predeterminada, el servidor TN acepta conexiones de ambos tipos de cliente, pero puede configurarlo de forma que escuche una dirección IP en concreto (utilizando el parámetro *listen_local_address* del programa de administración de la línea de mandatos o una aplicación NOF) para restringirlo a un tipo de conexión de cliente.
- Para el redirector TN, si Communications Server para Linux utiliza IPv4, ambas conexiones TCP/IP (del cliente a Communications Server para Linux y de Communications Server para Linux al host) deben utilizar también IPv4. Si Communications Server para Linux utiliza IPv6, la conexión TCP/IP del cliente a Communications Server para Linux sigue las mismas reglas que para el servidor TN. La conexión desde Communications Server para Linux hacia el host puede utilizar tanto IPv6 como IPv4. No existe ningún requisito para que las dos conexiones utilicen el mismo formato de direccionamiento.
- Para Enterprise Extender (HPR/IP), los puertos de ambos extremos de un enlace deben utilizar el mismo formato de direccionamiento (IPv4 o IPv6).
 - Si Communications Server para Linux utiliza IPv4, sólo se puede conectar a sistemas remotos que estén configurados para soportar IPv4.
 - Si Communications Server para Linux utiliza IPv6, puede configurarlo para que utilice IPv4 o IPv6 en un enlace de Enterprise Extender. La opción que elija debe coincidir con la configuración del sistema remoto.Además, todos los enlaces del mismo puerto de Enterprise Extender deben utilizar el mismo formato de direccionamiento (IPv4 o IPv6). Si necesita soportar enlaces con distintos formatos de direccionamiento, deberá utilizar puertos separados. De forma similar, todos los puertos de Enterprise Extender en la misma red de conexión deberán utilizar el mismo formato de direccionamiento.

Para comprobar si un servidor de Communications Server para Linux se está ejecutando en IPv4 o IPv6, utilice el mandato **ifconfig -a** y mire la dirección o direcciones IP en la salida. Habrá direcciones en formato decimal con puntos IPv4, direcciones hexadecimales IPv6 o ambas. Para un cliente Remote API Client en Windows, el mandato equivalente es **ipconfig** (sin ninguna opción de línea de mandatos). Si precisa cambiar el formato de direccionamiento de la IP del sistema, consulte la documentación del sistema operativo.

Si está actualizando un sistema existente de Communications Server para Linux a la versión 6.4 tal y como se describe en “Migración desde niveles anteriores de Communications Server para Linux” en la página 29, y desea cambiar también el direccionamiento IPv6, puede realizar los dos procesos en cualquier orden. No obstante, no podrá utilizar las nuevas posibilidades de direccionamiento IPv6 en la versión 6.4 hasta que se hayan completado los dos procesos.

- Para un sistema cliente/servidor deberá cambiar todos los servidores del dominio de IPv4 a IPv6 a la vez; no intente ejecutar un dominio mixto de servidores IPv4 e IPv6.
- Debido a que la actualización a Communications Server de Linux, versión 6.4, también requiere la actualización de todos los servidores a la vez, puede realizar

el cambio a un direccionamiento IPv6 a la misma vez que actualiza cada servidor. De forma alternativa, puede modificar todos los servidores en IPv6, ya sea antes o después de efectuar una actualización a la versión 6.4, lo que sea más conveniente.

- Tras modificar todos los servidores para utilizar el direccionamiento IPv6, puede cambiar clientes Remote API Client para utilizar el direccionamiento IPv6, según se necesite. Los clientes IPv4 puede continuar funcionando con servidores IPv6, por lo que no es necesario cambiar todos los clientes a la vez.

Si está instalando un nuevo sistema Communications Server para Linux, puede instalarlo sólo con direccionamiento IPv6 en todos los servidores y clientes o puede utilizar inicialmente el direccionamiento IPv4 y posteriormente pasar a IPv6 (sujeto a las restricciones citadas anteriormente para dominios de cliente/servidor).

Compatibilidad asegurada entre configuraciones de distintas plataformas

Los productos SNA que se ejecutan en diferentes plataformas (tales como IBM Personal Communications o Communications Server para Windows o VTAM NCP en un sistema principal) pueden trabajar con Communications Server para Linux si se cumplen determinados requisitos.

Por lo general, el release actual de un producto de red SNA podrá funcionar con Communications Server para Linux siempre que de soporte a nodos PU 2.1 y como mínimo a uno de los tipos de enlace soportados por Communications Server para Linux. Sin embargo, puede que algunos releases muy antiguos (como VTAM V2) no funcionen de manera fiable. Las posibilidades de cada producto de redes vienen documentadas en su guía del usuario correspondiente.

Otros factores que se deben tener en cuenta son los siguientes:

- Si utiliza LU 6.2 independientes y su red no es APPN, necesita asegurarse de que las LU asociadas están definidas para el sistema local.
- Debido a que los valores por omisión para los tamaños de ventana y los temporizadores de DLC varían de un dispositivo a otro, debe asegurarse de que sus dispositivos remotos utilicen el valor correcto. Por ejemplo, un tamaño de ventana de DLC que proporcione un buen rendimiento con un nodo Communications Server para Windows puede no funcionar bien con un nodo 3172.
- Cuando trabaje en un entorno heterogéneo (protocolos TCP/IP y SNA en la misma LAN) con varios segmentos de LAN, asegúrese de que sus dispositivos de interconexión de la LAN puedan simultáneamente “direccionar” TCP/IP y “crear puentes” para tramas SNA.

Convenios de denominación

Puede utilizar identificadores de red para segmentar lógicamente su red física. Asimismo, si tiene previsto conectarse con otras redes, le recomendamos encarecidamente que registre sus identificadores de red para evitar conflictos de denominación de redes.

Puede definir los nombres de red y de LU de la siguiente forma:

Nombres de red

Puede definir diferentes nombres de red (identificadores de red) para poder segmentar las redes APPN. La segmentación limita el tamaño de las

Convenios de denominación

bases de datos de topología de red y la frecuencia de las peticiones LOCATE de difusión a través de cada red.

Para garantizar la exclusividad de un ID de red, el administrador de la red puede registrar el identificador en el registro mundial de IBM. El registro de IBM garantiza que todos los ID de red son exclusivos entre los que están registrados en él. Los estándares de registro son coherentes con los de OSI (Interconexión de sistemas abiertos) , incluidos los códigos OSI de país, tal como han sido establecidos por la organización ISO (Organización internacional para la estandarización). Para ver más información sobre los registros, consulte el manual *User's Guide for SNA Network Registry*.

Nombres de LU

Puede utilizar comodines para los nombres de LU para minimizar la definición del sistema y las búsquedas en la red.

Capítulo 3. Instalación de Communications Server para Linux en servidores Linux

Este capítulo ofrece información general sobre los pasos que debe seguir para instalar Communications Server para Linux en un servidor Linux. Para ver instrucciones detalladas paso a paso sobre el proceso de instalación, consulte el archivo **README** en el CD de imagen de Communications Server para Linux, el cual ofrece información detallada y actualizada específica de la variante de Linux que tenga. El archivo **README** incluye:

- Los nombres exactos de los paquetes y/o los números de versión de los paquetes de software adicionales que necesita
- Los detalles de la instalación y los mandatos de configuración.

Empaquetado del programa bajo licencia de Communications Server para Linux

El programa bajo licencia Communications Server para Linux se suministra como tres imágenes de CD que contiene lo siguiente.

CD 1: Inicio rápido

Este CD contiene un completo conjunto de documentación en PDF relativa a Communications Server para Linux (en el directorio **/DOCS**).

CD 2: Servidor

Este CD contiene los archivos necesarios para instalar un servidor:

- los archivos **README** que contienen información sobre cualquier cambio del producto posterior a la publicación de Communications Server para Linux
- Los scripts de instalación
- Las imágenes de instalación para el servidor y para los manuales en PDF

CD 3: Clientes

Este CD contiene los archivos **README**, los scripts de instalación y las imágenes de instalación que se necesitan para instalar cada tipo de cliente:

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

Consulte los archivos **README** para obtener todos los detalles de los archivos incluidos en las imágenes del CD.

Nota: para ver los requisitos de almacenamiento, consulte “Requisitos de instalación” en la página 20.

Preparación de la instalación de Communications Server para Linux

Antes de instalar Communications Server para Linux, realice las siguientes tareas:

- Asegúrese de que el PC Linux no se ejecute con las funciones de Gestión de energía habilitadas.
- Asegúrese de que estén instalados todos los requisitos previos de software que se indican en el apartado “Requisitos de instalación” en la página 20.

Los siguientes apartados ofrecen información acerca de estas tareas.

Inhabilitación de las funciones de Gestión de energía

Antes de instalar Communications Server para Linux, debe comprobar si el PC Linux incluye Gestión avanzada de energía y, si es así, debe asegurarse de que las funciones estén inhabilitadas. Ahora, muchos PC disponen de estas funciones que se han diseñado para ahorrar energía si no se utilizan el teclado o el ratón (mediante la suspensión de la energía para dispositivos como, por ejemplo, las unidades de discos, y la reducción de la velocidad de reloj de CPU). La Administración avanzada de energía está diseñada para utilizarla en el PC como estación de trabajo; no es adecuada cuando el PC funciona como servidor, ya que un servidor puede funcionar con normalidad sin que se produzca ninguna actividad de teclado ni de ratón.

Para inhabilitar estas funciones, acceda a la configuración del BIOS durante el arranque del PC (normalmente, deberá pulsar **F1** al inicializar el hardware) e inhabilite la Gestión avanzada de energía y la Gestión de energía del hardware.

Para eliminar la función de Gestión avanzada de energía del PC, utilice el mandato siguiente.

```
rpm -e apmd
```

Instalación de software como requisito previo

Antes de instalar Communications Server para Linux, debe instalar el software de requisito previo que se indica en el apartado “Requisitos de instalación” en la página 20:

- LiS Streams
- OpenMotif
- Java
- SSL

Para ver todos los detalles de los paquetes de software necesarios y las instrucciones paso a paso para instalarlos, consulte el archivo **README** de la imagen del CD de Communications Server para Linux.

Visualización de información detallada sobre la instalación del producto

Puede visualizar información acerca de los paquetes de Communications Server para Linux y otros paquetes de software relacionados que ya estén instalados. Para ver todos los paquetes instalados, utilice el mandato siguiente:

```
rpm -q -a
```

Preparación de la instalación de Communications Server para Linux

Para ver más detalles de un paquete específico, utilice el mandato siguiente:

```
rpm -q -i nombrepaquete
```

nombrepaquete es el nombre base del paquete instalado, por ejemplo, **ibm-commserver**.

Cambio de la variable de entorno de idioma

Cuando utilice Communications Server para Linux, asegúrese de que la variable LANG esté configurada correctamente para que indique el idioma que desea utilizar.

Utilice el mandato siguiente para cambiar la variable LANG:

```
export LANG=idioma
```

Sustituya *idioma* por el identificador del idioma que desea utilizar, que puede ser uno de los siguientes:

Identificador	Idioma
en_US	Inglés (Estados Unidos)
ja_JP	Japonés (PC)
de_DE	Alemán
es_ES	Español
fr_FR	Francés
ko_KR	Coreano
pt_BR	Portugués
zh_CN	Chino (EUC simplificado)
zh_TW	Chino (tradicional)

Migración desde niveles anteriores de Communications Server para Linux

Consideraciones

Si está actualizando a Communications Server para Linux versión 6.4 desde una versión anterior de Communications Server para Linux, deberá tener en cuenta lo siguiente.

1. Si está ejecutando Communications Server para Linux en una configuración de cliente/servidor con dos o más servidores, es recomendable actualizar todos los servidores a la versión 6.4 a la vez antes de actualizar los clientes Remote API Client.
 - Durante el proceso de migración de servidores no podrá utilizar el programa de administración para Motif ni el programa de administración de la línea de mandatos en un servidor anterior para ver y gestionar recursos de un servidor ejecutando la versión 6.4.
 - Las versiones 6.3.1.0 y posteriores del cliente Remote API Client funcionarán con un servidor existente, pero sólo si el sistema operativo del cliente no está configurado para utilizar IPv6.
 - Las versiones anteriores del cliente Remote API Client no funcionarán con la versión 6.4 de Communications Server para Linux.
2. Varias estructuras de datos en la API de NOF se han modificado para aceptar formatos de dirección más largos de los que las direcciones IPv6 necesitan. Esto quiere decir que si utiliza cualquiera de los siguientes verbos y/o indicaciones

Migración desde niveles anteriores de Communications Server para Linux

en una aplicación NOF existente creada antes de la versión 6.2.3.0 (incluso si no está utilizando las nuevas posibilidades de direccionamiento de IPv6), deberá volver a compilar la aplicación para utilizarla con Communications Server para Linux versión 6.4.

- DEFINE_LS, DEFINE_PORT, QUERY_LS, QUERY_PORT cuando se utilice con un Enterprise Extender (HPR/IP), una LS o un puerto
 - 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 cualquier tipo de LU)
 - TN_REDIRECTION_INDICATION
3. Si desea utilizar las nuevas posibilidades de direccionamiento IPv6 de la versión 6.4, debe asegurarse de que los servidores de Communications Server para Linux están configurados para utilizar direccionamiento IPv6. Consulte “Direccionamiento IPv4 e IPv6” en la página 23 para obtener más detalles.
 4. Si está ejecutando SDLC o X.25 (QLLC) con un adaptador OEM, deberá contactar el OEM para obtener los controladores actualizados. Los controladores 6.2.2 no funcionan con Communications Server para Linux 6.2.3 ni 6.4.

Proceso de migración

Si ya tiene instalada una versión anterior de Communications Server para Linux y ahora está migrando a la versión 6.4 necesita seguir los pasos siguientes:

Guarde los archivos de configuración personalizados

Si existe alguno de los archivos indicados a continuación, guárdelo en un directorio temporal. No existirán todos estos archivos en todas las instalaciones.

```
/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/ibm/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
```

Además, si ha personalizado el archivo de arranque `/etc/rc.d/init.d/snastart` tal y como se describe en “Habilitación de Communications Server para Linux” en la página 74 para eliminar el mandato `sna start` para que Communications Server para Linux no se inicie automáticamente durante el arranque, debe anotar los cambios que haya hecho en este archivo.

Desinstale el release anterior

Utilice los siguientes mandatos para detener Communications Server para

Migración desde niveles anteriores de Communications Server para Linux

Linux y desinstalarlo. En función de la versión anterior instalada y de la forma en que se haya instalado, puede que su sistema no incluya todos los paquetes RPM que se indican.

```
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
```

Desinstale LiS

Utilice los mandatos siguientes para desinstalar el nivel actual del paquete fuente abierto de LiS.

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

Cambie PATH y otras variables de entorno

Si ha modificado alguna de las variables de entorno siguientes para la versión anterior de Communications Server para Linux, debe eliminar los cambios que ha realizado, porque las vías de acceso pueden ser diferentes para el producto del programa Communications Server para Linux versión 6.4.

```
PATH
LD_LIBRARY_PATH
LD_RUN_PATH
LD_PRELOAD
CLASSPATH
```

Es aconsejable utilizar el mandato **env** para comprobar todas las variables de entorno para ver las referencias a **sna**:

```
env | grep sna
```

Otros paquetes

Se recomienda comprobar la instalación de Java y actualizarla hasta el último nivel si es necesario.

Limpieza final

Los siguientes mandatos eliminarán cualquier elemento que quede del nivel anterior del producto. En función de la versión anterior instalada, puede que su sistema no incluya todos los directorios que se indican.

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

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

Migración desde niveles anteriores de Communications Server para Linux

Instale el nuevo nivel del producto del programa Communications Server para Linux versión 6.4

Siga las instrucciones de este manual y del archivo **README** para instalar el producto.

Restablezca la configuración que ha guardado

Si ha guardado algún archivo de configuración en el primer paso de este proceso, ahora puede restaurarlo. En primer lugar, detenga el software de Communications Server para Linux utilizando el siguiente mandato:

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

Si ha guardado algún archivo **ibmcs.*** en el primer paso de este proceso, elimine todos los archivos **ibmcs.*** del directorio **/etc/opt/ibm/sna** ahora. Por ejemplo, si ha guardado **ibmcs.kdb** y **ibmcs.sth**, debe eliminar **ibmcs.crl** y **ibmcs.rdb** aunque no haya guardado ningún archivo para sustituirlos. Es importante que no ejecute el programa combinando archivos guardados y nuevos.

Restablezca los archivos que ha guardado en el directorio **/etc/opt/ibm/sna**.

Además, si ha guardado los cambios en el archivo de arranque **/etc/rc.d/init.d/snastart**, realice los mismos cambios en la nueva copia del archivo, tal y como se describe en "Habilitación de Communications Server para Linux" en la página 74, para asegurarse de que Communications Server para Linux no se inicie de forma automática al arrancar el sistema.

Vuelva a iniciar el software de Communications Server para Linux con el siguiente mandato:

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

Instalación del programa bajo licencia Communications Server para Linux

Una vez que haya instalado el software que es requisito previo tal y como se describe en el apartado "Instalación de software como requisito previo" en la página 28, ya se puede instalar Communications Server para Linux. Utilice el procedimiento siguiente:

1. Inicie la sesión con privilegios de root.
2. Instale Communications Server para Linux tal y como se describe en "Instalación de Communications Server para Linux" en la página 33.
3. Si ha instalado el software GSKIT para utilizar el servidor TN o el redirector TN con la función SSL, debe configurar el software SSL después de haber instalado Communications Server para Linux. Consulte "Configuración de SSL para su uso con el servidor TN o el redirector TN" en la página 36 para obtener más información.
4. Personalice la información de configuración de Communications Server para Linux según sea necesario (consulte el Capítulo 8, "Configuración y utilización de Communications Server para Linux", en la página 71 o la publicación *IBM Communications Server para Linux, Guía de administración*).
5. Inicie Communications Server para Linux. Observe que después de la instalación el cliente se inicia automáticamente al reiniciar la máquina.

```
cd /
```

```
sna start
```

Instalación del programa bajo licencia Communications Server para Linux

Nota:

1. La instalación automática de Communications Server para Linux vuelve a configurar los controladores de dispositivo SNA en el nodo local. Si realiza la instalación en un sistema con memoria limitada, por ejemplo con 64 MB, es posible que deba arrancar de nuevo tras la instalación de Communications Server para Linux para poder iniciar el nodo SNA.
2. Puede instalar los adaptadores después de instalar Communications Server para Linux. No es necesario que vuelva a instalar Communications Server para Linux después de añadir un adaptador.

Instalación de Communications Server para Linux

1. Coloque el CD de instalación en la unidad adecuada de la estación de trabajo Linux.
2. Inicie la sesión con privilegios de root.
3. Ejecute el programa **installibmcs** desde el CD. Consulte el archivo **README** en el CD de imagen de Communications Server para Linux para ver los detalles sobre los mandatos necesarios para hacerlo.

Normalmente el programa le solicitará lo siguiente.

- Confirmación de que ha leído y aceptado los términos de la licencia de Communications Server para Linux.
- El nombre del servidor que será el servidor maestro en el dominio Communications Server para Linux. Si desea ejecutar Communications Server para Linux como un nodo autónomo, no especifique este parámetro; en este caso, el nodo no dará soporte a las funciones de cliente/servidor.

Puede alterar temporalmente estas solicitudes mediante la especificación de parámetros adicionales en el mandato **installibmcs**, tal como se describe más abajo.

4. Si desea instalar la documentación en PDF de Communications Server para Linux, ejecute el programa **installibmcsdocs** desde el CD.
5. Personalice la información de configuración de Communications Server para Linux (consulte el Capítulo 8, "Configuración y utilización de Communications Server para Linux", en la página 71 o la publicación *IBM Communications Server para Linux, Guía de administración*).

Si necesita efectuar una instalación desatendida, puede proporcionar parámetros adicionales en el mandato **installibmcs** para confirmar la aceptación de los términos de la licencia de Communications Server para Linux y especificar el nombre del servidor maestro. En este caso, el script de shell se ejecutará sin solicitar información adicional. Utilice el mandato siguiente:

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

nombre_maestro es el nombre del servidor maestro. Si desea ejecutar Communications Server para Linux como un nodo autónomo, no especifique este parámetro; en este caso, el nodo no dará soporte a las funciones de cliente/servidor.

Nota: La instalación automática de Communications Server para Linux vuelve a configurar los controladores de dispositivo SNA en el nodo local.

Documentación en línea de Communications Server para Linux

Siga los pasos del apartado “Instalación de Communications Server para Linux” en la página 33 para cargar el CD de instalación de Communications Server para Linux e inicie la sesión con privilegios de root y, a continuación, ejecute el script de shell `installibmcsdocs`:

```
./installibmcsdocs
```

Bibliotecas de clases de acceso a sistema principal (HACL)

Los ficheros HACL se instalan automáticamente al instalar Communications Server para Linux. El código de las bibliotecas se halla en el paquete `ibm-commserver-ecl` bajo `rpm`. Puede encontrar estos archivos, incluido el archivo README, en `/opt/ibm/sna/ecl` o emitiendo el mandato siguiente:

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

Configuración de WebSphere Application Server

Si va a ejecutar un sistema cliente/servidor en el que los clientes Remote API Client se conectan a servidores Communications Server para Linux utilizando HTTPS, necesitará un sistema donde se ejecute WebSphere Application Server para que estos clientes accedan a los servidores mediante HTTPS, tal y como se describe en “Requisitos de instalación” en la página 20.

Este apartado describe cómo configurar WebSphere para su utilización con Communications Server para Linux:

- Configuración de un certificado seguro en el servidor WebSphere que se mostrará a los clientes
- Configuración de WebSphere Application Server para trabajar con Communications Server para Linux
- Instalación del fichero de configuración en el servidor WebSphere

También necesitará configurar el certificado de seguridad del cliente y el archivo de datos de red del cliente en cada cliente Remote API Client para acceder a WebSphere Application Server. Para obtener más información, vea el capítulo sobre la instalación del tipo de cliente apropiado.

Configuración del certificado seguro de WebSphere Application Server

Consulte la documentación de WebSphere Application Server para obtener instrucciones sobre la configuración de un certificado seguro en el servidor. Este es el certificado del servidor que se mostrará al cliente Remote API Client durante el proceso de autenticación cuando el cliente intente conectarse utilizando HTTPS.

Es recomendable configurar WebSphere para que aplique la autenticación de servidor; consulte la documentación de WebSphere Application Server para obtener más información. De esta manera, WebSphere solicitará certificados de seguridad a los clientes Remote API Client durante el proceso de autenticación y aceptará una conexión entrante procedente de un proceso de un cliente Remote API Client sólo si puede verificar la autenticidad del certificado del cliente.

Configuración de WebSphere Application Server

Para configurar WebSphere Application Server para que trabaje con Communications Server para Linux, siga los siguientes pasos. Consulte la documentación de WebSphere Application Server para obtener más información.

1. Copie o transfiera mediante FTP los archivos **snahttpsrv.ear** y **snahttpsrv.cfg** del directorio **ibm-commserver-https** del CD de instalación del cliente Remote API Client a un directorio del sistema donde se ejecuta la consola de administración de WebSphere, o copie los archivos en un directorio de red al que se pueda acceder desde ese sistema.
Si la consola de administración se está ejecutando en Windows, no es necesario copiar los archivos, ya que puede acceder directamente a los archivos desde el CD. Solamente necesita insertar el CD de instalación del cliente Remote API Client en la unidad de CD del sistema Windows.
2. Inicie la consola de administración de WebSphere.
3. Utilice la documentación de WebSphere para crear un sistema principal virtual que sea accesible solamente mediante una conexión SSL protegida. El plug-in de Java encargado de gestionar las conexiones de HTTPS de SNA utilizará este sistema principal virtual
4. En la barra de menús, seleccione Aplicaciones, Instalar nueva aplicación.
5. Especifique la ubicación del archivo **snahttpsrv.ear**. Seleccione el botón Siguiente.
6. Cuando se le solicite especificar un nombre de sistema principal virtual en las dos primeras pantallas, escriba el nombre del sistema principal virtual que ha configurado para HTTPS. Puede aceptar las opciones por omisión para todos los demás parámetros a menos que necesite utilizar una configuración de WebSphere determinada; seleccione el botón Siguiente en los diálogos posteriores hasta que aparezca el botón Finalizar y selecciónelo. Normalmente la pantalla debe mostrar ahora que **La aplicación se ha instalado satisfactoriamente**.
7. Pulse en Guardar en configuración maestra y luego pulse el botón Guardar.
8. En la barra de menús, seleccione Aplicaciones, Aplicaciones empresariales.
9. Localice **SnaHttpTransport** en la lista de aplicaciones, pulse en la casilla situada junto a esa aplicación y luego pulse el botón Iniciar para iniciar la aplicación. (Una vez hecho esto, la aplicación se iniciará automáticamente cuando se inicie WebSphere Application Server).
10. En la barra de menús, seleccione Entorno, Actualizar plug-in de servidor Web y pulse el botón OK. Esto actualiza la configuración de WebSphere.

Instalación del archivo de configuración del servidor

Para poder trabajar con Communications Server para Linux, WebSphere Application Server requiere una lista de servidores Communications Server para Linux a la que puede accederse mediante HTTPS. Cree e instale esta lista utilizando los pasos siguientes.

1. En la barra de menús de la consola de administración, seleccione Entorno, Gestionar variables de WebSphere.
2. Busque la variable **USER_INSTALL_ROOT** en esta lista y anote su valor (el cual es la vía de acceso a un directorio situado en el servidor WebSphere). La lista de variables de entorno puede abarcar dos o más páginas, por lo que puede ser necesario pulsar el botón Siguiente para recorrer la lista.
3. Copie el archivo **snahttpsrv.cfg** desde la ubicación en la que lo haya guardado en el apartado "Configuración de WebSphere Application Server" (o desde el

Configuración de WebSphere Application Server

CD de instalación) en el directorio especificado por la variable `USER_INSTALL_ROOT` y luego edite este archivo mediante un editor de texto para incluir la lista de servidores Communications Server para Linux a los que pueden acceder los clientes Remote API Client utilizando HTTPS. Cada servidor se debe especificar en una línea separada del archivo, utilizando este formato:

```
server=nombre_servidor.nombre_dominio.com
```

Procedimientos posteriores a la instalación

Este apartado describe cómo realizar tareas de mantenimiento que pueden ser necesarias después de instalar Communications Server para Linux.

Trabajo en una configuración cliente/servidor

Después de la instalación, Communications Server para Linux trabaja inicialmente como servidor autónomo (con todos los componentes situados en un solo sistema Linux). Si desea ejecutarlo como servidor en un dominio cliente/servidor, consulte el capítulo sobre la gestión de sistemas cliente/servidor de Communications Server para Linux en la publicación *IBM Communications Server para Linux, Guía de administración* para obtener más información.

Visualización de manuales en PDF

Los manuales incluidos en el soporte de instalación de este producto están en PDF (Portable Document Format). El formato en copia software le permite realizar búsquedas, navegar o imprimir la información con facilidad y utiliza enlaces de hipertexto para ver la información relacionada. También facilita el compartimiento de la biblioteca de publicaciones en el sitio Web, pues existen visores PDF para muchas plataformas diferentes.

Si elige la instalación de los manuales PDF al instalar el producto, lo harán en el directorio `/opt/ibm/sna/docs`. Los manuales también se incluyen en el directorio `/DOCS` del soporte de instalación de Communications Server para Linux.

Puede leer los manuales en PDF utilizando cualquier visor PDF, como por ejemplo Adobe Acrobat en Windows o `xpdf` en Intel Linux.

Revisión de información de release actual

La última actualización del archivo **README** para el producto, ubicado en el directorio `/opt/ibm/sna`, contiene información acerca de los cambios realizados en el producto después de publicar la biblioteca de Communications Server para Linux. Este archivo está también incluido en el directorio raíz del soporte de instalación de Communications Server para Linux. Revise el archivo **README** siempre que reciba actualizaciones del producto.

Configuración de SSL para su uso con el servidor TN o el redirector TN

Si ha instalado el software GSKIT para utilizar el servidor TN o el redirector TN con la función SSL, debe configurar el software SSL después de haber instalado Communications Server para Linux.

El software SSL requiere dos componentes:

- Se requiere un par de claves para poder llevar a cabo el cifrado y el descifrado de datos.

- Se requiere un certificado para permitir la autenticación de servidor.

El certificado y el par de claves forman un solo registro de una base de datos de claves, que se almacena en el servidor Communications Server para Linux que ejecuta el servidor TN o el redirector TN. Communications Server para Linux utiliza la base de datos para implementar SSL.

Para gestionar la base de datos de claves, escriba el siguiente mandato en el indicador de mandatos de Linux:

snakeyman

El mandato **snakeyman** inicia un programa Java. Para obtener más indicaciones, consulte la ayuda proporcionada con este programa.

Cada registro de la base de datos se identifica mediante un nombre exclusivo conocido como etiqueta. Si tiene dos o más registros para utilizarlos en sesiones diferentes de servidor TN o de redirector TN, necesitará anotar las etiquetas que asigna al configurar la base de datos; estas etiquetas se utilizan para identificar el registro que debe utilizarse en cada sesión. También puede identificar uno de los registros como el registro por omisión, de modo que las sesiones utilicen ese registro a menos que especifique explícitamente la etiqueta de un registro diferente.

Después de utilizar **snakeyman** para actualizar los certificados de servidor, debe salir del programa **snakeyman** y, a continuación, detener y reiniciar el nodo Communications Server para Linux para utilizar los certificados actualizados. Utilice los mandatos siguientes para detener y reiniciar el nodo:

```
snaadmin term_node  
snaadmin init_node
```

Copia de seguridad de los archivos de configuración de Communications Server para Linux

Communications Server para Linux crea de forma automática una copia de seguridad de los archivos de configuración del nodo, dominio, datos del dispositivo TN3270 (**tn3270dev.dat**) y TP todas las veces que se hagan cambios que afecten a esos archivos (utilizando las herramientas de administración de Communications Server para Linux). Por ejemplo, cuando se efectúa un cambio que afecta al archivo de configuración del nodo (**sna_node.cfg**), Communications Server para Linux crea un archivo de copia de seguridad denominado **sna_node.bk n** , donde n es 1 ó 2:

- La primera vez que cambie el archivo, la configuración existente se guarda en **sna_node.bk1**.
- La segunda vez que cambie el archivo, la configuración existente se guarda en **sna_node.bk2**, sin cambiar **sna_node.bk1**.
- La tercera vez que cambie el archivo, y las veces posteriores, **sna_node.bk1** se elimina, **sna_node.bk2** pasa a llamarse **sna_node.bk1** y la configuración existente se guarda en **sna_node.bk2**.

Este proceso significa que en todo momento existe un máximo de dos archivos de copia de seguridad para el archivo de configuración del nodo. Se utiliza el mismo procedimiento para generar extensiones de nombre de archivo para otros archivos de copia de seguridad.

Procedimientos posteriores a la instalación

Además de copias de seguridad automáticas, debe efectuar copias de seguridad de archivos de configuración para prevenir la pérdida de datos en una de las condiciones siguientes:

- Antes de instalar un nuevo nivel del sistema operativo Linux
- Antes de instalar un nuevo release de Communications Server para Linux
- Después de crear una configuración nueva.

Para realizar copias de seguridad de los archivos de configuración, utilice estos mandatos:

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

Restauración de una copia de seguridad de los archivos de configuración de Communications Server para Linux

Para restaurar los archivos de configuración de Communications Server para Linux cuya copia de seguridad se ha realizado tal como se describe en el apartado “Copia de seguridad de los archivos de configuración de Communications Server para Linux” en la página 37, realice lo siguiente:

1. Asegúrese de que no está activo Communications Server para Linux. Para determinarlo, especifique el mandato siguiente:

```
snaadmin status_node
```

Si Communications Server para Linux está activo, el mandato muestra información acerca del estado del nodo local; si no, muestra un mensaje que indica que Communications Server para Linux está inactivo.

Si Communications Server para Linux está activo, escriba el mandato siguiente para desactivarlo:

```
sna stop
```

2. Entre los mandatos siguientes:

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

En este mandato, *nombreDispositivo* es la vía de acceso y el nombre de archivo del dispositivo que ha utilizado al hacer copia de seguridad de los archivos.

Este mandato sobregraba los archivos de configuración existentes con los mismos nombres en el directorio */etc/opt/ibm/sna*.

Reinicialización de los archivos de configuración

Si los archivos de configuración de Communications Server para Linux se modifican por error y no se puede utilizar la información que contienen, es posible que deba reinicializarlos para poder volver a configurar Communications Server para Linux como si acabara de instalarse. Realice esta operación sólo si está completamente seguro de que no puede recuperarse la información de configuración.

Nota: si dispone de copias de seguridad válidas de los archivos de configuración, puede copiar estos archivos en el directorio */etc/opt/ibm/sna* y utilizarlos para inicializar el nodo con el mandato **sna start**.

Puede reinicializar los archivos de configuración siguientes:

- Archivo de configuración de nodo **sna_node.cfg**
- Archivo de configuración de dominio **sna_domn.cfg**
- Archivo de configuración de TP **sna_tps**
- Archivo de base de datos de claves SSL y archivo de ocultación de contraseñas

Para reinicializar los archivos de configuración, siga estos pasos:

1. Salga del programa de administración si está activo e inhabilite Communications Server para Linux emitiendo el mandato siguiente:

```
sna stop
```

2. Realice una copia de seguridad de los archivos de configuración existentes; para ello, copie los archivos que vaya a reinicializar en otra ubicación.
3. Suprima los archivos que está reinicializando.
4. Si ha suprimido el archivo de configuración del dominio, emita el mandato siguiente para volver a crearlo (se copia el archivo de configuración de dominio vacío proporcionado con Communications Server para Linux):

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

Este mandato crea un nuevo archivo de configuración de dominio, que es necesario para iniciar Communications Server para Linux.

5. Si ha suprimido el archivo de base de datos de claves SSL, emita el siguiente mandato para volverlo a crear (copiándolo del archivo de ejemplo que se proporciona con Communications Server para Linux):

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

6. Emita el mandato siguiente para reiniciar Communications Server para Linux:

```
sna start
```

7. Inicie el programa de administración de Motif:

```
xsnaadmin &
```

Si no existe el archivo **sna_node.cfg**, el programa de administración le solicita que configure el nodo. A continuación configure el nodo y los demás recursos tal como se describe en Capítulo 8, "Configuración y utilización de Communications Server para Linux", en la página 71 o *IBM Communications Server para Linux, Guía de administración*.

Si el archivo **sna_node.cfg** es válido, el nuevo archivo de configuración se utiliza para inicializar el nodo.

Desinstalación de Communications Server para Linux

Puede desinstalar el producto Communications Server para Linux en cualquier momento. Utilice el procedimiento siguiente:

1. Inicie la sesión con privilegios de root.
2. Asegúrese de que no está activo Communications Server para Linux. Para determinarlo, especifique el mandato siguiente:

```
snaadmin status_node
```

Si Communications Server para Linux está activo, el mandato muestra información acerca del estado del nodo local; si no, muestra un mensaje que indica que Communications Server para Linux está inactivo.

Desinstalación de Communications Server para Linux

Si Communications Server para Linux está activo, escriba el mandato siguiente para desactivarlo:

```
sna stop
```

3. Elimine el paquete de Communications Server para Linux y los paquetes de software asociados utilizando las instrucciones siguientes:

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

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

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

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

Capítulo 4. Instalación de clientes IBM Remote API Client en Linux

Este capítulo describe cómo instalar el cliente IBM Remote API Client en Linux, lo que permite que una estación de trabajo Linux ejecute aplicaciones SNA sin tener una aplicación completa de SNA. Un cliente Remote API Client en Linux puede conectar a uno o más servidores Communications Server para Linux (o servidores CS/AIX, pero no ambos de forma simultánea) utilizando una red TCP/IP. (Los servidores CS Linux no pueden funcionar en el mismo dominio que los servidores CS/AIX).

Este capítulo es aplicable a los clientes IBM Remote API Client que se ejecutan en sistemas Intel de 32 bits (i686), AMD64/Intel EM64T de 64 bits (x86_64) y pSeries (ppc64). Si instala el cliente IBM Remote API Client en un sistema System z(s390 / s390x), consulte el Capítulo 5, “Instalación de clientes IBM Remote API en Linux para System z”, en la página 47.

El programa de instalación y los archivos asociados, incluido el archivo README de IBM Remote API Client, se encuentran en el CD de instalación, en el directorio correspondiente al tipo de cliente:

Tipo de cliente	Directorio del CD
Intel de 32 bits (i686)	<code>/ibm-commserver-clients/linux</code>
AMD64/Intel EM64T de 64 bits (x86_64)	<code>/ibm-commserver-clients/linux-x86_64</code>
pSeries (ppc64)	<code>/ibm-commserver-clients/linux—ppc64</code>

Es recomendable que lea el archivo README del cliente IBM Remote API Client antes de instalar el software.

Si está actualizando a partir de una versión anterior de Communications Server para Linux y los clientes Remote API Clients, es preferible actualizar todos los servidores antes de actualizar los clientes Remote API Client. Consulte “Migración desde niveles anteriores de Communications Server para Linux” en la página 29 para obtener más detalles.

Requisitos de hardware y software

Requisitos de hardware

El cliente IBM Remote API Client necesita un sistema soportado por alguna de las siguientes distribuciones de Linux.

Utilice el mandato `uname -m` para verificar la clase de CPU del sistema de destino. La tabla siguiente muestra el hardware adecuado para cada tipo de cliente y la respuesta de `uname -m` para este hardware.

Requisitos de hardware y software

Tipo de cliente	Hardware	Respuesta de uname
Intel de 32	Sistema Intel Pentium II o posterior de 32 bits o sistema basado en Opteron	i686
AMD64/Intel EM64T de 64 bits	Sistema x86_64 (AMD64 o Intel EM64T)	x86_64
pSeries	Sistema pSeries POWER5 u OpenPower	ppc64

Versión del sistema operativo Linux

La versión actual del cliente IBM Remote API Client se ha probado con las siguientes versiones del sistema operativo Linux. Puede que también se ejecute correctamente en otras distribuciones de Linux.

- RedHat Enterprise Linux 4 (RHEL4)
- RedHat Enterprise Linux 5 (RHEL5)
- SUSE Linux Enterprise Server 9 (SLES9)
- SUSE Linux Enterprise Server 10 (SLES10)
- SUSE Linux Enterprise Server 11 (SLES11)

Consulte el archivo **README** del CD de instalación para obtener detalles sobre qué paquetes opcionales pueden ser necesarios.

Java

Si utiliza la API de CPI-C para Java, es necesario el software de Java. Consulte el archivo **README** del CD de instalación para conocer detalles.

GSKIT

Si el cliente se conecta a servidores Communications Server para Linux utilizando HTTPS, necesitará el software de GSKIT para habilitar el acceso HTTPS a los servidores a través de un servidor WebSphere. El software de GSKIT se incluye en el CD de instalación, pero pueden ser necesarios algunos paquetes opcionales del sistema operativo Linux para poder instalarlo; consulte el archivo **README** del CD de instalación para obtener información sobre los paquetes opcionales que pueden ser necesarios.

Cuando el proceso de instalación del cliente, descrito más adelante en este capítulo, instala todos los paquetes necesarios, el software de GSKIT se instala automáticamente como parte de ese proceso de instalación. En otro caso, el usuario puede instalar más tarde el software de GSKIT.

Visualización de información detallada sobre la instalación del producto

Puede visualizar información acerca del cliente Remote API Client y los paquetes de software asociados que ya están instalados. Para ver todos los paquetes instalados, utilice el mandato siguiente:

```
rpm -q -a
```

Para ver más detalles de un paquete específico, utilice el mandato siguiente:

```
rpm -q -i nombrepaquete
```

nombrepaquete es el nombre base del paquete instalado, por ejemplo **ibm-commserver-client**.

Configuración de la variable de entorno de idioma

Utilice el mandato siguiente para cambiar la variable LANG e indicar el idioma que desee utilizar:

```
export LANG=idioma
```

Sustituya *idioma* por el identificador del idioma que desea utilizar, que puede ser uno de los siguientes:

Identificador	Idioma
en_US	Inglés (Estados Unidos)
ja_JP	Japonés (PC)
de_DE	Alemán
es_ES	Español
fr_FR	Francés
ko_KR	Coreano
pt_BR	Portugués
zh_CN	Chino (EUC simplificado)
zh_TW	Chino (tradicional)

Instalación del cliente Remote API Client de Linux

Después de haber instalado el software previo necesario, está preparado para instalar el cliente IBM Remote API Client.

Si ya tiene instalado un nivel anterior del cliente IBM Remote API Client, siga los pasos del apartado “Desinstalación del cliente Remote API Client de Linux” en la página 46 para eliminar la versión anterior antes de instalar la nueva. La información de configuración existente se conservará para su utilización por la nueva instalación.

1. Inicie la sesión con privilegios de root.
2. Monte el CD y haga que sea el directorio actual.

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

El nombre del directorio **/media/cdrom** puede ser diferente si tiene una unidad de DVD. Utilice el mandato **df** para ver en qué sitio ha montado Linux el CD.

3. Vaya al subdirectorio del CD apropiado y ejecute el script del shell para instalar el cliente. El ejemplo siguiente muestra el subdirectorio **/linux** para un cliente Intel de 32 bits (i686); sustitúyalo por **/linux-x86_64** o **/linux-ppc64** si es necesario.

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

El script de shell comprueba si se cumplen determinados requisitos y emite mensajes de aviso si no se satisfacen esos requisitos. Se le solicitará que lea y acepte el acuerdo de licencia; a continuación el script instalará los RPM. Si los productos necesarios apropiados ya están instalados, el script también instalará el software de GSKIT.

Instalación del cliente Remote API Client de Linux

4. Añada los directorios binarios del cliente IBM Remote API Client a la variable PATH. Puede cambiar el perfil para realizarlo automáticamente:

```
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
```

Para aplicaciones CPI-C de Java también debe establecer la variable de entorno siguiente:

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

Para algunas aplicaciones también deberá establecer la variable de entorno LD_PRELOAD, pero no debe hacerlo como un cambio global en el perfil:

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

5. Inicie el cliente IBM Remote API Client. Después de la instalación, el cliente se inicia automáticamente al reiniciar la máquina. Cuando reinicie la máquina, asegúrese de que no esté todavía en los directorios del CD:

```
cd /  
sna start
```

Nota: Para que el cliente IBM Remote API Client se pueda conectar a servidores utilizando HTTPS, debe utilizar el programa gestor de claves de GSKIT para crear la configuración de certificados de seguridad en el cliente. Consulte "Configuración de certificados de seguridad de HTTPS utilizando GSKIT" para más información.

También deberá actualizar el archivo de datos de red del cliente para especificar los servidores Communications Server para Linux a los que se puede conectar el cliente y el nombre del servidor WebSphere que permite que se pueda utilizar HTTPS. Consulte el apartado sobre la gestión de clientes Remote API Client en la publicación *IBM Communications Server para Linux, Guía de administración* para obtener más detalles.

Configuración de certificados de seguridad de HTTPS utilizando GSKIT

Si el cliente se conecta a servidores Communications Server para Linux utilizando HTTPS, debe tener instalado el software del gestor de claves de GSKIT. Normalmente el gestor de claves se instala como parte de la instalación del cliente, siempre que estén instalados los requisitos previos necesarios del sistema operativo Linux tal como se describe en el archivo **README** del CD de instalación. Si GSKIT no se ha instalado como parte de la instalación del cliente, pero tiene instalados los prerrequisitos, puede instalar el software de GSKIT siguiendo estos pasos:

1. Inicie la sesión con privilegios de root.
2. Monte el CD y haga que sea el directorio actual.

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

El nombre del directorio **/media/cdrom** puede ser diferente si tiene una unidad de DVD. Utilice el mandato **df** para ver en qué sitio ha montado Linux el CD.

Configuración de certificados de seguridad de HTTPS utilizando GSKIT

3. Vaya al subdirectorio del CD apropiado y ejecute el script del shell para instalar el software GSKIT. El ejemplo siguiente muestra el subdirectorio `/linux` para un cliente Intel de 32 bits (i686); sustitúyalo por `/linux-x86_64` o `/linux-ppc64` si es necesario.

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

Para que el cliente IBM Remote API Client se pueda conectar a servidores utilizando HTTPS, debe utilizar el programa gestor de claves de GSKIT para crear la configuración de certificados de seguridad en el cliente. Siga los pasos siguientes.

1. Ejecute el gestor de claves de GSKIT utilizando el mandato siguiente:

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

Desde la interfaz de usuario del gestor de claves, abra el archivo de base de datos de claves, `/etc/opt/ibm/sna/ibmcs.kdb`, el cual está en formato CMS.

2. La contraseña inicial de la base de datos de claves es `ibmcs`. Para configurar los certificados de seguridad, **debe** cambiar esta contraseña para mantener segura la configuración. En el diálogo para cambiar la contraseña, debe marcar la casilla 'Stash the password to a file?' para que se guarde la nueva contraseña y el cliente pueda abrir la base de datos de claves.
3. Obtenga un ejemplar del certificado emitido por la Autoridad certificadora que se utilizó para firmar el certificado de seguridad del servidor Web e instale el certificado en la base de datos de claves. Para ello, seleccione "Signer Certificates" en la interfaz de usuario del gestor de claves y pulse en "Add".
4. Si el servidor WebSphere está configurado para solicitar certificados de seguridad de cliente, el cliente debe tener un certificado emitido por una autoridad certificadora cuyo propio certificado esté contenido en la base de datos de certificados de seguridad del servidor Web. Para solicitar un nuevo certificado:
 - a. Seleccione "Create", "New Certificate Request" en la interfaz de usuario del gestor de claves y proporcione los datos solicitados.
 - b. Guarde el certificado, colóquelo en un archivo y envíelo a la autoridad certificadora.
 - c. Cuando se emita el certificado, guárdelo en la base de datos del servidor Web. Para ello, seleccione "Personal Certificates" en la interfaz de usuario del gestor de claves y pulse en "Receive".

Como medida temporal con fines de prueba interna, puede crear un certificado de cliente autofirmado en lugar de obtener un certificado a partir de la autoridad certificadora. Pero esto no proporciona el nivel necesario de seguridad y no se debe utilizar en un sistema real. Para crear un certificado autofirmado:

- a. Seleccione "Create", "New Self-Signed Certificate" en la interfaz de usuario del gestor de claves y proporcione los datos solicitados.
 - b. Guarde el certificado y colóquelo en un archivo.
 - c. Almacene el archivo de certificado en la base de datos del servidor Web. Para ello, seleccione "Personal Certificates" en la interfaz de usuario del gestor de claves y pulse en "Receive".
5. Salga del gestor de claves de GSKIT cuando termine de configurar certificados.

Desinstalación del cliente Remote API Client de Linux

Puede desinstalar el cliente Remote API Client de Linux utilizando los mandatos siguientes.

```
/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
```

No todos los paquetes listados en esos mandatos estarán instalados en cada sistema.

La desinstalación del cliente IBM Remote API Client en Linux no altera la información de configuración personalizada existente para su utilización en una instalación posterior.

Capítulo 5. Instalación de clientes IBM Remote API en Linux para System z

Este capítulo describe cómo instalar el cliente IBM Remote API Client en Linux, lo que permite que un sistema principal System z ejecute aplicaciones SNA sin tener una aplicación completa de SNA. Un cliente Remote API Client en Linux para System z puede conectar uno o más servidores Communications Server para Linux (o servidores CS/AIX) utilizando una red TCP/IP.

Es recomendable que lea el archivo README del cliente IBM Remote API Client antes de instalar el software. Este archivo está situado en el directorio `/ibm-commserver-clients/linux-systemz` del CD de instalación.

Si está actualizando a partir de una versión anterior de Communications Server para Linux y los clientes Remote API Clients, es preferible actualizar todos los servidores antes de actualizar los clientes Remote API Client. Consulte “Migración desde niveles anteriores de Communications Server para Linux” en la página 29 para obtener más detalles.

Requisitos de hardware y software

Requisitos de hardware

El cliente IBM Remote API Client necesita un sistema System z de 31 bits o 64 bits que sea compatible con una de las distribuciones de Linux que aparecen de la lista en “Versión del sistema operativo Linux”.

Utilice el mandato `uname -m` para verificar la clase de CPU. La información resultante del mandato debe ser `s390` para denotar un entorno de 31 bits, o `s390x` para denotar un entorno de 64 bits.

Versión del sistema operativo Linux

La versión actual del cliente IBM Remote API Client se ha probado con las siguientes versiones del sistema operativo Linux. Puede que también se ejecute correctamente en otras distribuciones de 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 el archivo **README** del CD de instalación para obtener detalles sobre qué paquetes opcionales pueden ser necesarios.

Java

Si utiliza la API de CPI-C para Java, es necesario el software de Java. Consulte el archivo **README** del CD de instalación para conocer detalles.

GSKIT

Si el cliente se conecta a servidores Communications Server para Linux utilizando HTTPS, necesitará el software de GSKIT para habilitar el acceso HTTPS a los servidores a través de un servidor WebSphere. El software de GSKIT se incluye en el CD de instalación, pero pueden ser necesarios algunos paquetes opcionales del sistema operativo Linux para instalar ese software; consulte el archivo **README** situado en el directorio **/ibm-commserver-clients/linux-systemz** del CD de instalación para conocer detalles sobre qué paquetes opcionales pueden ser necesarios.

Cuando el proceso de instalación del cliente, descrito más adelante en este capítulo, instala todos los paquetes necesarios, el software de GSKIT se instala automáticamente como parte de ese proceso de instalación. En otro caso, el usuario puede instalar más tarde el software de GSKIT.

Visualización de información detallada sobre la instalación del producto

Puede visualizar información acerca del cliente Remote API Client y los paquetes de software asociados que ya están instalados. Para ver todos los paquetes instalados, utilice el mandato siguiente:

```
rpm -q -a
```

Para ver más detalles de un paquete específico, utilice el mandato siguiente:

```
rpm -q -i nombrepaquete
```

nombrepaquete es el nombre base del paquete instalado, por ejemplo **ibm-commserver-client**.

Configuración de la variable de entorno de idioma

Utilice el mandato siguiente para cambiar la variable LANG e indicar el idioma que desee utilizar:

```
export LANG=idioma
```

Sustituya *idioma* por el identificador del idioma que desea utilizar, que puede ser uno de los siguientes:

Identificador	Idioma
en_US	Inglés (Estados Unidos)
ja_JP	Japonés (PC)
de_DE	Alemán
es_ES	Español
fr_FR	Francés
ko_KR	Coreano
pt_BR	Portugués
zh_CN	Chino (EUC simplificado)
zh_TW	Chino (tradicional)

Instalación del cliente Remote API Client de Linux para System z

Después de haber instalado el software previo necesario, está preparado para instalar el cliente IBM Remote API Client.

Si ya tiene instalado un nivel anterior del cliente IBM Remote API Client, siga los pasos del apartado “Desinstalación del cliente Remote API Client de Linux para System z” en la página 51 para eliminar la versión anterior antes de instalar la nueva. La información de configuración existente se conservará para su utilización por la nueva instalación.

1. Copie o transfiera mediante FTP el archivo **ibm-commserver-client-6.4.0.0-s390x.tgz** desde el directorio **/ibm-commserver-clients/linux-systemz** del CD-ROM al sistema System z de Linux. Asegúrese de que utiliza la modalidad binaria para copiar o transferir el archivo mediante FTP.
2. Inicie la sesión como usuario root en el sistema System z de Linux.
3. Descomprima y desempaque el archivo tar en un directorio temporal vacío:
mkdir /tmp/ibmcs
cd /tmp/ibmcs
tar -xzf ibm-commserver-client-6.4.0.0-s390x.tgz

4. Ejecute el script de shell **installibmcscli**:

```
./installibmcscli
```

Este script de shell comprueba si se cumplen determinados requisitos y emite mensajes de aviso si no se satisfacen. También le solicita que confirme que ha leído y aceptado los términos de la licencia de Communications Server para Linux. Puede alterar temporalmente esta solicitud mediante la especificación de parámetros adicionales en el mandato **installibmcscli**, tal como se describe más abajo. Cuando haya respondido a la solicitud, el script de shell instalará los paquetes **rpm**. Si los productos necesarios apropiados ya están instalados, el script también instalará el software de GSKIT.

5. Añada los directorios binarios del cliente IBM Remote API Client a la variable PATH. Puede cambiar el perfil para realizarlo automáticamente:

```
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
```

Si ejecutará aplicaciones de 64 bits, utilice lo siguiente:

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

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

Para aplicaciones CPI-C de Java también debe establecer la variable de entorno siguiente:

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

Para algunas aplicaciones también deberá establecer la variable de entorno **LD_PRELOAD**, pero no debe hacerlo como un cambio global en el perfil:

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

6. Inicie el cliente IBM Remote API Client. Después de la instalación, el cliente se inicia automáticamente al reiniciar la máquina. Cuando reinicie la máquina, asegúrese de que no esté todavía en los directorios del CD:

```
cd /  
sna start
```

Instalación del cliente Remote API Client de Linux para System z

7. Cuando haya finalizado la instalación, puede borrar el archivo **tgz** y el directorio temporal que se han creado durante el proceso de instalación.

Nota: Para que el cliente IBM Remote API Client se pueda conectar a servidores utilizando HTTPS, debe utilizar el programa gestor de claves de GSKIT para crear la configuración de certificados de seguridad en el cliente. Consulte “Configuración de certificados de seguridad de HTTPS utilizando GSKIT” para más información.

También deberá actualizar el archivo de datos de red del cliente para especificar los servidores Communications Server para Linux a los que se puede conectar el cliente y el nombre del servidor WebSphere que permite que se pueda utilizar HTTPS. Consulte el apartado sobre la gestión de clientes Remote API Client en la publicación *IBM Communications Server para Linux, Guía de administración* para obtener más detalles.

Configuración de certificados de seguridad de HTTPS utilizando GSKIT

Si el cliente se conecta a servidores Communications Server para Linux utilizando HTTPS, debe tener instalado el software del gestor de claves de GSKIT. Normalmente el gestor de claves se instala como parte de la instalación del cliente, siempre que estén instalados los requisitos previos necesarios del sistema operativo Linux tal como se describe en el archivo **README** del CD de instalación. Si GSKIT no se ha instalado como parte de la instalación del cliente, pero tiene instalados los prerrequisitos, puede instalar el software de GSKIT siguiendo estos pasos:

1. Copie o transfiera mediante FTP el archivo **ibm-commserver-client-6.4.0.0-s390x.tgz** desde el directorio **/ibm-commserver-clients/linux-systemz** del CD-ROM al sistema System z de Linux. Asegúrese de que utiliza la modalidad binaria para copiar o transferir el archivo mediante FTP.
2. Inicie la sesión como usuario root en el sistema System z de Linux.
3. Descomprima y desempaquete el archivo tar en un directorio temporal vacío:
mkdir /tmp/ibmcs
cd /tmp/ibmcs
tar -xzf ibm-commserver-client-6.4.0.0-s390x.tgz
4. Ejecute el script de shell **installgskit**:
./installgskit
5. Cuando haya finalizado la instalación, puede borrar el archivo **tgz** y el directorio temporal que se han creado durante el proceso de instalación.

Para que el cliente IBM Remote API Client se pueda conectar a servidores utilizando HTTPS, debe utilizar el programa gestor de claves de GSKIT para crear la configuración de certificados de seguridad en el cliente. Siga los pasos siguientes.

1. Ejecute el gestor de claves de GSKIT utilizando el mandato siguiente:

/opt/ibm/sna/bin/snakeyman

Desde la interfaz de usuario del gestor de claves, abra el archivo de base de datos de claves, **/etc/opt/ibm/sna/ibmcs.kdb**, el cual está en formato CMS.

2. La contraseña inicial de la base de datos de claves es **ibmcs**. Para configurar los certificados de seguridad, **debe** cambiar esta contraseña para mantener segura

Configuración de certificados de seguridad de HTTPS utilizando GSKIT

la configuración. En el diálogo para cambiar la contraseña, debe marcar la casilla 'Stash the password to a file?' para que se guarde la nueva contraseña y el cliente pueda abrir la base de datos de claves.

3. Obtenga un ejemplar del certificado emitido por la Autoridad certificadora que se utilizó para firmar el certificado de seguridad del servidor Web e instale el certificado en la base de datos de claves. Para ello, seleccione "Signer Certificates" en la interfaz de usuario del gestor de claves y pulse en "Add".
4. Si el servidor WebSphere está configurado para solicitar certificados de seguridad de cliente, el cliente debe tener un certificado emitido por una autoridad certificadora cuyo propio certificado esté contenido en la base de datos de certificados de seguridad del servidor Web. Para solicitar un nuevo certificado:
 - a. Seleccione "Create", "New Certificate Request" en la interfaz de usuario del gestor de claves y proporcione los datos solicitados.
 - b. Guarde el certificado, colóquelo en un archivo y envíelo a la autoridad certificadora.
 - c. Cuando se emita el certificado, guárdelo en la base de datos del servidor Web. Para ello, seleccione "Personal Certificates" en la interfaz de usuario del gestor de claves y pulse en "Receive".

Como medida temporal con fines de prueba interna, puede crear un certificado de cliente autofirmado en lugar de obtener un certificado a partir de la autoridad certificadora. Pero esto no proporciona el nivel necesario de seguridad y no se debe utilizar en un sistema real. Para crear un certificado autofirmado:

- a. Seleccione "Create", "New Self-Signed Certificate" en la interfaz de usuario del gestor de claves y proporcione los datos solicitados.
 - b. Guarde el certificado y colóquelo en un archivo.
 - c. Almacene el archivo de certificado en la base de datos del servidor Web. Para ello, seleccione "Personal Certificates" en la interfaz de usuario del gestor de claves y pulse en "Receive".
5. Salga del gestor de claves de GSKIT cuando termine de configurar certificados.

Desinstalación del cliente Remote API Client de Linux para System z

Puede desinstalar el cliente Remote API Client de Linux para System z utilizando los mandatos siguientes.

```
/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
```

No todos los paquetes listados en esos mandatos estarán instalados en cada sistema.

La desinstalación del cliente IBM Remote API Client en Linux para System z no altera la información de configuración personalizada existente para su utilización en una instalación posterior.

Capítulo 6. Instalación de clientes IBM Remote API Client en AIX

Este capítulo describe cómo instalar el cliente IBM Remote API Client en AIX, lo que permite que una estación de trabajo AIX ejecute aplicaciones SNA sin tener una aplicación completa de SNA. Un cliente Remote API Client en AIX puede conectar uno o más servidores Communications Server para Linux (o servidores CS/AIX) utilizando una red TCP/IP.

Es recomendable que lea el archivo README del cliente IBM Remote API Client antes de instalar el software. Este archivo está ubicado en el directorio `/ibm-commserver-clients/aix` del CD de instalación. Si está actualizando a partir de una versión anterior de Communications Server para Linux y los clientes Remote API Client, es preferible actualizar todos los servidores antes de actualizar los clientes Remote API Client. Consulte “Migración desde niveles anteriores de Communications Server para Linux” en la página 29 para obtener más detalles.

Requisitos de hardware y software

Requisitos de hardware

El cliente IBM Remote API Client necesita un sistema pSeries compatible con uno de los sistemas operativos AIX listados en “Versión del sistema operativo”.

Versión del sistema operativo

La versión actual del cliente IBM Remote API Client se ha probado con las versiones siguientes del sistema operativo.

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

El cliente puede ejecutarse en un entorno global o en un sistema o aplicación WPAR. Asegúrese de que los WPAR en los que se ejecute el cliente tengan un nombre de sistema principal exclusivo que DNS pueda resolver.

Java

Si utiliza la API de CPI-C para Java, es necesario el software de Java. El último SDK de Java disponible en <http://www.ibm.com/developerworks/java/jdk> cumple todos los requisitos.

Instale el paquete SDK de Java con el mandato **installp**.

GSKIT

Si el cliente se conecta a servidores Communications Server para Linux utilizando HTTPS, necesitará el software de GSKIT para habilitar el acceso HTTPS a los servidores a través de un servidor WebSphere. Consulte el archivo **README** situado en el directorio `/ibm-commserver-clients/aix` del CD de instalación para obtener detalles. El software de GSKIT se instala como parte del proceso de instalación principal del cliente, que se describe más adelante en este capítulo.

Cambio de la variable de entorno de idioma

Cuando utilice el cliente Remote API Client, asegúrese de que la variable LANG no tenga el valor C.

Siga el procedimiento siguiente para conocer el valor actual de la variable LANG o para cambiar el valor de LANG:

1. En el menú principal de SMIT, seleccione **Entornos del sistema**.
2. En el menú siguiente de SMIT, seleccione **Gestionar Entorno de Idioma**.
3. En el menú siguiente de SMIT, seleccione **Cambiar/Mostrar Entorno de Idioma Principal**.
4. En el menú siguiente de SMIT, seleccione **Cambiar/Mostrar Convenio Cultural, Idioma o Teclado**.
5. Seleccione el idioma que desee utilizar. Por ejemplo, si está utilizando mensajes escritos en inglés americano, seleccione en_US.

Instalación del cliente Remote API Client de AIX

Después de haber instalado el software previo necesario, está preparado para instalar el cliente IBM Remote API Client.

Si ya tiene instalado un nivel anterior del cliente IBM Remote API Client, siga los pasos del apartado “Desinstalación del cliente Remote API Client de AIX” en la página 56 para eliminar la versión anterior antes de instalar la nueva. La información de configuración existente se conservará para su utilización por la nueva instalación.

Instalación del cliente Remote API Client mediante la copia de archivos en la estación de trabajo AIX

Para instalar el cliente Remote API Client, siga los pasos siguientes.

1. Copie o transfiera mediante FTP el archivo **sna.client.6.4.0.0.I** desde el directorio **/ibm-commserver-clients/aix** del CD-ROM a la estación de trabajo AIX. Asegúrese de que utiliza la modalidad binaria para copiar o transferir el archivo mediante FTP.

Si el cliente se va a conectar a servidores Communications Server para Linux utilizando HTTPS, es necesario también que copie o transfiera mediante FTP los dos archivos **gskta.*.I** y **gksa.*.I** que se encuentran en el mismo directorio del CD. Estos archivos contienen el software de GSKIT necesario para el acceso mediante HTTPS desde el cliente.

2. Inicie la sesión como raíz en la estación de trabajo AIX.
3. Instale el cliente AIX utilizando **smit** o **installp**. Para obtener instrucciones sobre cómo hacerlo, consulte el archivo **README** situado en el directorio **/ibm-commserver-clients/aix** del CD de instalación.
4. Si el cliente se va a conectar a servidores Communications Server para Linux utilizando HTTPS, instale los archivos GSKIT siguiendo las instrucciones del archivo **README**.
5. Cuando finalice el proceso de instalación, puede suprimir el archivo **sna.client.6.4.0.0.I** y los archivos de GSKIT en el directorio de trabajo.
6. Inicie el cliente IBM Remote API Client. Después de la instalación, el cliente se inicia automáticamente al reiniciar la máquina.

```
cd /  
sna start
```

Nota: Para que el cliente IBM Remote API Client se pueda conectar a servidores utilizando HTTPS, debe utilizar el programa gestor de claves de GSKIT para crear la configuración de certificados de seguridad en el cliente. Consulte “Configuración de certificados de seguridad de HTTPS utilizando GSKIT” en la página 56 para más información.

También deberá actualizar el archivo de datos de red del cliente para especificar los servidores Communications Server para Linux a los que se puede conectar el cliente y el nombre del servidor WebSphere que permite que se pueda utilizar HTTPS. Consulte el apartado sobre la gestión de clientes Remote API Client en la publicación *IBM Communications Server para Linux, Guía de administración* para obtener más detalles.

Instalación del cliente Remote API Client desde el CD

Para instalar el cliente Remote API Client, siga los pasos siguientes.

1. Inicie la sesión como raíz en la estación de trabajo AIX.
2. Monte el CD en la estación de trabajo AIX utilizando el mandato siguiente.
mount -o ro /dev/cd0 /mnt
3. Instale el cliente AIX utilizando **smit** o **installp**. Para obtener instrucciones sobre cómo hacerlo, consulte el archivo **README** situado en el directorio **/ibm-commserver-clients/aix** del CD de instalación.
4. Si el cliente se va a conectar a servidores Communications Server para Linux utilizando HTTPS, instale los archivos GSKIT siguiendo las instrucciones del archivo **README**.
5. Cuando finalice el proceso de instalación, desmonte el CD utilizando el mandato siguiente.
unmount /mnt
6. Inicie el cliente IBM Remote API Client. Después de la instalación, el cliente se inicia automáticamente al reiniciar la máquina. Cuando reinicie la máquina, asegúrese de que no esté todavía en los directorios del CD:

```
cd /  
sna start
```

Nota: Para que el cliente IBM Remote API Client se pueda conectar a servidores utilizando HTTPS, debe utilizar el programa gestor de claves de GSKIT para crear la configuración de certificados de seguridad en el cliente. Consulte “Configuración de certificados de seguridad de HTTPS utilizando GSKIT” en la página 56 para más información.

También deberá actualizar el archivo de datos de red del cliente para especificar los servidores Communications Server para Linux a los que se puede conectar el cliente y el nombre del servidor WebSphere que permite que se pueda utilizar HTTPS. Consulte el apartado sobre la gestión de clientes Remote API Client en la publicación *IBM Communications Server para Linux, Guía de administración* para obtener más detalles.

Configuración de certificados de seguridad de HTTPS utilizando GSKIT

Para que el cliente IBM Remote API Client se pueda conectar a servidores utilizando HTTPS, debe utilizar el programa gestor de claves de GSKIT para crear la configuración de certificados de seguridad en el cliente. Siga los pasos siguientes.

1. Ejecute el gestor de claves de GSKIT utilizando el mandato siguiente:

/usr/bin/snakeyman

Desde la interfaz de usuario del gestor de claves, abra el archivo de base de datos de claves, */etc/sna/ibmcs.kdb*, el cual está en formato CMS.

2. La contraseña inicial de la base de datos de claves es *ibmcs*. Para configurar los certificados de seguridad, **debe** cambiar esta contraseña para mantener segura la configuración. En el diálogo para cambiar la contraseña, debe marcar la casilla 'Stash the password to a file?' para que se guarde la nueva contraseña y el cliente pueda abrir la base de datos de claves.
3. Obtenga un ejemplar del certificado emitido por la Autoridad certificadora que se utilizó para firmar el certificado de seguridad del servidor Web e instale el certificado en la base de datos de claves. Para ello, seleccione "Signer Certificates" en la interfaz de usuario del gestor de claves y pulse en "Add".
4. Si el servidor WebSphere está configurado para solicitar certificados de seguridad de cliente, el cliente debe tener un certificado emitido por una autoridad certificadora cuyo propio certificado esté contenido en la base de datos de certificados de seguridad del servidor Web. Para solicitar un nuevo certificado:
 - a. Seleccione "Create", "New Certificate Request" en la interfaz de usuario del gestor de claves y proporcione los datos solicitados.
 - b. Guarde el certificado, colóquelo en un archivo y envíelo a la autoridad certificadora.
 - c. Cuando se emita el certificado, guárdelo en la base de datos del servidor Web. Para ello, seleccione "Personal Certificates" en la interfaz de usuario del gestor de claves y pulse en "Receive".

Como medida temporal con fines de prueba interna, puede crear un certificado de cliente autofirmado en lugar de obtener un certificado a partir de la autoridad certificadora. Pero esto no proporciona el nivel necesario de seguridad y no se debe utilizar en un sistema real. Para crear un certificado autofirmado:

- a. Seleccione "Create", "New Self-Signed Certificate" en la interfaz de usuario del gestor de claves y proporcione los datos solicitados.
 - b. Guarde el certificado y colóquelo en un archivo.
 - c. Almacene el archivo de certificado en la base de datos del servidor Web. Para ello, seleccione "Personal Certificates" en la interfaz de usuario del gestor de claves y pulse en "Receive".
5. Salga del gestor de claves de GSKIT cuando termine de configurar certificados.

Desinstalación del cliente Remote API Client de AIX

Puede desinstalar el cliente Remote API Client utilizando los mandatos siguientes.

1. Detenga el software del cliente si está en ejecución, mediante el mandato siguiente.

sna stop

Desinstalación del cliente Remote API Client de AIX

2. Inicie la sesión con privilegios de root.
3. Desinstale el paquete del cliente Remote API Client y los paquetes de software asociados utilizando uno de los mandatos siguientes.

Para desinstalar el paquete utilizando **installp**:

installp -u sna.client

Para desinstalar el paquete utilizando **smit**:

smit remove

Desinstalación del cliente Remote API Client de AIX

Capítulo 7. Planificación e instalación del cliente Remote API Client de Windows

Este capítulo describe cómo instalar el cliente IBM Remote API Client en Windows, lo que permite que un PC ejecute aplicaciones SNA sin tener una instalación completa de SNA en el PC. Un cliente Remote API Client en Windows puede conectar uno o más servidores Communications Server para Linux (o servidores CS/AIX) utilizando una red TCP/IP.

Si está actualizando a partir de una versión anterior de Communications Server para Linux y los clientes Remote API Clients, es preferible actualizar todos los servidores antes de actualizar los clientes Remote API Client. Consulte “Migración desde niveles anteriores de Communications Server para Linux” en la página 29 para obtener más detalles.

Hay dos variantes del cliente IBM Remote API Client sobre Windows, en función del hardware y de la versión de Windows en concreto que se utilice. La información de este capítulo es aplicable a ambas variantes, a excepción de los lugares en los que se observan diferencias explícitamente.

- El cliente de 32 bits se ejecuta en un sistema basado en Intel de 32 bits que ejecuta Microsoft Windows 2000, Windows 2003, Windows XP, Windows Vista de 32 bits o Windows Server 2008 de 32 bits.
- El cliente x64 se ejecuta en un sistema AMD64 o Intel EM64T que ejecuta Microsoft Windows 2003 Server x64 Edition, Windows XP Professional x64 Edition, Windows Vista de 64 bits o Windows Server 2008 de 64 bits.

En términos generales, las interfaces proporcionadas por el cliente IBM Remote API Client en Windows son compatibles con las proporcionadas por IBM Communications Server para Windows y los productos Microsoft Host Integration Server.

El SDK (Software Development Kit) del cliente IBM Remote API Client en Windows es un paquete opcional que le permite utilizar el cliente Remote API Client para desarrollar programas de aplicación utilizando las API de APPC, CPI-C, LUA y CSV. Vea la guía de consulta de programación adecuada para obtener más información acerca de estas API. No es necesario que instale este paquete si el cliente Remote API Client sólo se utilizará para ejecutar aplicaciones existentes (no para desarrollar otras nuevas).

Requisitos de hardware y software

Para ejecutar el programa **Setup** y el cliente Remote API Client de Windows, el sistema debe cumplir los requisitos siguientes:

- Debe ejecutar uno de los sistemas operativos siguientes. Para obtener información actualizada acerca de los números de versión compatibles con cada versión del sistema operativo y cualquier otro requisito para versiones específicas, consulte la información del cliente Windows en el archivo **README** en el CD de instalación.

:

- Para el cliente Windows de 32 bits:
 - Windows 2000

Requisitos de hardware y software

- Windows XP
- Windows 2003
- Windows Vista de 32 bits
- Windows Server 2008 de 32 bits
- Para el cliente Windows x64:
 - Microsoft Windows XP Professional x64 Edition
 - Microsoft Windows 2003 Server x64 Edition
 - Windows Vista de 64 bits
 - Windows Server 2008 de 64 bits
- Debe tener acceso a uno o más servidores Communications Server para Linux utilizando uno de los mecanismos siguientes:
 - Acceso al servidor a través de una red TCP/IP
 - Acceso a un servidor de WebSphere que proporcione acceso HTTPS a Communications Server para servidores Linux.

Nota: En función de la versión de Windows que utilice o las funciones del cliente Remote API Client que desee utilizar, es posible que necesite realizar alguna otra configuración antes de poder instalar y utilizar el cliente Remote API Client en Windows. Consulte la información de cliente de Windows del archivo **README** en el CD de instalación para obtener más detalles.

Acceso al programa Setup

El cliente Remote API Client y el software de SDK, el software de GSKIT y el programa **Setup** se incluyen en el CD de instalación en formato de Windows, para que pueda instalarlos desde el CD en el sistema Windows. Debe instalar el software del cliente Remote API Client en cada PC de cliente de Windows; así también se instala el software GSKIT de forma automática. El SDK sólo es necesario si se utiliza el cliente para desarrollar nuevas aplicaciones utilizando las API remotas de Windows; no es necesario el SDK si solamente utiliza el cliente para ejecutar aplicaciones existentes.

La imagen de instalación del cliente Remote API Client de Windows es un archivo ejecutable ZIP, de descompresión automática que se proporciona en el CD de instalación.

- Para el cliente de 32 bits, se trata del archivo **i_w32cli.exe** del directorio **/ibm-commserver-clients/windows** del CD.
- Para los clientes x64, se trata del archivo **i_w64cli.exe** del directorio **/ibm-commserver-clients/win-x64** del CD.

Puede copiar este archivo en otros PC Windows de la red para poder instalarlos sin tener acceso directo al CD de distribución de Communications Server para Linux. Cuando ejecuta este ejecutable, descomprime la imagen de instalación y ejecuta automáticamente el programa **Setup**. Si simplemente desea descomprimir la imagen de instalación y colocarla en un directorio temporal, por ejemplo para ejecutar el programa **Setup** desde la línea de mandatos, puede hacerlo cargando el archivo ZIP ejecutable en el programa de descompresión.

La primera vez que ejecute el programa **Setup** en un sistema en particular, lo hará desde el origen seleccionado. El programa maneja todo el proceso de instalación, instala una configuración básica y también instala y crea su propio icono. Cuando

se complete la instalación, puede utilizar el programa **Setup** (seleccionándolo en el Administrador de archivos o seleccionando su icono) si debe volver a instalar el software.

Después de haber extraído la imagen de instalación del cliente Remote API Client para colocarla en un directorio temporal, puede instalar el software en una de dos maneras:

- Ejecute el programa **Setup** en Windows, tal como se explica en el apartado “Instalación del cliente Remote API Client para Windows utilizando el programa Setup”. Debe utilizar este método si desea instalar el SDK.
- Emita el mandato **setup** en la línea de mandatos, tal como se explica en el apartado “Instalación del software del cliente Remote API Client desde la línea de mandatos” en la página 65. Este método no permite instalar el SDK.

Nota: Antes de que el cliente IBM Remote API Client pueda conectarse a servidores mediante HTTPS, deberá actualizar el archivo de datos de red del cliente para especificar los servidores Communications Server para Linux a los que se puede conectar el cliente y el nombre del servidor WebSphere que permite que se pueda utilizar HTTPS. Consulte el apartado sobre la gestión de clientes Remote API Client en la publicación *IBM Communications Server para Linux, Guía de administración* para obtener más detalles.

Instalación del cliente Remote API Client para Windows utilizando el programa Setup

Ejecute el programa **setup**, ya sea automáticamente como parte de la ejecución del archivo ZIP ejecutable auto-extraíble **i_w32cli.exe** (cliente de 32 bits) o **i_w64cli.exe** (cliente x64) o manualmente desde la línea de mandatos. El programa primero muestra una pantalla de selección del idioma de instalación.

1. Seleccione el idioma que desea utilizar para instalar y configurar el cliente Remote API Client y seleccione **Aceptar**.

El programa visualiza una pantalla de bienvenida que le introduce en el programa **Setup**.

2. Seleccione **Siguiente** para continuar con la instalación.

El programa visualiza el Acuerdo de licencia de software, que debe leer y comprender.

3. Si desea aceptar los términos de la licencia, seleccione **Aceptar** para continuar.

El programa le solicita que especifique el directorio de destino en el que deben instalarse los archivos.

4. Escriba el directorio de destino.

El programa le pregunta que seleccione el tipo de instalación que desea:

Estándar

Seleccione esta opción si no necesita instalar el SDK. El SDK sólo es necesario si se utiliza el cliente para desarrollar nuevas aplicaciones utilizando las API remotas de Windows; no es necesario el SDK si solamente utiliza el cliente para ejecutar aplicaciones existentes.

Desarrollador

Seleccione esta opción si necesita instalar el SDK: es decir, si va a utilizar el cliente para desarrollar aplicaciones nuevas utilizando las API remotas de Windows.

Nota: Si desea instalar el SDK, debe seleccionar **Desarrollador**.

Instalación del cliente Remote API Client para Windows utilizando el programa Setup

5. Elija el tipo de instalación.
El programa le solicita entonces que escriba el nombre de la carpeta de programa en la que desea que aparezcan los iconos del cliente Remote API Client de Windows.
6. Escriba el nombre de la carpeta.
7. Si el directorio System ya contiene archivos **.DLL** cuyos nombres son iguales a los archivos utilizados por el programa **Setup**, pero que no son archivos del cliente Remote API Client (por ejemplo, archivos procedentes de otro software SNA), el programa le solicita que realice una de las acciones siguientes:
 - Copiar los archivos **.DLL** del cliente Remote API Client sobre los archivos **.DLL** existentes
 - Copiar los archivos **.DLL** existentes en un subdirectorío denominado **OTHERSNA** del directorío de instalación y luego instalar los archivos **.DLL** del cliente Remote API Client. Esta opción le permite restaurar la configuración original existente antes de instalar el cliente Remote API Client si desinstala los archivos más tarde (consulte el apartado “Desinstalación del software del cliente Remote API Client” en la página 69).
 - Cancelar la instalación del software del cliente.Si los archivos **.DLL** del cliente Remote API Client ya están presentes, el programa **Setup** muestra un mensaje para indicar ese hecho. Los nuevos archivos **.DLL** sobregrabarán los archivos **.DLL** existentes solamente si éstos tienen números de versión menores que los archivos **.DLL** del programa **Setup**.
8. En este punto, el programa **Setup** copiará los archivos de la fuente especificada y los instalará en los sitios adecuados. Durante este proceso, una barra de información visualiza la parte de la instalación que se ha completado. Los archivos **.DLL** se copian en el directorío Sistema o equivalente y los demás archivos se copian en el directorío de destino que ha especificado en el paso 2. Durante cada operación de transferencia de archivos, se graba un registro en el archivo **setup.log**, que se crea en el directorío que ha especificado. Si alguno de los archivos que se deben sobregrabar es de “sólo lectura” o no se puede copiar algún archivo por cualquier otra razón, los nuevos archivos se eliminarán y recibirá un mensaje indicándole que consulte el archivo **setup.log**.
9. Si la fuente desde la que ejecuta el programa **Setup** no contiene todos los archivos requeridos, el programa le solicitará un nombre de directorío. Escriba el nombre del directorío en el que están ubicados los archivos requeridos.
Si la información que ha especificado no es suficiente para localizar copias de los archivos del cliente Remote API Client, el programa vuelve a mostrar esta pantalla.
10. Cuando se han copiado los archivos necesarios, el programa **Setup** muestra la ventana de configuración.
Los valores de configuración por omisión se toman del archivo de configuración del dominio. Para obtener más información, consulte la publicación *IBM Communications Server para Linux, Guía de administración*. Si no desea utilizar los valores por omisión, puede configurarlos tal como se indica a continuación:
Dominio
Especifique el nombre de dominio de cliente/servidor de Communications Server para Linux.

Instalación del cliente Remote API Client para Windows utilizando el programa Setup

Si el cliente utiliza el direccionamiento IPv6, deberá configurar los valores siguientes. Son opcionales si el cliente utiliza el direccionamiento IPv4.

Nombre de servidor

La pantalla muestra una lista de nueve servidores como máximo a los que este cliente se puede conectar. El orden en el que los servidores aparecen en esta lista es el orden en el que el cliente selecciona estos servidores. Si el cliente no se puede conectar al primer servidor de la lista, intenta el siguiente servidor.

Si el cliente utiliza el direccionamiento IPv6, como mínimo deberá configurar un servidor. Si el cliente utiliza el direccionamiento IPv4, no será necesario que especifique ningún servidor si utiliza la opción *Difusiones UDP*; si especifica uno o varios servidores, el cliente intentará con éstos a su vez si no puede contactar un servidor utilizando difusiones UDP.

- Para añadir un nuevo servidor a la lista utilice el botón **Añadir**.
- Para eliminar un servidor de la lista, seleccione el servidor y utilice el botón **Suprimir**.
- Para subir o bajar un servidor en la lista, seleccione el servidor y utilice los botones de deslizamiento situados al lado de la lista.

Si el cliente está en la misma red privada que sus servidores y accede a ellos utilizando TCP/IP, cada servidor se identifica simplemente por el nombre de su servidor.

Si el cliente utiliza HTTPS para acceder a sus servidores, es necesario que identifique cada servidor especificando el nombre del servidor WebSphere que proporciona soporte a HTTPS y el nombre del servidor Communications Server para Linux, utilizando el formato siguiente:

nombreServidorWeb : nombreServidor1

En esa especificación se supone que WebSphere está configurado para utilizar el puerto por omisión 443 para las conexiones HTTPS. Si el administrador de la red ha configurado WebSphere para utilizar un número de puerto diferente, especifique el número de puerto utilizando el formato siguiente:

nombreServidorWeb : númeroPuerto : nombreServidor1

Para obtener más información sobre la configuración de WebSphere para poder utilizar conexiones HTTPS, consulte “Configuración de WebSphere Application Server” en la página 34.

Difusiones UDP

Especifique si este cliente utilizará difusiones UDP para conectarse a un servidor. Cuando esta opción está seleccionada, el cliente envía difusiones UDP por la red para localizar una conexión de servidor en lugar de intentar conectarse directamente a un servidor específico.

El valor por omisión es utilizar difusiones UDP. Para cambiar este valor, pulse en el recuadro.

Si el cliente utiliza el direccionamiento IPv6, las difusiones UDP no se soportan. Desactive esta opción para utilizar difusiones UDP y especifique un *Nombre de servidor* como mínimo.

Instalación del cliente Remote API Client para Windows utilizando el programa Setup

Los valores siguientes son opcionales:

Avanzado

Para suministrar valores adicionales en lugar de los valores por omisión suministrados por el programa **Setup**, pulse en el botón **Avanzado** en la parte inferior de la ventana. El programa **Setup** visualiza la ventana Opciones avanzadas, que contiene valores avanzados para la configuración del cliente Windows. La mayoría de usuarios pueden utilizar los valores por omisión para estos parámetros, por lo que probablemente no deba alterar los valores de este diálogo.

Para obtener más información acerca de estos parámetros consulte el apartado "Opciones avanzadas para la configuración del cliente Remote API Client".

Para obtener más información acerca de los parámetros de configuración o de los valores, pulse en **Ayuda**.

11. Cuando haya completado la ventana Configuración, pulse en **Aceptar**. El programa **Setup** muestra un mensaje si no ha completado correctamente esta pantalla.
12. Cuando la instalación se ha completado satisfactoriamente, se visualiza la ventana Finalizar. Puede seleccionar una o las dos acciones siguientes para que se lleven a cabo después de salir del programa de instalación:

Ver el archivo README

Visualiza el archivo **README**.

Iniciar el cliente

Empiece la ejecución del cliente de Communications Server para Linux.

Seleccione **Finalizar** para salir del programa de instalación.

Opciones avanzadas para la configuración del cliente Remote API Client

La ventana Opciones avanzadas le permite configurar algunos parámetros avanzados para el cliente Remote API Client. La mayoría de usuarios no necesitan modificar estos parámetros, pero se pueden ajustar los valores por omisión si es necesario.

Tiempo de espera de acceso a LAN

Especifique el tiempo, en segundos, que la conexión del cliente con un servidor puede permanecer desocupada antes de que se cierre. Cuando este recuadro de selección está vacío, significa que no se ha especificado ningún tiempo de espera de acceso a LAN (y por lo tanto se utilizará un tiempo de espera excedido infinito). Si selecciona este recuadro, puede entrar un valor de tiempo de espera, en segundos, en el campo adyacente. El valor mínimo es 60 (60 segundos); si deja la casilla en blanco o especifica un valor menor que 60, el cliente Remote API Client utiliza el valor mínimo 60.

Intentos de difusión máx.

Especifique el número máximo de veces que el cliente puede intentar conectarse a un servidor mediante difusión. Cuando se abre la ventana Opciones avanzadas, se visualiza el valor por omisión 5. El valor de este recuadro sólo se utiliza si se ha marcado el recuadro de selección Difusiones UDP en la ventana principal Configuración.

Opciones avanzadas para la configuración del cliente Remote API Client

Tiempo de espera de reconexión

Especifique el tiempo en segundos que el cliente debe esperar para poder intentar la reconexión con un servidor después de que el servidor se haya desactivado. Cuando se abre la ventana Opciones avanzadas, aparece el valor por omisión 200.

Para obtener más información acerca de estos parámetros, pulse en **Ayuda**.

Cuando haya completado la ventana Opciones avanzadas, pulse en **OK**. Si ha completado la pantalla correctamente, el programa **Setup** volverá a la ventana Configuración. Si está instalando un nuevo cliente Remote API Client, vuelva al paso 11 en la página 64. De lo contrario, pulse en el botón **OK** del diálogo Configuración para completar la configuración.

Instalación del software del cliente Remote API Client desde la línea de mandatos

Nota: si desea instalar el SDK, debe utilizar el programa **Setup**, tal como se describe en “Instalación del cliente Remote API Client para Windows utilizando el programa Setup” en la página 61. No puede instalar el SDK desde la línea de mandatos.

Después de extraer la imagen de instalación del cliente Remote API Client y colocarla en un directorio temporal, puede instalar el software del cliente Remote API Client desde la línea de mandatos en lugar de utilizar el programa **Setup** en Windows. En la línea de mandatos, escriba el mandato **setup** con una o varias opciones. Puede escribir estas opciones en mayúsculas o minúsculas y puede anteponerles / (barra inclinada) o - (guión). Si un parámetro como, por ejemplo *carpeta*, es una serie que contiene un espacio, debe encerrar la serie entre comillas dobles.

Después de escribir el mandato **setup**, el programa **Setup** le solicitará la información que no haya incluido en la línea de mandatos y visualizará mensajes de confirmación en varias fases de la instalación. Si desea que el programa **Setup** no le solicite información, utilice la opción **-accept -s** para ejecutar el programa en modalidad desatendida, que acepta los términos del Acuerdo de licencia de software.

Estas son las opciones del mandato **setup**:

-? Visualiza una lista de las opciones de la línea de mandatos. Es igual que la opción **-h**.

-h Visualiza una lista de las opciones de la línea de mandatos. Es igual que la opción **-?** .

-accept -s

Ejecuta la instalación en modalidad silenciosa y acepta los términos del contrato de licencia de software. Este acuerdo se encuentra en el subdirectorio **license** de la imagen de instalación de Windows.

La opción **-s** debe ser la última de la línea de mandatos y debe estar seguro de que ha especificado el nombre del dominio (utilizando la opción **-i**) y cualquier otros parámetros que desee especificar. Cuando la instalación se ejecuta en modalidad silenciosa, no solicita ningún parámetro ni visualiza mensajes de confirmación. Cualquier argumento de la línea de mandatos posterior a **-s** se pasa por alto.

Instalación del software del cliente Remote API Client desde la línea de mandatos

- f2 Especifica el nombre de vía de acceso completo del archivo de registro de la instalación durante la instalación en modalidad silenciosa (utilizando la opción -s).

Si no especifica esta opción, el archivo se crea como **setup.log** en el directorio desde el que se ejecuta el programa de instalación. Si realiza la instalación en modalidad silenciosa desde la unidad de CD, debe especificar esta opción para asegurarse de que el archivo se crea en el sistema (porque no puede crearse en la unidad de CD).
- k*carpeta*
 Especifique la carpeta del programa.
- p*directorio*
 Especifique el directorio de instalación.
- i*dominio*
 Especifique un nombre de dominio para este cliente. Este parámetro es necesario; no hay valor por omisión.
- w*directorio*
 Especifique el directorio fuente que contiene los archivos de software del cliente Communications Server para Linux si la fuente está ubicada en un disco o CD. De lo contrario, utilice al opción -v.
- v*servidor*
 Especifique el servidor del que se deben descargar los archivos de software de cliente. Puede especificar el nombre del servidor o la dirección TCP/IP. Si copia los archivos fuente desde un disco o CD, utilice la opción -w en lugar de la opción -v.
- l*servidor*
 Especifique el servidor que se debe incluir en la lista de servidores a los que este cliente puede acceder.

Si el cliente está en la misma red privada que sus servidores y accede a ellos utilizando TCP/IP, cada servidor se identifica simplemente por el nombre de su servidor.

Si el cliente utiliza HTTPS para acceder a sus servidores, es necesario que identifique cada servidor especificando el nombre del servidor WebSphere que proporciona soporte a HTTPS y el nombre del servidor Communications Server para Linux, utilizando el formato siguiente:

nombreServidorWeb : nombreServidor1

En esa especificación se supone que WebSphere está configurado para utilizar el puerto por omisión 443 para las conexiones HTTPS. Si el administrador de la red ha configurado WebSphere para utilizar un número de puerto diferente, especifique el número de puerto utilizando el formato siguiente:

nombreServidorWeb : númeroPuerto : nombreServidor1

Para obtener más información sobre la configuración de WebSphere para poder utilizar conexiones HTTPS, consulte "Configuración de WebSphere Application Server" en la página 34.
- o Sobregrafa los archivos **.DLL** existentes. Si los archivos **.DLL** del cliente Remote API Client ya están presentes, el programa **Setup** sobregrafa estos archivos aunque su número de versión sea mayor que el de los archivos **.DLL** del programa **Setup**.

Instalación del software del cliente Remote API Client desde la línea de mandatos

- y Guarda los archivos **.DLL** existentes. Si los archivos **.DLL** del cliente Remote API Client ya existen en los directorios necesarios, el programa **Setup** copia los archivos **.DLL** en un subdirectorio del directorio de instalación y luego instala los archivos **.DLL** del cliente Remote API Client. Las copias existentes en el subdirectorio garantizan que si el usuario desinstala el software del cliente Remote API Client, el proceso de desinstalación se completará.
- n Cancela la instalación si se encuentran archivos **.DLL** del cliente Remote API Client.
- atiempo de espera*
Especifique el tiempo de espera de acceso a la LAN. Esto es el período de tiempo que la conexión de un cliente con un servidor puede permanecer desocupada antes de que se cierre. El valor 0 indica que no hay tiempo de espera.
- bnúmero máximo de difusiones*
Especifique el número máximo de intentos de difusión UDP. Una difusión UDP es el intento que un cliente realiza de conectarse a cualquier servidor del dominio en lugar de intentar conectarse a un servidor específico. El valor 0 indica que no se realiza ningún intento de difusión.
- jtiempo de espera de reconexión*
Especifique el tiempo en segundos que el cliente debe esperar para poder intentar la reconexión con un servidor después de que el servidor se haya desactivado.

A continuación encontrará una línea de mandatos de ejemplo para instalar el cliente Remote API Client:

```
setup -imy_domain -lserver1.company.com -lserver2.company.com -b0 -j30 -accept  
-s -f2C:\instrapi.log -y
```

En este ejemplo:

- El cliente se instala en el dominio **my_domain**.
- El cliente tiene acceso a dos servidores en la misma red privada como cliente y no utiliza difusiones UDP para contactar con cualquier otro servidor. Espera 30 segundos antes de volver a contactar si pierde la conexión con un servidor.
- La instalación se realiza en modalidad silenciosa y escribe la información de registro de instalación en el archivo **C:\instrapi.log** del cliente.
- Se guardan las copias existentes de los archivos **.DLL** del cliente Remote API Client en el subdirectorio antes de que se instalen los nuevos archivos.

Configuración de certificados de seguridad de HTTPS utilizando GSKIT

Para que el cliente IBM Remote API Client se pueda conectar a servidores utilizando HTTPS, debe utilizar el programa gestor de claves de GSKIT para crear la configuración de certificados de seguridad en el cliente. Siga los pasos siguientes.

1. Ejecute el programa gestor de claves de GSKIT, *installdir\snakeyman.exe*. *installdir* representa el directorio en el que ha instalado el software de cliente, que es **C:\IBMCS\w32cli** (cliente de 32 bits) o **C:\IBMCS\w64cli** (cliente de 64 bits) si no ha especificado una ubicación distinta durante la instalación del cliente.

Configuración de certificados de seguridad de HTTPS utilizando GSKIT

Desde la interfaz de usuario del gestor de claves, abra el archivo de base de datos de claves, *dirinstal\ibmcs.kdb*, el cual está en formato CMS.

2. La contraseña inicial de la base de datos de claves es *ibmcs*. Para configurar los certificados de seguridad, **debe** cambiar esta contraseña para mantener segura la configuración. En el diálogo para cambiar la contraseña, debe marcar la casilla 'Stash the password to a file?' para que se guarde la nueva contraseña y el cliente pueda abrir la base de datos de claves.
3. Obtenga un ejemplar del certificado emitido por la Autoridad certificadora que se utilizó para firmar el certificado de seguridad del servidor Web e instale el certificado en la base de datos de claves. Para ello, seleccione "Signer Certificates" en la interfaz de usuario del gestor de claves y pulse en "Add".
4. Si el servidor WebSphere está configurado para solicitar certificados de seguridad de cliente, el cliente debe tener un certificado emitido por una autoridad certificadora cuyo propio certificado esté contenido en la base de datos de certificados de seguridad del servidor Web. Para solicitar un nuevo certificado:
 - a. Seleccione "Create", "New Certificate Request" en la interfaz de usuario del gestor de claves y proporcione los datos solicitados.
 - b. Guarde el certificado, colóquelo en un archivo y envíelo a la autoridad certificadora.
 - c. Cuando se emita el certificado, guárdelo en la base de datos del servidor Web. Para ello, seleccione "Personal Certificates" en la interfaz de usuario del gestor de claves y pulse en "Receive".

Como medida temporal con fines de prueba interna, puede crear un certificado de cliente autofirmado en lugar de obtener un certificado a partir de la autoridad certificadora. Pero esto no proporciona el nivel necesario de seguridad y no se debe utilizar en un sistema real. Para crear un certificado autofirmado:

- a. Seleccione "Create", "New Self-Signed Certificate" en la interfaz de usuario del gestor de claves y proporcione los datos solicitados.
 - b. Guarde el certificado y colóquelo en un archivo.
 - c. Almacene el archivo de certificado en la base de datos del servidor Web. Para ello, seleccione "Personal Certificates" en la interfaz de usuario del gestor de claves y pulse en "Receive".
5. Salga del gestor de claves de GSKIT cuando termine de configurar certificados.

Personalización del software del cliente Remote API Client después de la instalación

Puede cambiar cualquiera de los valores personalizados en cualquier momento después de la instalación inicial mediante la ejecución del **Programa de utilidad de configuración** que se encuentra en el grupo de programas de Communications Server para Linux. El programa visualiza la misma ventana Configuración que se ha visualizado en el proceso de instalación inicial. Puede cambiar la información de cualquier campo siguiendo el procedimiento del apartado "Instalación del cliente Remote API Client para Windows utilizando el programa Setup" en la página 61.

Si no instaló los archivos del SDK durante la instalación inicial y ahora desea añadirlos, puede hacerlo ejecutando el programa Setup de nuevo y seleccionando **Desarrollador** para el tipo de instalación.

Reinstalación del software del cliente Remote API Client

Puede reinstalar el software del cliente Remote API Client en cualquier momento, por ejemplo, cuando desee actualizar el software.

Para ello, ejecute el programa Setup como antes, utilizando las instrucciones de los apartados “Instalación del cliente Remote API Client para Windows utilizando el programa Setup” en la página 61 o “Instalación del software del cliente Remote API Client desde la línea de mandatos” en la página 65. El programa **Setup** visualiza la ubicación desde la que se han copiado los archivos de software de cliente durante la instalación inicial. Pulse en **OK** para obtener nuevas copias de los archivos en esta misma ubicación. Cuando pulse en **OK**, el programa **Setup** copiará los archivos y volverá a la pantalla Opciones.

Nota: si vuelve a instalar el software del cliente Remote API Client en la modalidad desatendida (tal como se describe en “Instalación del software del cliente Remote API Client desde la línea de mandatos” en la página 65), puede ser necesario reiniciar el sistema para completar la instalación. Esto es debido a que algunos archivos del programa pueden estar en uso durante el proceso de instalación (por ejemplo, si se está ejecutando el cliente Remote API Client) y, por tanto, no se pueden sustituir por archivos nuevos. En este caso, los nuevos archivos se copian en un directorio temporal y se colocarán en su lugar automáticamente la próxima vez que se reinicie el sistema.

Para comprobar si necesita reiniciar el sistema, utilice un editor de texto como por ejemplo, **Bloc de notas** para ver el contenido del archivo de registro de instalación después de que se haya completado el proceso de instalación. El archivo de registro de instalación se denomina **setup.log** y se crea en el directorio desde el que se ejecuta el programa Setup, a menos que utilice la opción de línea de mandatos **-f2** para especificar una vía de acceso y un nombre de archivo diferente.

Al final del archivo, bajo la cabecera **Response Result**, el texto **Result code** debe ir seguido de uno de los dos valores 0 (cero) o -12. Si el valor es 0, no hay necesidad de reiniciar el sistema; si el valor es -12, reinicie el sistema antes de intentar utilizar el cliente Windows.

Desinstalación del software del cliente Remote API Client

Puede desinstalar el software del cliente Remote API Client en cualquier momento utilizando la opción **Agregar o quitar programas** del Panel de control de Windows. Una vez confirmado el proceso de desinstalación, Windows hace lo siguiente:

- Suprime todos los archivos instalados.
- Si se han guardado archivos **.DLL** en un subdirectorio durante la instalación inicial, restaura los archivos a su ubicación original.
- Suprime el subdirectorio en el que se han almacenado los archivos **.DLL** guardados, siempre que el subdirectorio esté vacío.
- Elimina la carpeta del programa y el directorio creado si están vacíos.
- Si la desinstalación no es satisfactoria, suprime el archivo **setup.log**, que contiene todas las transferencias y supresiones de archivos.
- Visualiza un mensaje que indica que la desinstalación ha sido satisfactoria o que el usuario debe comprobar el archivo **setup.log** porque parte de la instalación ha fallado.

Desinstalación del software del cliente Remote API Client desde la línea de mandatos

El botón **Salir** le devuelve a Windows.

Desinstalación del software del cliente Remote API Client desde la línea de mandatos

Puede desinstalar el software del cliente Remote API Client desde la línea de mandatos, en vez de utilizar la opción **Agregar o quitar programas** del panel de control de Windows. Utilice el mandato siguiente:

installdir\sxcluninst -y

- *installdir* representa el directorio en el que ha instalado el software de cliente, que es **C:\IBMCS\w32cli** (cliente de 32 bits) o **C:\IBMCS\w64cli** (cliente de 64 bits) a menos que haya especificado una ubicación distinta durante la instalación del cliente.
- La opción **-y** se utiliza como confirmación, para prevenir un uso accidental de este mandato.

El programa de desinstalación se completa sin ningún aviso y no necesita ninguna otra entrada.

Ayuda

Para obtener Ayuda en cualquier momento, pulse la tecla **F1**. Las ventanas Configuración y Opciones avanzadas también disponen de botones **Ayuda**.

Capítulo 8. Configuración y utilización de Communications Server para Linux

La forma más sencilla de definir y modificar la configuración de Communications Server para Linux es utilizar el programa de administración de Motif (**xsnaadmin**). Este programa proporciona una interfaz gráfica de usuario desde la que puede ver y gestionar los recursos SNA del nodo local. También puede utilizar otras herramientas de administración como la administración desde la línea de mandatos, pero se recomienda utilizar el programa Motif.

El programa de administración de Motif incluye pantallas de ayuda que ofrecen información general sobre SNA y Communications Server para Linux, información de referencia para los diálogos de Communications Server para Linux y orientaciones para realizar tareas específicas. Para cada tarea (tal como configurar el nodo) o para cada tipo de comunicaciones (tal como TN3270 o APPC), el programa le indica cómo configurar los recursos necesarios.

El programa de administración de Motif permite configurar todos los parámetros necesarios para las configuraciones estándar de Communications Server para Linux. El programa de administración de Motif proporciona valores por omisión para los parámetros avanzados. El administrador sólo debe suministrar la información esencial de la configuración, lo que le permite configurar las comunicaciones SNA de forma rápida y sencilla.

También puede utilizar el programa de administración de Motif para gestionar el sistema Communications Server para Linux que se ejecuta. El programa de administración le permite realizar cambios y aplicarlos a la configuración mientras Communications Server para Linux está activo y ofrece un acceso fácil a la información de estado para los recursos de nodo.

El programa de administración de Motif visualiza automáticamente la información de estado de los recursos de Communications Server para Linux. La mayor parte de esta información se muestra en la ventana Nodo (consulte "Gestión de Communications Server para Linux con el programa de administración de Motif" en la página 74). Además, puede controlar determinados recursos (por ejemplo, nodos y estaciones de enlace) mediante los botones **Iniciar** y **Detener** de la ventana Nodo. Hay recursos que se inician y detienen automáticamente, de modo que no es necesario controlarlos manualmente.

Nota:

1. Debe ser miembro del grupo de inicio de sesión `sna` para definir o modificar recursos de Communications Server para Linux.
2. Para utilizar el programa de administración de Motif, debe disponer de un terminal X.
3. Para obtener más información sobre la interfaz de usuario del programa de administración de Motif, incluidos los botones e iconos que aparecen en la ventanas, consulte las pantallas de ayuda del programa o la publicación *IBM Communications Server para Linux, Guía de administración*.

Configuración y utilización de Communications Server para Linux

4. Es posible que las ventanas y los diálogos del programa de administración de Motif sean distintos de los que se muestran en esta publicación, según las opciones que seleccione en un diálogo determinado.

Para obtener más información sobre otras herramientas de Communications Server para Linux, incluidos los programas de aplicación NOF y de administración de línea de mandatos, consulte las publicaciones *IBM Communications Server para Linux, Guía de administración*, *IBM Communications Server for Linux Administration Command Reference*, o *IBM Communications Server for Linux NOF Programmer's Guide*.

Planificación de la configuración de Communications Server para Linux

Antes de realizar un cambio de configuración, es muy importante que lo planifique de forma exhaustiva. Los cambios que realice pueden perjudicar no solamente a los usuarios del nodo local, sino también a posibles usuarios que estén trabajando en la red.

Es recomendable diseñar un diagrama de los cambios que se desean realizar en la topología de la red. Si añade o elimina conexiones con otros nodos, diseñe un gráfico que muestre su nodo y los demás nodos. Puede utilizar el programa de administración de Motif para recopilar información sobre la configuración de todas las conexiones existentes y añadir dicha información al diagrama.

Cuando añada recursos al diagrama, le resultará fácil ver si son recursos duplicados o si existen nombres que entran en conflicto. Asimismo, el diagrama puede ayudarle a decidir qué recursos debe eliminar, a fin de evitar la supresión de recursos esenciales.

Si está configurando un sistema de cliente/servidor de Communications Server para Linux con más de un nodo, asegúrese de que incluya todos los nodos de Communications Server para Linux y sus recursos de conectividad en el diagrama. A continuación puede configurar cada nodo tal como se describe en este capítulo, de la misma manera configuraría un nodo autónomo.

Una vez que haya determinado los cambios que debe realizar, recopile la información de configuración necesaria. Para guiarle en la recopilación de información de configuración para las funciones específicas de Communications Server para Linux, puede utilizar las hojas de tareas que encontrará en la ayuda en línea del programa de administración de Motif, o las hojas de trabajo de planificación que encontrará en la publicación *IBM Communications Server para Linux, Guía de administración*.

Este capítulo ofrece instrucciones para configurar las funciones utilizadas con más frecuencia disponibles en Communications Server para Linux. Esta guía también le indica la información que debe recopilar antes de configurar el recurso para cada tarea de configuración.

Nota: Esta guía no ofrece descripciones detalladas de la información de configuración que debe entrar en los diálogos de Communications Server para Linux. Para obtener más información acerca de los campos de un diálogo en particular, consulte la ayuda en línea para ese diálogo en el programa de administración de Motif.

Hojas de trabajo de planificación

Antes de empezar a configurar los recursos de Communications Server para Linux, recopile todos los datos de configuración de los recursos nuevos. Para registrar toda la información de una aplicación o función determinada a la que necesite proporcionar soporte, utilice las hojas de trabajo de planificación *IBM Communications Server para Linux, Guía de administración*.

Puede que tenga que recopilar información de configuración de fuentes diversas como administradores de la red o del sistema principal, programadores de aplicaciones y usuarios finales.

Si intenta conectarse a otro nodo, el administrador de dicho nodo es un contacto muy importante. El administrador de un nodo le puede indicar los nombres, las direcciones o las características de todos los recursos de dicho nodo. Con frecuencia, deberá asegurarse de que los parámetros especificados en el nodo local y remoto coincidan.

Hojas de tareas

Las pantallas de ayuda en línea del programa de administración de Motif contienen hojas de tareas que sirven de guía en las tareas específicas de configuración. Las hojas de tareas contienen punteros que conducen a todas las pantallas de ayuda de los diálogos que va a utilizar para especificar la información de configuración. Utilícelos para examinar la ayuda y ver exactamente los datos que debe recopilar.

Las hojas de tareas también hacen referencia a una ayuda más detallada para cada ventana y diálogo que debe utilizar para especificar información de configuración. Estas pantallas de ayuda explican cada campo que debe rellenar o seleccionar.

Utilización del programa de administración de Motif

Antes de utilizar el programa de administración de Motif, puede añadir, si lo desea, información de vía de acceso a su archivo `.login` o `.profile` para permitir que el sistema encuentre los programas ejecutables (consulte el apartado "Especificación de la vía de acceso de los programas de Communications Server para Linux"). Además, debe habilitar el software de Communications Server para Linux antes de poder utilizar el programa de administración (consulte el apartado "Habilitación de Communications Server para Linux" en la página 74).

Para obtener información sobre cómo invocar el programa de administración de Motif y una visión general de la utilización del programa, consulte "Gestión de Communications Server para Linux con el programa de administración de Motif" en la página 74.

Especificación de la vía de acceso de los programas de Communications Server para Linux

Para ejecutar los programas de Communications Server para Linux, debe especificar la vía de acceso del directorio que contiene los programas ejecutables de Communications Server para Linux. Para especificar la vía de acceso, añada el directorio a la variable de entorno `PATH` antes de ejecutar los programas o bien incluya el nombre del directorio cada vez que ejecute los programas.

El programa de administración de Motif se almacena en el directorio `/opt/ibm/sna/bin/X11` y los demás programas se almacenan en el directorio

Utilización del programa de administración de Motif

`/opt/ibm/sna/bin`. Si añade estos directorios a la definición de la variable de entorno `PATH` en el archivo `.login` o `.profile`, Communications Server para Linux localizará los programas automáticamente. También puede especificar el nombre del directorio cuando ejecute el programa, como en los ejemplos siguientes:

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

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

Las líneas de mandatos de ejemplo indican que se han añadido los directorios a la variable de entorno `PATH` y, por consiguiente, no se incluyen los nombres de directorio.

Habilitación de Communications Server para Linux

Communications Server para Linux debe estar habilitado en el sistema local para poder configurar o gestionar el nodo local. Igual que con cualquier aplicación de X/Motif, puede que tenga que configurar la variable de entorno `DISPLAY` para indicar un servidor X adecuado.

Para habilitar Communications Server para Linux, escriba el mandato siguiente en la solicitud de mandatos de Linux:

```
sna start
```

Nota: Si utiliza el mandato `sna start`, Communications Server para el software de Linux utiliza el directorio a partir del que ha lanzado el mandato como su directorio de trabajo actual y mantiene uno o varios descriptores de archivo abiertos en dicho directorio. Esto significa que no podrá desmontar el sistema de archivos que contiene dicho directorio mientras Communications Server para el software de Linux esté en ejecución. Para evitar problemas, debería iniciar Communications Server para el software de Linux desde el directorio de un sistema de archivos que no precise ser desmontado; por ejemplo, podría utilizar `cd /` para cambiar al directorio raíz antes de utilizar el mandato `sna start`.

Cuando se instala Communications Server para Linux, el programa de utilidad de instalación actualiza el archivo de arranque `/etc/rc.d/init.d/snastart` de forma automática para que incluya el mandato `sna start`. Esto garantiza que Communications Server para Linux se inicie automáticamente al arrancar el sistema. Si no desea que Communications Server para Linux se inicie automáticamente, puede eliminar esta línea o ponerla como comentario y, a continuación, seguir las instrucciones de este apartado para habilitar el software de Communications Server para Linux manualmente.

Communications Server para Linux graba mensajes en la salida de error estándar (normalmente a la pantalla del terminal) para indicar que se está inicializando y para indicar si la inicialización se ha completado correctamente.

Gestión de Communications Server para Linux con el programa de administración de Motif

Para utilizar el programa de administración de Motif para Communications Server para Linux, asegúrese primero de que Communications Server para Linux se haya inicializado tal como se describe en el apartado "Habilitación de Communications Server para Linux". (Puede que tenga que configurar la variable de entorno `DISPLAY` para indicar un servidor X adecuado.)

Utilización del programa de administración de Motif

Para iniciar el programa de administración de Motif en segundo plano, emita este mandato:

xsnaadmin &

Communications Server para Linux muestra la ventana Dominio. Esta ventana muestra todo los nodos definidos y permite iniciar y detener los nodos. Si efectúa una doble pulsación en cualquier nodo aparecerá su ventana Nodo, tal como se muestra en la Figura 4 en la página 76.

La ventana Nodo muestra información sobre el nodo y sus recursos. programa de administración le solicita que lo haga tal como se describe en “Configuración del nodo” en la página 80.

Nota: esta guía utiliza el término ventana para describir las ventanas de Motif que muestran información sobre recursos de Communications Server para Linux. Una ventana puede contener una o más secciones o paneles. Un diálogo es una ventana de Motif en la que el usuario puede entrar información.

La ventana Nodo muestra casi toda la información que necesita, y desde ella, puede acceder fácilmente a todos los demás paneles o ventanas. Contiene los recursos clave del nodo local.

Si configura un sistema cliente/servidor de Communications Server para Linux con más de un nodo, siga las instrucciones de este capítulo para configurar un nodo cada vez (volviendo a la ventana Dominio para seleccionar el siguiente nodo).

Desde el menú **Ventanas** de la ventana Nodo puede acceder a otras ventanas. Estas ventanas son las siguientes:

- Ventana Agrupaciones de LU
- Ventana Nombres de destino CPI-C

El menú **Servicios** de la ventana Nodo proporciona una forma rápida de añadir recursos y proporcionar ayuda para las tareas de configuración y gestión. El menú **Diagnóstico** le lleva a los diálogos Anotaciones y Rastreo.

Ventana Nodo

En la Figura 4 se muestra un ejemplo de ventana Nodo. La barra de título muestra el nombre del sistema Linux.

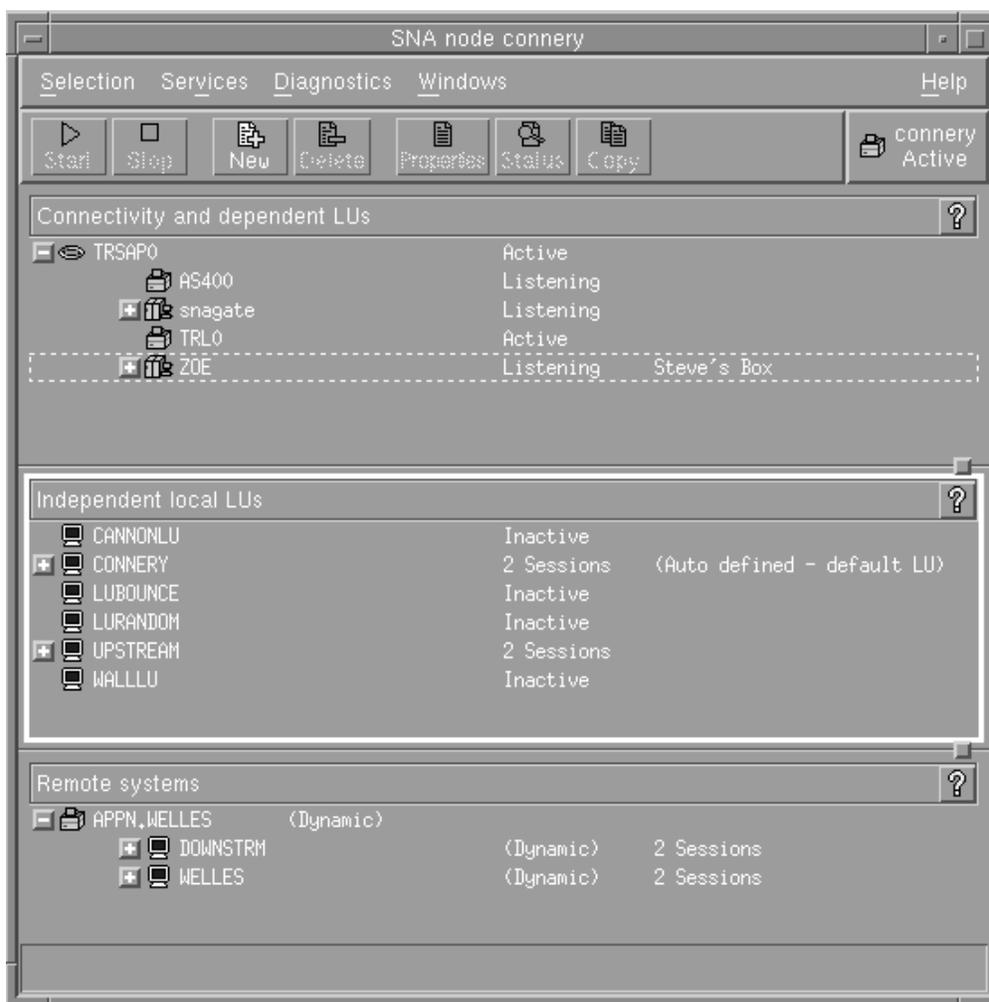


Figura 4. Ventana Nodo

En la ventana Nodo, puede configurar y gestionar todos los recursos y componentes del nodo Communications Server para Linux.

- Puertos
- Estaciones de enlace
- LU de tipo 0-3 y LU dependientes de tipo 6.2
- PU internas de DLUR
- LU locales independientes
- Nodos remotos
- LU asociadas

Desde la ventana Nodo, puede añadir, suprimir, modificar y gestionar todos estos recursos. La disposición de los recursos en la ventana muestra las relaciones entre los recursos y le permite decidir cuáles desea visualizar.

Utilización del programa de administración de Motif

Los puertos, las LU locales y los nodos remotos siempre se visualizan. La ventana Nodo muestra cada estación de enlace por debajo de su puerto superior, y cada LU dependiente por debajo de su estación de enlace superior. También muestra las LU asociadas por debajo de las LU locales y por debajo de los nodos remotos.

La ventana Nodo contiene secciones diferentes según el tipo de recurso del nodo:

- El recuadro Nodo en la esquina superior derecha de la ventana Nodo indica si el nodo está **Activo** o **Inactivo**.
- El panel superior de la ventana Nodo (panel **Conectividad**) lista los recursos de conectividad del nodo, incluidos los puertos, las estaciones de enlace, las PU de cada puerto y las LU dependientes de una PU o estación de enlace específica. Esta ventana muestra información de estado actual sobre cada recurso.
- El panel del medio (panel **LU locales independientes**) muestra las LU independientes definidas en el nodo local. Esta ventana también muestra información sobre sesiones que utilizan una LU especificada y sobre registros que definen la ubicación de una LU asociada según la estación de enlace que utiliza para acceder a la LU asociada.
- El panel inferior (panel **Sistemas remotos**) muestra información sobre nodos remotos y LU asociadas. También muestra información de sesión para cada nodo remoto o LU asociada.

Puede seleccionar cualquiera de estos paneles pulsando en uno de ellos. También puede seleccionar recursos específicos dentro de un panel con solo pulsar en la línea del recurso. Para ver o modificar la configuración de un elemento, pulse dos veces sobre éste. (Puede utilizar los botones y menús de esta ventana para acceder a la información de configuración de recursos específicos.)

Los recursos de cada elemento listado aparecen jerarquizados dentro de la información de dicho elemento. Por ejemplo, las estaciones de enlace se agrupan debajo del puerto al que pertenecen. Puede pulsar en el botón **Expandir (+)** situado junto a un elemento para visualizar todos sus recursos si no se muestran en ese momento o pulsar en el botón **Contraer (-)** para ocultar los recursos de un elemento.

Desde la ventana Nodo puede realizar las tareas de administración siguientes:

Iniciar o detener un recurso

Seleccione el recurso y pulse el botón **Iniciar** o **Detener**. (También puede seleccionar **Iniciar elemento** o **Detener elemento** en el menú **Selección**.)

Añadir un recurso a un elemento

Seleccione el elemento y pulse el botón **Nuevo** (o seleccione **Nuevo** en el menú **Selección**). Por ejemplo, para añadir una estación de enlace a un puerto, seleccione el puerto y pulse el botón **Nuevo**.

Suprimir un recurso

Seleccione el recurso y pulse el botón **Suprimir** (o seleccione **Suprimir** en el menú **Selección**).

Ver o modificar la configuración de un recurso

Seleccione el recurso y pulse el botón **Propiedades** (o seleccione **Propiedades** en el menú **Selección**).

Obtener información de estado sobre un recurso

Seleccione el recurso y pulse el botón **Estado** (o seleccione **Estado** en el menú **Selección**).

Utilización del programa de administración de Motif

Copiar la configuración de un recurso

Seleccione el recurso y pulse el botón **Copiar** (o seleccione **Copiar** en el menú **Selección**).

Además, puede elegir tareas de configuración específicas del nodo en el menú **Servicios**; rastreo (del nodo) y anotaciones (del dominio) de control en el menú **Diagnóstico** y ver o modificar recursos del dominio si selecciona uno de los elementos del menú **Ventanas**.

Elementos de los recursos

La disposición de los recursos en la ventana muestra las relaciones entre ellos.

Si un elemento tiene uno o más elementos dependientes asociados a él, aparecerá junto a éste un símbolo **Expandir** (+) o un símbolo **Contraer** (-):

- Un símbolo **Expandir** indica que los elementos dependientes asociados están ocultos. Para verlos, pulse en el símbolo **Expandir** o pulse la tecla + del teclado numérico.
- Un símbolo **Contraer** indica que no hay elementos dependientes ocultos. Puede pulsar en el símbolo **Contraer** o pulsar la tecla - del teclado numérico para ocultarlos.
- Si el elemento no tiene ningún símbolo asociado, significa que no tiene recursos dependientes asociados.

Por ejemplo, una estación de enlace está asociada a un puerto específico. En el panel Conectividad de la ventana Nodo, la estación de enlace se visualiza por debajo de su puerto superior, junto con las otras estaciones de enlace asociadas a ese puerto. El puerto siempre estará visible, pero puede decidir que la lista de estaciones de enlace asociadas esté visible o no. Asimismo, las listas de estaciones de enlace con LU asociadas pueden expandirse para mostrar las LU o contraerse para ocultarlas.

Un recurso superior siempre debe configurarse antes que los recursos dependientes; si se suprime el recurso superior también se eliminarán todos sus recursos dependientes.

Botones de la barra de herramientas

Las ventanas de recursos contienen botones de barra de herramientas a fin de que resulte más fácil realizar las tareas habituales. En la Figura 5 se muestra una barra de herramientas de Communications Server para Linux.



Figura 5. Barra de herramientas de Communications Server para Linux

En las barras de herramientas de cada ventana de recursos no aparecen todos los botones. Si la operación de un botón no es válida para el elemento seleccionado en ese momento (o una operación necesita que se seleccione un elemento, pero no hay ninguno seleccionado), el perfil del botón aparece de color gris, y la función no puede seleccionarse (aunque pulse el botón, no tendrá ningún efecto). En las ventanas de recursos pueden aparecer los botones siguientes:

Iniciar Inicia el elemento seleccionado.

Detener

Detiene el elemento seleccionado.

Nuevo

Añade un recurso nuevo.

Suprimir

Suprime los recursos seleccionados.

Propiedades

Abre el diálogo del elemento seleccionado para ver o modificar la configuración del mismo.

Estado

Muestra el estado actual del elemento seleccionado.

Copiar

Copia el elemento seleccionado. Si pulsa este botón, se abre un diálogo cuyos campos duplican la configuración del elemento seleccionado. Rellene los campos del diálogo (escribiendo el nombre del elemento nuevo) para añadir el recurso nuevo.

Muchos recursos, como los puertos y las estaciones de enlace, no pueden modificarse mientras están activos. No obstante, puede ver los parámetros de un recurso activo si selecciona el recurso y pulsa el botón **Propiedades** para abrir su diálogo. Pulse el botón **Cerrar** cuando haya terminado.

Configuración de las funciones de cliente/servidor

Este apartado sólo es pertinente si ha instalado Communications Server para Linux para ejecutarlo en un entorno de cliente/servidor (con varios nodos Communications Server para Linux en la misma red).

En un entorno de cliente/servidor, un servidor puede tener que actuar como servidor de configuración; Communications Server para Linux mantiene una lista de estos servidores de configuración. El primer servidor que aparece es el servidor maestro y los demás son servidores de reserva. Los servidores se relacionan por orden, por lo que el segundo servidor (el primer servidor de reserva) toma el control si el servidor maestro no está disponible, el tercer servidor (el segundo servidor de reserva) toma el control si no está disponible el servidor maestro ni el primer servidor de reserva, etcétera.

Cuando alguno de los nodos del dominio está activo, el primer servidor de configuración disponible del dominio (el primer servidor con el que se puede establecer contacto que ejecute el software de Communications Server para Linux) se convierte en el servidor maestro. Si el maestro actual no está disponible (porque no se puede establecer contacto con él, quizás debido a una anomalía en la red o porque se ha detenido el software SNA que ejecutaba), el siguiente servidor de configuración disponible de la lista se convierte en el nuevo maestro.

Communications Server para Linux puede ejecutarse sin maestro. Esto ocurre si no se puede establecer contacto con ninguno de los servidores de la lista de servidores de configuración. Si ocurre esto, sólo podrá ver y configurar los recursos de nodo de los servidores con los que pueda establecer contacto.

Nota: no podrá indicar directamente el nodo que debe actuar como servidor maestro; el servidor maestro se selecciona basándose en el orden en que se añaden los nodos a la lista de servidores de configuración. Si desea mover un servidor al principio de la lista, elimine los demás nodos de la lista y, a continuación, vuelva a añadirlos.

Configuración de las funciones de cliente/servidor

Para añadir un servidor de configuración en la ventana Dominio del programa de administración de Motif, seleccione **Crear servidor de configuración** del menú **Selección**. El servidor se añade al final de la lista; sólo se convertirá en el servidor maestro si ninguno de los demás servidores de configuración está disponible. Para eliminar un servidor, seleccione **Eliminar servidor de configuración** en el menú **Selección**.

Nota: No puede eliminar un servidor si es el único de la lista en el que se ejecuta el software de Communications Server para Linux, porque en este caso no hay otro servidor que pueda tomar el relevo como servidor maestro. Es necesario como mínimo un servidor maestro habilitado en una configuración cliente/servidor.

Para obtener más información sobre la configuración y gestión de un sistema cliente/servidor de Communications Server para Linux, consulte la publicación *IBM Communications Server para Linux, Guía de administración*. Este manual también ofrece información acerca de la configuración avanzada de cliente/servidor, que incluye cómo trasladar clientes y servidores a diferentes dominios de Communications Server para Linux y cómo configurar los detalles del funcionamiento del cliente.

Configuración del nodo

El primer paso para configurar Communications Server para Linux en un sistema es configurar el nodo local. La configuración del nodo proporciona la información básica que el nodo necesita para comunicarse en una red SNA. Debe configurar el nodo antes de definir la conectividad u otros recursos del nodo.

Si el nodo ya está configurado, puede utilizar los procedimientos descritos en este apartado para modificar su configuración; pero debe detenerlo antes de realizar los cambios.

Antes de configurar el nodo, decida si desea configurarlo como un nodo APPN o no APPN. Esta decisión depende de las posibilidades de los otros nodos SNA con los que se comunica.

En la Figura 6 se muestra un nodo Communications Server para Linux que se comunica directamente con un sistema principal.

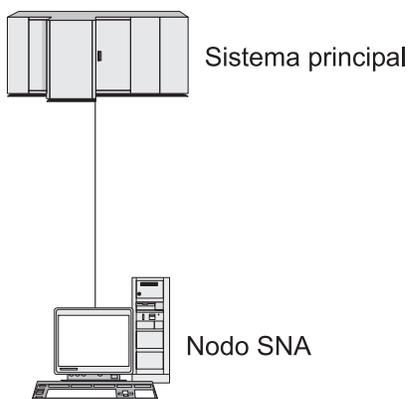


Figura 6. Nodo Communications Server para Linux que se comunica directamente con un sistema principal

Si el sistema principal no es compatible con APPN, configure el nodo Communications Server para Linux como nodo LEN. Si el sistema principal es compatible con APPN, puede configurar el nodo Communications Server para Linux como nodo de red APPN o nodo final APPN (si Communications Server para Linux utiliza SNA solamente para la comunicación con el sistema principal, puede ser conveniente configurar el nodo Communications Server para Linux como nodo final o nodo de red de ramificación).

En la Figura 7 se muestran varios nodos Communications Server para Linux en una red APPN.

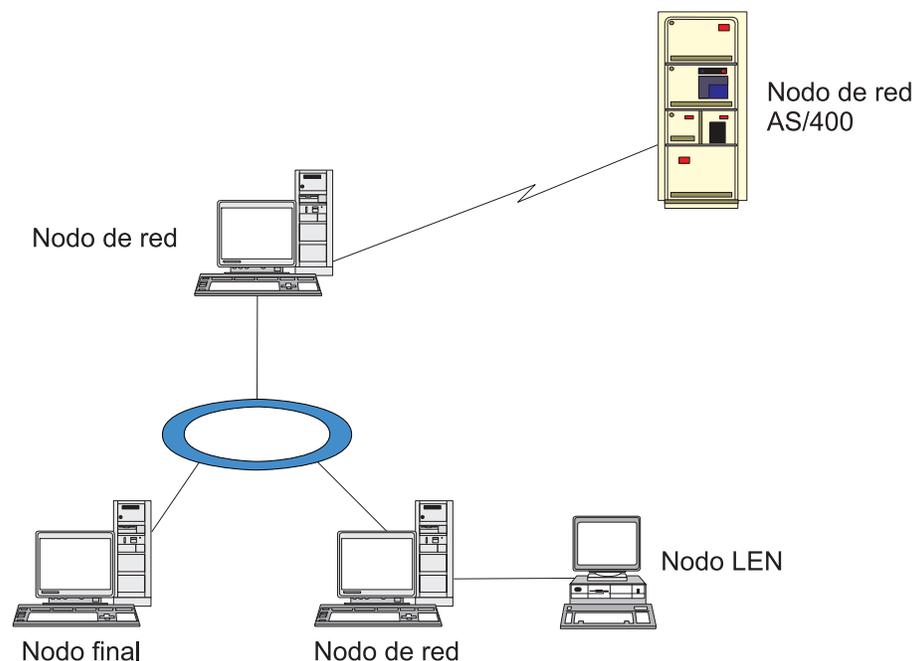


Figura 7. Nodos Communications Server para Linux en una red APPN

Cuando el nodo local forme parte de una red APPN, configúrelo como un nodo de red APPN si el nodo va a proporcionar servicios de direccionamiento APPN para otros nodos. Si hay otros nodos que proporcionan servicios de direccionamiento, configure el nodo local como un nodo final APPN. Si el nodo local sólo se comunica con un nodo conectado directamente (que puede ser de cualquier tipo), configure el nodo como un nodo LEN.

Antes de empezar a configurar el nodo, recopile la información siguiente:

- Tipo de soporte APPN (nodo de red, nodo de red de ramificación, nodo final o nodo LEN).
- Nombre de punto de control (y el alias, si es distinto). Póngase en contacto con su planificador de red para determinar el nombre.
- ID de nodo por omisión. (Puede alterar temporalmente este valor por omisión configurando un enlace de comunicaciones individual.)

Para configurar el nodo, siga estos pasos desde la ventana **Nodo**:

1. Seleccione **Configurar parámetros de nodo** en el menú **Servicios** o efectúe una doble pulsación en el recuadro **Nodo** de la esquina superior derecha de la ventana **Nodo**. Communications Server para Linux muestra el diálogo **Parámetros de nodo**.

Configuración del nodo

2. Especifique el nivel de soporte APPN, el nombre de punto de control y (si es necesario) el ID de nodo por omisión.
3. Pulse el botón **OK** para definir el nodo. Cuando el usuario define el nodo, Communications Server para Linux define automáticamente una LU por omisión con el mismo nombre que el punto de control.

Para salir sin guardar los valores especificados, pulse el botón **Cancelar**.

Configuración de la conectividad

Para que un nodo Communications Server para Linux se comunique con otros nodos, debe configurar la conectividad con al menos un nodo adyacente. Un enlace de conectividad puede configurarse para soportar tráfico dependiente, independiente o ambos.

Puede tener tarjetas adaptadoras para uno o más protocolos de enlace instalados en su sistema. La mayor parte de la información que debe especificar para configurar la conectividad depende del protocolo de enlace que utilice. Para obtener una lista de los protocolos de enlace compatibles con Communications Server para Linux, consulte "Requisitos de instalación" en la página 20.

Para configurar un enlace, debe definir un puerto y (en la mayoría de los casos) una estación de enlace. Al utilizar el programa de administración de Motif, se configura automáticamente un DLC (control de enlace de datos) como parte de la configuración del puerto. Además, tiene la opción de definir el puerto como parte de una red de conexión.

Los enlaces que necesita configurar dependen de lo que intenta conseguir y de si su red es una red APPN. La información necesaria depende del protocolo de enlace, y de si el enlace es para tráfico dependiente, independiente o ambos.

Como ejemplo, en este apartado se explica cómo configurar los tipos de enlace siguientes:

- Enlace que soporta tráfico dependiente con un sistema principal que utiliza una línea SDLC.
- Enlace que soporta tráfico dependiente e independiente en una red APPN y que utiliza un protocolo de enlace Ethernet. Este ejemplo también define una red de conexión en el puerto Ethernet.
- Enlace Enterprise Extender en una red APPN (observe que los enlaces Enterprise Extender sólo soportan el tráfico independiente).

Para obtener información sobre otros protocolos de enlace, consulte la publicación *IBM Communications Server para Linux, Guía de administración* o la ayuda en línea del programa de administración de Motif.

Configuración de un enlace SDLC para tráfico dependiente

Para un puerto SDLC (control síncrono de enlace de datos), necesita la información siguiente:

- Nombre de puerto SNA (por norma, puede utilizar el valor por omisión). Puede ser también necesario proporcionar el número de dispositivo SDLC.
- Indicación de si el puerto se debe activar automáticamente al iniciar el nodo.
- Tipo de línea (línea conmutada de salida, conmutada de entrada o alquilada).
- Función del enlace (primario, secundario, negociable, multipunto primario o multi-PU secundario).

- Dirección de sondeo (solamente para una línea entrante conmutada en un puerto no primario). Para otros tipos de puertos puede configurar la dirección de sondeo en la estación de enlace.

Para una estación de enlace SDLC, necesita la información adicional siguiente:

- Método de activación (por administrador, al iniciar el nodo o por solicitud).
- Tipo de tráfico soportado (para este ejemplo, dependiente solamente).
- Función del nodo remoto (para este ejemplo, sistema principal).

Para configurar el enlace SDLC, ejecute estos pasos en la ventana **Nodo**:

1. Configure el puerto:
 - a. Seleccione el panel **Conectividad** de la ventana.
 - b. Seleccione **Nuevo puerto** en el submenú **Conectividad** del menú **Servicios** (o pulse el botón **Nuevo** de la barra de botones).
 - c. En el diálogo que aparece, seleccione el tipo de protocolo en el menú de opciones y, a continuación, defina un puerto.
Al pulsar en el botón **OK**, **Communications Server para Linux** muestra el diálogo **Puerto SDLC**.
 - d. Especifique los valores adecuados en los campos del diálogo.
 - e. Pulse el botón **OK** para definir el puerto.
El puerto aparece en el panel **Conectividad** de la ventana **Nodo**.
2. Defina una estación de enlace en el puerto:
 - a. Asegúrese de haber seleccionado el puerto al que va a añadirse la estación de enlace en el panel **Conectividad** de la ventana **Nodo**.
 - b. Seleccione **Nueva estación de enlace** en el submenú **Conectividad** del menú **Servicios** (o pulse el botón **Nuevo** de la barra de botones).
 - c. Pulse el botón **OK**.
Communications Server para Linux muestra el diálogo **Estación de enlace SDLC**.
 - d. Especifique los valores adecuados en los campos del diálogo.
 - e. Pulse el botón **OK** para definir la estación de enlace.
La estación de enlace se muestra por debajo del puerto al que pertenece en el panel **Conectividad** de la ventana **Nodo**.

Configuración de un enlace Ethernet para tráfico dependiente e independiente

Este ejemplo muestra cómo configurar un enlace Ethernet que soporte tráfico dependiente e independiente en una red APPN. Además, define una red de conexión en el puerto Ethernet.

Para un puerto Ethernet, necesita la información siguiente:

- Nombre de puerto SNA (por norma, puede utilizar el valor por omisión). Si tiene varias tarjetas adaptadoras Ethernet, debe proporcionar el número de tarjeta Ethernet. También necesita especificar el número de SAP (punto de acceso a servicio) (normalmente 04 para adaptadores Intel y OSA2). Para los adaptadores OSA-Express, el número SAP local debe coincidir con el definido en OSA/SF para las direcciones de dispositivo de E/S que corresponden a la interfaz ethX de esta imagen de Linux.
- Indicación de si el puerto se debe activar automáticamente al iniciar el nodo.

Configuración de la conectividad

- Nombre de red de conexión (debe ser el mismo en todos los puertos de la misma red de conexión).

Para una estación de enlace Ethernet, necesita la siguiente información adicional:

- Método de activación (por administrador, al iniciar el nodo o por solicitud).
- Tipo de tráfico soportado (para este ejemplo, dependiente e independiente).
- Nombre de punto de control de nodo remoto (obligatorio sólo para un nodo LEN).
- Tipo de nodo remoto (nodo de red, nodo final o descubrir).
- Función de nodo remoto (para este ejemplo, pasarela SNA en sentido descendente o DLUR de paso a través).
- Para configurar una estación de enlace selectiva, necesita la dirección MAC (control de acceso medio) y el número de SAP (normalmente 04) para la estación remota. Si no proporciona información de dirección, y especifica Por administrador en el campo *Activación*, la estación de enlace es una estación de enlace de escucha no selectiva.

Para configurar el enlace Ethernet, siga estos pasos desde la ventana **Nodo**:

1. Configure el puerto:
 - a. Seleccione el panel **Conectividad** de la ventana.
 - b. Seleccione **Nuevo puerto** en el submenú **Conectividad** del menú **Servicios** (o pulse el botón **Nuevo** de la barra de botones).
 - c. En el diálogo que aparece, seleccione el tipo de protocolo en el menú de opciones y, a continuación, defina un puerto.
Al pulsar en el botón **OK**, Communications Server para Linux muestra el diálogo SAP Ethernet.
 - d. Especifique los valores adecuados en los campos del diálogo.
 - e. Pulse el botón **OK** para definir el puerto.
El puerto aparece en el panel **Conectividad** de la ventana **Nodo**.
2. Defina una estación de enlace en el puerto:
 - a. Asegúrese de haber seleccionado el puerto al que va a añadirse la estación de enlace en el panel **Conectividad** de la ventana **Nodo**.
 - b. Seleccione **Nueva estación de enlace** en el submenú **Conectividad** del menú **Servicios** (o pulse el botón **Nuevo** de la barra de botones).
 - c. Pulse el botón **OK**.
Communications Server para Linux muestra el diálogo Estación de enlace Ethernet.
 - d. Especifique los valores adecuados en los campos del diálogo.
 - e. Pulse el botón **OK** para definir la estación de enlace.
La estación de enlace se muestra por debajo del puerto al que pertenece en el panel **Conectividad** de la ventana **Nodo**.

Configuración de un enlace Enterprise Extender

Este ejemplo muestra cómo configurar un enlace Enterprise Extender en una red APPN. Observe que los enlaces Enterprise Extender sólo soportan el tráfico de LU independiente.

Para un puerto Enterprise Extender, necesita la información siguiente:

- Nombre de puerto SNA (por norma, puede utilizar el valor por omisión). Si dispone de varias tarjetas adaptadoras de red que ejecutan IP, también deberá suministrar el nombre de interfaz IP que desea utilizar (por ejemplo, eth0).
- Indicación de si el puerto se debe activar automáticamente al iniciar el nodo.

Para una estación de enlace Enterprise Extender, necesita la siguiente información adicional:

- Método de activación (por administrador, al iniciar el nodo o por solicitud).
- Tipo de nodo remoto (nodo de red, nodo final o descubrir).
- Para configurar una estación de enlace selectiva, necesita el nombre de sistema principal IP o la dirección IP de la estación remota. Si no proporciona esta información, y especifica Por administrador en el campo *Activación*, la estación de enlace es una estación de enlace de escucha no selectiva.

Para configurar el enlace Enterprise Extender, lleve a cabo estos pasos desde la ventana Nodo:

1. Configure el puerto:
 - a. Seleccione el panel Conectividad de la ventana.
 - b. Seleccione **Nuevo puerto** en el submenú **Conectividad** del menú **Servicios** (o pulse el botón **Nuevo** de la barra de botones).
 - c. En el diálogo que aparece, seleccione el tipo de protocolo en el menú de opciones y, a continuación, defina un puerto.
Al pulsar en el botón **OK**, Communications Server para Linux muestra el diálogo Puerto IP.
 - d. Especifique los valores adecuados en los campos del diálogo.
 - e. Pulse el botón **OK** para definir el puerto.
El puerto aparece en el panel Conectividad de la ventana Nodo.
2. Defina una estación de enlace en el puerto:
 - a. Asegúrese de haber seleccionado el puerto al que va a añadirse la estación de enlace en el panel Conectividad de la ventana Nodo.
 - b. Seleccione **Nueva estación de enlace** en el submenú **Conectividad** del menú **Servicios** (o pulse el botón **Nuevo** de la barra de botones).
 - c. Pulse el botón **OK**.
Communications Server para Linux muestra el diálogo Estación de enlace IP.
 - d. Especifique los valores adecuados en los campos del diálogo.
 - e. Pulse el botón **OK** para definir la estación de enlace.
La estación de enlace se muestra por debajo del puerto al que pertenece en el panel Conectividad de la ventana Nodo.

Configuración de las LU de tipo 0–3

Para poder utilizar aplicaciones de usuario que hacen uso de unidades LU de tipo 0–3, debe configurar unidades LU dependientes. Antes de hacerlo, debe realizar estos pasos de configuración:

- Configure el nodo según se describe en “Configuración del nodo” en la página 80.
- Configure un enlace para dar soporte al tráfico de LU dependiente tal como se describe en “Configuración de la conectividad” en la página 82.

Configuración de las LU de tipo 0–3

No es necesario que configure un enlace directo con el sistema principal si tiene un enlace ascendente hacia otro nodo y utiliza una pasarela SNA, o si está utilizando DLUR. Para obtener más información, consulte “Configuración de la pasarela SNA” en la página 95 y “Configuración del DLUR” en la página 98.

Debe configurar unidades LU dependientes de los tipos 0–3 para permitir la comunicación con un sistema principal. Puede utilizar la información de esta sección para definir una LU y dar soporte a la concentración de LUA, DLUR o PU. Puede también definir un rango de unidades LU para configurar varias LU del mismo tipo en una sola operación.

Además, puede definir una agrupación de unidades LU para ser utilizadas cuando convenga, ya sea asignando una LU a una agrupación cuando defina la LU o asignando unidades LU definidas previamente a una agrupación.

Definición de las LU de tipo 0–3

Antes de configurar la LU 3270, recopile la información siguiente:

- Nombre de LU (Se trata de un identificador local y no tiene que coincidir con la configuración del sistema principal.)
- Número de LU (o números para un rango de LU)
- Tipo de LU (modelo de pantalla 3270 o impresora 3270)
- Nombre de agrupación (si añade la LU a una agrupación)

Para configurar una LU de los tipos 0–3 para una estación de enlace previamente definida, siga estos pasos desde la ventana Nodo:

1. Seleccione la estación de enlace para el sistema principal en el panel Conectividad de la ventana.
2. Pulse el botón **Nuevo**.
3. Seleccione el tipo de LU (**Nueva LU de pantalla 3270** o **Nueva LU de impresora 3270**) en el diálogo que aparece.
Cuando selecciona este elemento y pulsa **OK**, Communications Server para Linux muestra el diálogo LU de tipo 0–3.
4. Especifique los valores adecuados en los campos del diálogo.
5. Pulse **OK** para definir la LU.

La LU aparece en el panel Conectividad de la ventana Nodo, por debajo de la estación de enlace para el sistema principal.

Definición de una agrupación de LU

Para la LU de tipo 0–3, puede definir agrupaciones de unidades LU para simplificar la configuración de usuarios y proporcionar una mayor flexibilidad al establecer sesiones de sistema principal. Por ejemplo, puede definir varias unidades LU en una misma agrupación de unidades LU y después configurar varios usuarios utilizando esta agrupación de unidades LU. Esto facilita la configuración de las sesiones de usuario y permite que cualquier sesión utilice cualquier LU de la agrupación.

Nota: puede asignar la sesión de un usuario a una LU específica o a una agrupación de LU.

- Si asigna la sesión de usuario a una LU específica que se encuentra en una agrupación, la sesión utilizará esa LU si está disponible; de lo contrario, utilizará cualquier LU libre de la agrupación, como si la hubiera asignado a la agrupación de LU en vez de asignarla a una LU específica.

- Si desea que el usuario sólo utilice la LU especificada y que no pueda establecer la sesión de usuario si la LU ya se utiliza, asegúrese de que la LU no se encuentre en una agrupación.

Puede ver las agrupaciones de unidades LU para el nodo Communications Server para Linux local utilizando la ventana Agrupaciones de LU. Esta ventana muestra las agrupaciones de LU configuradas en el sistema local y le permite seleccionar las LU que desee añadir a una agrupación de LU.

Puede añadir los tipos de LU siguientes a una agrupación (no mezcle unidades LU de tipos distintos en la misma agrupación):

- LU de pantalla 3270
- LU no restringida

Antes de añadir una o varias unidades LU a una agrupación, las LU deben estar definidas en el nodo local.

Para configurar una agrupación de LU, siga estos pasos desde la ventana Nodo:

1. Seleccione **Agrupaciones de LU** en el menú **Ventanas**.
Communications Server para Linux muestra la ventana Agrupaciones de LU.
2. Pulse el botón **Nuevo**.
Communications Server para Linux muestra el diálogo Configuración de una agrupación de LU.
El recuadro de la derecha muestra las LU que no se han asignado todavía a ninguna agrupación. Cualquiera de ellas pueden incluirse en la nueva agrupación.
3. Seleccione las LU que desea añadir a la agrupación y pulse el botón **Nuevo** para mover las LU seleccionadas al recuadro de la izquierda.
Para eliminar una LU del recuadro de la izquierda, selecciónela y pulse el botón **Eliminar**.
4. Pulse **OK** para definir la agrupación de LU.
Todas las LU del recuadro de la izquierda se añaden a la agrupación de LU.
La agrupación aparece en la ventana Agrupaciones de LU.

Configuración de la comunicación APPC

Las aplicaciones APPC y las aplicaciones CPI-C necesitan que primero se configure APPC. Una aplicación APPC utiliza los recursos de LU de tipo 6.2 del nodo para comunicarse con otra aplicación APPC o CPI-C de un sistema principal o un sistema igual, utilizando una modalidad especificada.

Antes de configurar la comunicación APPC, debe llevar a cabo la configuración siguiente:

1. Configure el nodo según se describe en “Configuración del nodo” en la página 80.
2. Configure la conectividad según se describe en “Configuración de la conectividad” en la página 82.

Los pasos de configuración siguientes dependen de si la configuración soporta tráfico dependiente, independiente o ambos.

Configuración de la comunicación APPC

APPC independiente

APPC independiente utiliza LU independientes. Cada sesión LU-LU comprende una LU local y una LU asociada.

Para la LU local, puede utilizar la LU por omisión predefinida asociada al punto de control de nodo o bien puede configurar LU locales nuevas.

No es necesario configurar la LU asociada si el nodo Communications Server para Linux es un nodo final o nodo de una red APPN, pues APPN puede localizar dinámicamente las LU asociadas. Sin embargo, deberá configurar la LU asociada si la red no es una red APPN o si el nodo es un nodo LEN. En este caso, debe configurar el nodo remoto donde reside la LU asociada y, a continuación, definir la LU asociada en el nodo remoto.

APPC dependiente

Si el nodo remoto es un sistema principal que no soporta la LU 6.2 independiente, realice la configuración para el tráfico dependiente. Para APPC dependiente, debe configurar una LU local.

Si las aplicaciones utilizan CPI-C, puede que necesite efectuar una configuración de CPI-C adicional después de la configuración de APPC (consulte “Configuración de CPI-C” en la página 93). Una aplicación CPI-C utiliza los recursos de LU de tipo 6.2 y de modalidad del nodo para comunicarse con otra aplicación APPC o CPI-C de un sistema principal o un sistema igual. Para una aplicación CPI-C debe definir los mismos recursos que para una aplicación APPC. Además, si el TP del sistema Communications Server para Linux es el TP solicitante, también denominado TP de origen (el TP que inicia la conversación), puede ser necesario definir una o más entradas de información adicional para él, tal como se describe en “Configuración de CPI-C” en la página 93. Cada una de estas entradas proporciona información sobre un TP asociado y sobre los recursos de LU y de modalidad utilizados para acceder al TP asociado, así como la información de seguridad necesaria.

En este apartado se explica cómo configurar una red APPN sencilla (utilizando una LU 6.2 independiente) que se compone de un nodo de red, un nodo final y un nodo LEN, como se describe en “Configuración de una red APPN sencilla”. (También se muestra cómo obtener información de estado para sesiones CP-CP entre dos nodos.)

Además, se explica cómo configurar comunicación APPC dependiente, según se describe en “Configuración de APPC dependiente” en la página 93.

En estos dos casos, se presupone que las sesiones APPC utilizan una clase de servicio (COS) y una modalidad estándar.

Para obtener información sobre la configuración de información adicional de APPC, como por ejemplo, modalidades, seguridad y TP invocables (de destino), consulte la publicación *IBM Communications Server para Linux, Guía de administración*.

Configuración de una red APPN sencilla

La red APPN más sencilla que puede configurar consta de dos nodos: un nodo de red APPN y un nodo final APPN. El nodo de red gestiona el direccionamiento de la sesión para el nodo final.

Configuración de un nodo de red

Este escenario supone que está utilizando la LU de punto de control y una modalidad estándar, y que utiliza un tipo de enlace LAN (Token Ring, Ethernet). Para configurar el nodo de red basta con realizar las tareas siguientes:

1. Configure el nodo según se describe en “Configuración del nodo” en la página 80. En el campo *Soporte para APPN*, seleccione el valor *Nodo de red*. Anote el nombre del punto de control.
2. Configure la conectividad según se describe en “Configuración de la conectividad” en la página 82. Configure el enlace para soportar tráfico independiente.

Para acceder a este nodo de red desde un nodo final adyacente, debe conocer la dirección MAC y el número de SAP del puerto del nodo de red. Puede utilizar el procedimiento siguiente para obtener la dirección MAC en un nodo Communications Server para Linux:

1. Seleccione el puerto en la ventana *Nodo*.
2. Pulse el botón **Iniciar** para iniciar el puerto.
3. Pulse el botón **Estado** para obtener la información de estado del puerto. El diálogo de estado de puerto muestra la dirección MAC y el número de SAP.
4. Anote la dirección MAC y el número de SAP y especifique dichos valores en el diálogo de configuración de la estación de enlace del nodo final.

Configuración de un nodo final

Este escenario supone que está utilizando la LU de punto de control y una modalidad estándar, y que utiliza un tipo de enlace LAN (Token Ring, Ethernet). Para configurar el nodo de red basta con realizar las tareas siguientes:

1. Configure el nodo según se describe en “Configuración del nodo” en la página 80. En el campo *Soporte para APPN*, seleccione el valor *Nodo final*.
2. Configure la conectividad según se describe en “Configuración de la conectividad” en la página 82. Configure el enlace para soportar tráfico independiente y proporcione la información siguiente para la estación de enlace:
 - Especifique el nombre del nodo de red (consulte “Configuración de un nodo de red”) como valor del campo *Nodo remoto*.
 - Especifique la dirección MAC y el número de SAP para el puerto del nodo remoto en el panel Información de contacto del diálogo de configuración de la estación de enlace.

En una red APPN, puede utilizarse una sola estación de enlace para un nodo de red adyacente para comunicarse con cualquier nodo remoto de la red, de modo que no es necesario configurar una estación de enlace diferente para cada nodo remoto.

Verificación de conectividad entre dos nodos

Para este caso se presupone que se ha configurado un nodo de red como se describe en “Configuración de un nodo de red” y un nodo final como se describe en “Configuración de un nodo final”. Desde el nodo final efectúe el procedimiento siguiente:

1. En la ventana *Nodo*, seleccione la estación de enlace que se conecta al nodo de red adyacente.
2. Pulse el botón **Iniciar** para iniciar la estación de enlace.

Configuración de la comunicación APPC

Una vez iniciada la estación de enlace, las sesiones CP-CP entre dos nodos se establecen automáticamente. Estas sesiones se visualizan en el panel LU locales independientes de la ventana Nodo.

3. Para obtener información de estado sobre una sesión, seleccione la sesión en la ventana Nodo y pulse el botón **Estado**.

Configuración de una LU APPC independiente

En muchos casos, las aplicaciones pueden utilizar la LU de punto de control del nodo local, que se define automáticamente al configurar el nodo. Es la LU por omisión (si la aplicación no especifica una LU determinada, puede utilizar ésta). Si la aplicación utiliza la LU por omisión, no es necesario definir una LU local. Consulte la documentación de su aplicación APPC o póngase en contacto con el programador de la aplicación.

Para configurar una LU 6.2 independiente, necesita esta información:

- Nombre de LU local.
- Alias de LU local (si se utiliza un alias en un TP soportado por esta LU).

Para configurar una LU local independiente, siga estos pasos desde la ventana Nodo:

1. Seleccione el panel LU locales independientes en la ventana.
2. Seleccione **Nueva LU local independiente** en el submenú **APPC** del menú **Servicios** (o pulse el botón **Nuevo**).
Communications Server para Linux muestra el diálogo LU local.
3. Especifique los valores adecuados en los campos del diálogo.
4. Pulse el botón **OK** para definir la LU local. En el panel LU locales independientes de la ventana Nodo aparece la LU independiente.

Configuración de LU asociadas para un nodo LEN

Debe definir un nodo remoto (y las LU asociadas del nodo) en las situaciones siguientes:

- Si el nodo local es un nodo LEN, debe definir todos los nodos remotos y todas las LU asociadas del nodo remoto con el que se comunica mediante APPC. Un nodo LEN no puede encontrar dinámicamente las LU asociadas; la definición de nodo remoto le permite hacerlo.
- Si el nodo local no forma parte de una red APPN (por ejemplo, si tiene dos nodos finales conectados directamente, sin ningún servidor de nodos de red), no es posible encontrar dinámicamente las LU. En este caso, debe configurar cada una de las LU asociadas.
- Si el nodo remoto es un nodo LEN y el nodo local es un nodo de red que actúa como servidor de nodos de red del nodo LEN, debe definir el nodo LEN (y sus LU asociadas) como un nodo remoto en el servidor de nodos de red. Esta definición permite que los nodos del resto de la red APPN encuentren las LU del nodo LEN.
- Si el nodo remoto está en otra red APPN, debe definir el nodo remoto porque no puede encontrarse dinámicamente.

No defina las LU asociadas si los nodos remotos y locales forman parte de la misma red APPN.

Al añadir una definición de nodo remoto, se añade automáticamente una LU asociada con el mismo nombre que el nodo remoto; ésta es la LU de punto de control del nodo remoto. Si su aplicación utiliza esta LU asociada, no es necesario

añadir otra LU asociada, aunque tal vez desee añadir un alias de LU para la LU asociada. Para añadir un alias, pulse dos veces en la LU asociada y especifique el alias en el diálogo de configuración de LU asociada.

Si su aplicación utiliza un alias de LU para referirse a su LU asociada, debe añadir una definición de alias de LU asociada.

Si el nodo local o el nodo remoto es un nodo LEN, debe definir la LU asociada como dependiente del nodo remoto, ya que un nodo LEN no puede participar en la ubicación dinámica de LU. Si su aplicación utiliza la LU de punto de control del nodo remoto como su LU asociada, la LU de punto de control se ha definido automáticamente al definir el nodo remoto.

Puede utilizar el programa de administración de Motif si desea añadir un alias de LU asociada (consulte “Definición de un alias de LU asociada”), añadir una definición de una LU asociada en un nodo remoto específico (consulte “Definición de una LU asociada en un nodo remoto” en la página 92) o definir varias LU asociadas con comodines (consulte “Definición de varias LU asociadas mediante comodines” en la página 92).

Definición de un nodo remoto: Antes de configurar un nodo remoto, necesita la información siguiente:

- Nombre de red SNA del nodo completamente calificado.

Para configurar un nodo remoto, siga estos pasos desde la ventana Nodo:

1. Seleccione el panel Sistemas remotos en la ventana.
2. Seleccione **Nuevo nodo remoto** del submenú **APPC** del menú **Servicios** (o pulse el botón **Nuevo** de la barra de botones y, a continuación, seleccione **Definir nodo remoto**).

Communications Server para Linux muestra el diálogo Configuración de nodo remoto.

3. Especifique los valores adecuados en los campos del diálogo.
4. Pulse el botón **OK** para definir el nodo remoto. El nodo remoto aparece en el panel Sistemas remotos de la ventana Nodo.

Cuando se define un sistema remoto, Communications Server para Linux define automáticamente la LU de punto de control del nodo remoto como LU asociada del nodo local.

Definición de un alias de LU asociada: Para definir un alias de LU asociada, necesita esta información:

- Nombre de LU asociada completamente calificado (nombre de red SNA y nombre de LU).
- Alias de LU asociada utilizado por un TP local.

Para añadir un alias de LU asociada, siga estos pasos desde la ventana Nodo:

1. Seleccione el panel Sistemas remotos en la ventana.
2. Seleccione **APPC**, **Nuevas LU asociadas** y **Alias de LU asociada** en el menú **Servicios** (o pulse el botón **Nuevo** de la barra de botones y seleccione **Definir alias de LU asociada**).

Communications Server para Linux muestra el diálogo Configuración de alias de LU asociada.

3. Especifique el nombre de la LU asociada y el alias en el diálogo.

Configuración de la comunicación APPC

4. Pulse el botón **OK** para definir el alias de LU asociada. Éste aparece en el panel Sistemas remotos de la ventana Nodo (como parte de la definición de red).

Definición de una LU asociada en un nodo remoto: Para definir una LU asociada en un nodo remoto específico, necesita la información siguiente:

- Nombre de LU asociada completamente calificado.
- Alias de LU asociada (si el TP local utiliza un alias).
- Nombre completamente calificado del nodo que contiene información de directorio para la LU asociada.

Para añadir una definición de LU asociada para un nodo remoto específico, siga estos pasos desde la ventana Nodo:

1. Seleccione el nodo remoto.
2. Seleccione **APPC**, **Nuevas LU asociadas** y **LU asociada en nodo remoto** en el menú **Servicios** (o pulse el botón **Nuevo** de la barra de botones y seleccione **Definir LU asociada en nodo remoto**).
Communications Server para Linux muestra el diálogo Configuración de LU asociada.
3. Especifique los valores adecuados en los campos del diálogo.
4. Pulse el botón **OK** para definir la LU asociada. El alias de LU asociada aparece en el panel Sistemas remotos de la ventana Nodo, en el sistema remoto al que pertenece.

Definición de varias LU asociadas mediante comodines: Puede utilizar comodines para configurar la ubicación de un conjunto de LU asociadas que se encuentran en el mismo nodo remoto y cuyos nombres empiezan por los mismos caracteres. Si utiliza comodines, no necesitará configurar cada LU asociada individualmente.

Para definir LU asociadas mediante comodines, debe proporcionar esta información:

- Nombre de la LU asociada comodín. El nombre de LU asociada comodín consta de dos cadenas EBCDIC de tipo A, cada una de ellas de 1–8 caracteres, que coinciden con los nombres de LU completamente calificados de varias LU asociadas.
La primera cadena puede ser un nombre de red SNA completo que coincida exactamente con el nombre de red de las LU asociadas, o un prefijo comodín que coincida con el principio del nombre de red. Si especifica un prefijo comodín para el nombre de red, deje la segunda cadena en blanco.
Si proporciona un nombre de red SNA completo para la primera cadena, también puede especificar un valor para la segunda cadena. (No puede especificar la segunda cadena si no ha proporcionado un nombre de red SNA válido para la primera.) La segunda cadena se trata como un prefijo comodín, que debe coincidir con el principio de la segunda parte de los nombres de LU asociada completamente calificados.
- Nombre del nodo donde se encuentran las LU asociadas.

Para añadir varias LU asociadas, siga estos pasos desde la ventana Nodo:

1. Seleccione el nodo remoto para el que va a definir las LU asociadas.
2. Seleccione **APPC**, **Nuevas LU asociadas** y **Comodín de LU asociadas en nodo remoto** en el menú **Servicios** (o pulse el botón **Nuevo** de la barra de botones y seleccione **Definir comodín de LU asociadas en nodo remoto**).

Communications Server para Linux muestra el diálogo Configuración de LU asociada comodín.

3. Especifique la información adecuada en los campos del diálogo.
4. Pulse el botón **OK** para definir las LU asociadas. Las LU asociadas aparecen en el panel Sistemas remotos de la ventana Nodo, en el nodo remoto al que pertenecen.

Configuración de APPC dependiente

Para configurar una LU 6.2 dependiente, necesita esta información:

- Nombre de LU local.
- Alias de LU local (si se utiliza un alias en un TP soportado por esta LU).
- Nombre de la estación de enlace que proporciona la conexión con el sistema principal.
- Número de LU.
- Si la LU debe asignarse a la agrupación por omisión para la LU 6.2 dependiente.

Si está configurando LU dependientes de tipo 6.2 para utilizarlas con aplicaciones APPC o CPI-C, puede definirlos como miembros de la agrupación por omisión. A una aplicación que no especifica una LU local determinada se le asigna una LU que no esté en uso de la agrupación de LU definidas como LU por omisión.

Para configurar una LU local dependiente, siga estos pasos desde la ventana Nodo:

1. Seleccione una estación de enlace en el panel Conectividad de la ventana
2. Seleccione **Nueva LU local dependiente** del submenú **APPC** del menú **Servicios** (o pulse el botón **Nuevo** de la barra de botones y, a continuación, seleccione **Nueva LU local dependiente**).

Communications Server para Linux muestra el diálogo LU local.

3. Especifique los valores adecuados en los campos del diálogo.
4. Pulse el botón **OK** para definir la LU local. La LU dependiente aparece en el panel Conectividad, en la estación de enlace a la que pertenece.

Configuración de CPI-C

Si da soporte a una aplicación CPI-C que utiliza nombres de destino simbólico CPI-C, debe definir información complementaria de CPI-C. La información complementaria asocia el nombre de destino simbólico con información sobre el TP asociado, la LU asociada, la modalidad y la seguridad de la conversación.

Para determinar el nombre de destino simbólico para CPI-C, póngase en contacto con el desarrollador de la aplicación (o, si se trata de una aplicación de terceros, consulte la documentación del producto).

Antes de configurar información complementaria de CPI-C, necesita la información siguiente:

- Nombre de destino simbólico utilizado por el TP
- Nombre del TP asociado
- Nombre o alias de la LU asociada
- Nombre de modalidad

Configuración de CPI-C

Para configurar información complementaria de CPI-C, siga estos pasos desde la ventana Nodo:

1. Seleccione **CPI-C** del submenú **APPC** del menú **Servicios**.
Communications Server para Linux muestra la ventana Nombres de destino CPI-C.
2. Pulse el botón **Nuevo**.
Communications Server para Linux muestra el diálogo Configuración de destino de CPI-C.
3. Especifique los valores adecuados en los campos del diálogo.
4. Pulse el botón **OK** para definir la información complementaria de CPI-C.

Configuración de LUA

La API de LUA puede utilizarse para aplicaciones que utilizan LU de tipo 0-3 para comunicarse con un sistema principal. (Para obtener información detallada acerca de la API LUA, consulte la publicación *IBM Communications Server for AIX or Linux LUA Programmer's Guide*.)

Antes de configurar LUA, lleve a cabo esta configuración:

1. Configure el nodo según se describe en "Configuración del nodo" en la página 80.
2. Configure la conectividad para el tráfico dependiente según se describe en "Configuración de la conectividad" en la página 82. (Si está utilizando una pasarela SNA en sentido ascendente o un DLUR, configure el enlace con el nodo en sentido ascendente en lugar de un enlace directo con el sistema principal.)

Para configurar LUA, necesita esta información:

- Nombre de LU o nombre de la agrupación de LU.
- Número de LU para cada LU. El número de LU debe coincidir con el número de LU configurado en el sistema principal.

Para configurar LUA, defina la LU utilizando este procedimiento:

1. Seleccione la estación de enlace para el sistema principal en el panel Conectividad de la ventana Nodo.
2. Pulse el botón **Nuevo**.
3. En el diálogo que aparece, seleccione **Nueva LU para LUA**.
4. Especifique los valores adecuados en los campos del diálogo. Especifique el tipo de LU Sin restringir.
5. Pulse el botón **OK**. La LU aparece en el panel Conectividad de la ventana Nodo, por debajo de la estación de enlace para el sistema principal.
6. Si va a utilizar agrupaciones de LU, defínalas tal como se describe en el apartado "Definición de una agrupación de LU".

Definición de una agrupación de LU

Puede definir las agrupaciones de LU para simplificar la configuración de usuario y proporcionar una mayor flexibilidad en el establecimiento de sesiones de sistema principal. Por ejemplo, puede definir varias LU en una sola agrupación de LU y después configurar múltiples aplicaciones LUA utilizando esta agrupación de LU. Esto facilita la configuración de aplicaciones y permite que cualquier aplicación utilice cualquier LU de la agrupación.

Nota: puede asignar la sesión de un usuario a una LU específica o a una agrupación de LU.

- Si asigna la sesión de usuario a una LU específica que se encuentra en una agrupación, la sesión utilizará esa LU si está disponible; de lo contrario, utilizará cualquier LU libre de la agrupación, como si la hubiera asignado a la agrupación de LU en vez de asignarla a una LU específica.
- Si desea que el usuario sólo utilice la LU especificada y que no pueda establecer la sesión de usuario si la LU ya se utiliza, asegúrese de que la LU no se encuentre en una agrupación.

Puede ver las agrupaciones de unidades LU para el nodo Communications Server para Linux local utilizando la ventana Agrupaciones de LU. Esta ventana muestra las agrupaciones de LU configuradas en el sistema local y le permite seleccionar las LU que desee añadir a una agrupación de LU.

Puede añadir los tipos de LU siguientes a una agrupación para que 3270 los utilice (no mezcle LU de distintos tipos en la misma agrupación):

- LU de pantalla 3270
- LU no restringida

Antes de añadir una o varias unidades LU a una agrupación, las LU deben estar definidas en el nodo local.

Para configurar una agrupación de LU, siga estos pasos desde la ventana Nodo:

1. Seleccione **Agrupaciones de LU** en el menú **Ventanas**.

Communications Server para Linux muestra la ventana Agrupaciones de LU.

2. Pulse el botón **Nuevo**.

Communications Server para Linux muestra el diálogo Configuración de una agrupación de LU.

El recuadro de la derecha muestra las LU que no se han asignado todavía a ninguna agrupación. Cualquiera de estas LU con el tipo LU sin restringir se puede incluir en la nueva agrupación para LUA.

3. Seleccione las LU que desea añadir a la agrupación y pulse el botón **Nuevo** para mover las LU seleccionadas al recuadro de la izquierda.

Para eliminar una LU del recuadro de la izquierda, selecciónela y pulse el botón **Eliminar**.

4. Pulse **OK** para definir la agrupación de LU.

Todas las LU del recuadro de la izquierda se añaden a la agrupación de LU.

La agrupación aparece en la ventana Agrupaciones de LU.

Configuración de la pasarela SNA

Además de proporcionar acceso directo a un sistema principal, Communications Server para AIX puede proporcionar recursos de pasarela SNA. Esta característica permite que otros sistemas accedan a un sistema principal a través de un nodo Communications Server para Linux en lugar de necesitar una conexión separada con el sistema principal desde cada sistema.

Configuración de la pasarela SNA

La característica de pasarela SNA se muestra en la Figura 8.

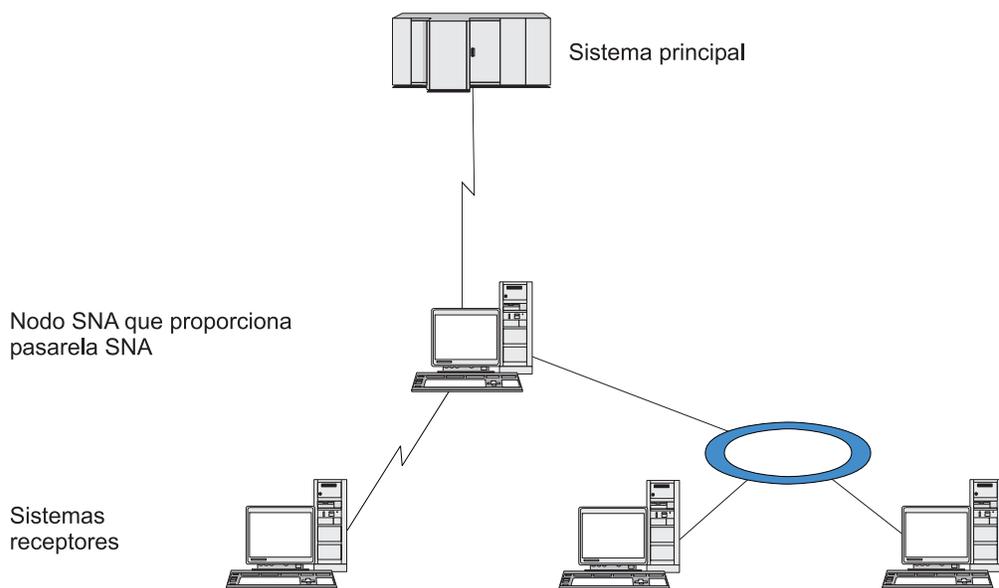


Figura 8. Pasarela SNA

El sistema en sentido descendente debe contener una PU SNA de tipo 2.0 ó 2.1 para soportar unidades LU dependientes. Por ejemplo, el sistema en sentido descendente podría ser otro sistema Communications Server para Linux o un PC que ejecute Communications Server para Windows.

Cuando el nodo Communications Server para Linux local utiliza la función de pasarela SNA, todos los datos transferidos entre el sistema principal y el sistema en sentido descendente se direccionan a través del nodo local. Esto permite a un sistema en sentido descendente compartir una conexión de sistema principal con Communications Server para Linux o con otros sistemas en sentido descendente, en lugar de necesitar un enlace directo. Por ejemplo, podría configurar varios sistemas en sentido descendente conectados a Communications Server para Linux a través de una red Token Ring local, de modo que todos ellos pudieran acceder a la misma línea dedicada de larga distancia desde Communications Server para Linux al sistema principal.

El uso de la pasarela SNA también simplifica la configuración en el sistema principal ya que no es necesario definir los sistemas en sentido descendente ni los enlaces de comunicaciones con esos sistemas. La configuración del sistema principal sólo debe incluir el sistema Communications Server para Linux y su enlace de comunicaciones con el sistema principal; las LU de los sistemas en sentido descendente se configuran como parte de los recursos del sistema Communications Server para Linux. El sistema principal no sabe que se está utilizando una pasarela SNA.

Antes de configurar la pasarela SNA, debe llevar a cabo las tareas de configuración siguientes:

- Defina el nodo local según se describe en “Configuración del nodo” en la página 80.
- Configure un puerto y una estación de enlace para el tráfico dependiente entre el nodo local y el sistema principal, como se describe en “Configuración de la conectividad” en la página 82. Asimismo, configure puertos y estaciones de

enlace para el tráfico dependiente entre el nodo local y los nodos en sentido descendente. Si necesita dar soporte a LU en sentido descendente que no están definidas previamente, puede definir una plantilla en el puerto para soportar PU implícitas y LU en sentido descendente (consulte “Soporte para LU implícitas en sentido descendente”).

- Defina las LU en el nodo local que se utilizan para la comunicación con el sistema principal (LU en sentido ascendente). Defina las LU en sentido ascendente como LU de tipo 0–3 con una LU de tipo *Sin restringir* (desconocido). (Las LU en nodos en sentido descendente pueden ser de cualquier tipo.)
- Si va a utilizar agrupaciones de LU, defínalas tal como se describe en el apartado “Definición de una agrupación de LU” en la página 86.

Soporte para LU implícitas en sentido descendente

Para dar soporte a las LU en sentido descendente que no se han predefinido en Communications Server para Linux, puede definir una plantilla en el puerto para PU y LU implícitas en sentido descendente (para la configuración básica de puertos, consulte el apartado “Configuración de la conectividad” en la página 82). Estas plantillas proporcionan soporte para LU en sentido descendente, de modo que no es necesario que configure una LU en el nodo local para soportar cada LU de un nodo en sentido descendente.

Antes de configurar una LU en sentido descendente para la pasarela SNA, necesita la información siguiente:

- Rango de números de LU para soportar LU en sentido descendente.
- Nombre de LU del sistema principal.

Para definir una plantilla para LU implícitas en sentido descendente, siga estos pasos:

1. Si ya ha configurado el puerto, pulse dos veces en la definición de puerto del panel Conectividad de la ventana Nodo. Communications Server para Linux muestra el diálogo Configuración de puerto.
Si no ha configurado el puerto, siga estos pasos:
 - a. Seleccione el panel Conectividad en la ventana Nodo.
 - b. Pulse el botón **Nuevo**.
 - c. En el diálogo que aparece, defina un puerto y seleccione el tipo de protocolo de enlace.
Communications Server para Linux muestra el diálogo Configuración de puerto.
 - d. Especifique los parámetros básicos de puerto según se describe en “Configuración de la conectividad” en la página 82.
2. Pulse el botón **Avanzado** en la parte inferior del diálogo.
Communications Server para Linux muestra el diálogo Parámetros de puerto. El panel inferior muestra valores que afectan a las plantillas de LU en sentido descendente.
3. Seleccione la opción *Configurar LU en sentido descendente para acceso de PU implícita*.
4. Pulse **OK**.
Communications Server para Linux muestra el diálogo Configuración de plantilla de LU en sentido descendente.
5. Especifique los valores adecuados en los campos del diálogo.

Configuración de la pasarela SNA

6. Pulse **OK** para definir la plantilla de LU implícita en sentido descendente.

Definición de LU en sentido descendente

Antes de configurar una LU en sentido descendente para la pasarela SNA, necesita la información siguiente:

- Nombre de LU para cada LU en sentido descendente. (Se trata de un identificador local y no tiene que coincidir con la configuración del sistema en sentido descendente.)
- Número de LU para cada LU en sentido descendente.
- Estación de enlace para el nodo en sentido descendente.
- Nombre de LU en sentido ascendente (para la LU del sistema principal).

Para configurar una LU en sentido descendente para la pasarela SNA, siga estos pasos:

1. Seleccione la estación de enlace para el nodo en sentido descendente en el panel Conectividad de la ventana Nodo.
2. Pulse el botón **Nuevo**.
3. Seleccione **Nueva LU en sentido descendente** y pulse **OK**.
Communications Server para Linux muestra el diálogo LU en sentido descendente.
4. Especifique los valores adecuados en los campos del diálogo.
5. Pulse **OK** para definir la LU en sentido descendente.

La definición de LU aparece en el panel Conectividad de la ventana Nodo, por debajo de la estación de enlace para el nodo en sentido descendente.

Configuración del DLUR

Además de proporcionar acceso directo a un sistema principal, Communications Server para Linux puede proporcionar recursos de peticionario de LU dependiente (DLUR). Esta característica permite que las sesiones para unidades LU dependientes abarquen varios nodos de una red APPN, en lugar de necesitar una conexión directa con el sistema principal.

Por regla general, una sesión de LU dependiente necesita un enlace de comunicaciones directo con el sistema principal. Si hay muchos nodos (incluido un nodo de sistema principal) conectados en una red APPN, puede que algunos no tengan conexión directa con el sistema principal, sino sólo una conexión indirecta a través de otro nodo. No es posible establecer sesiones de LU dependientes con el sistema principal desde las LU de estos nodos conectados indirectamente.

El peticionario de LU dependientes (DLUR) es una característica de APPN diseñada para superar esta limitación.

DLUR en un nodo APPN (por ejemplo, el nodo Communications Server para Linux) trabaja en combinación con el servidor de LU dependiente (DLUS) en el sistema principal para direccionar sesiones desde LU dependientes del nodo DLUR al sistema principal DLUS a través de la red APPN. La ruta hacia el sistema principal puede abarcar varios nodos y puede aprovechar las funciones de gestión de red, ubicación dinámica de recursos y cálculo de rutas de APPN. El DLUR debe estar disponible en el nodo donde se encuentran las LU, y el DLUS debe estar disponible en el nodo de sistema principal, pero el DLUR no es necesario en los nodos intermedios de la ruta de la sesión.

Si el nodo DLUR de Communications Server para Linux es un nodo de red o un nodo de red de ramificación, también puede proporcionar recursos DLUR de paso a través para unidades LU dependientes en sistemas en sentido descendente conectados al nodo Communications Server para Linux. Estas LU pueden utilizar DLUR en el nodo Communications Server para Linux para acceder al sistema principal a través de la red, de la misma manera que las LU internas acceden al nodo. Los sistemas en sentido descendente no ejecutan el DLUR y, en realidad, no necesitan saber que se está utilizando el DLUR.

La Figura 9 muestra un servidor Communications Server para Linux configurado como nodo de red APPN, que implementa DLUR de paso a través para dar soporte a sesiones entre las LU del sistema principal (nodo en sentido ascendente) y las LU de los nodos de la red APPN (los nodos en sentido descendente).

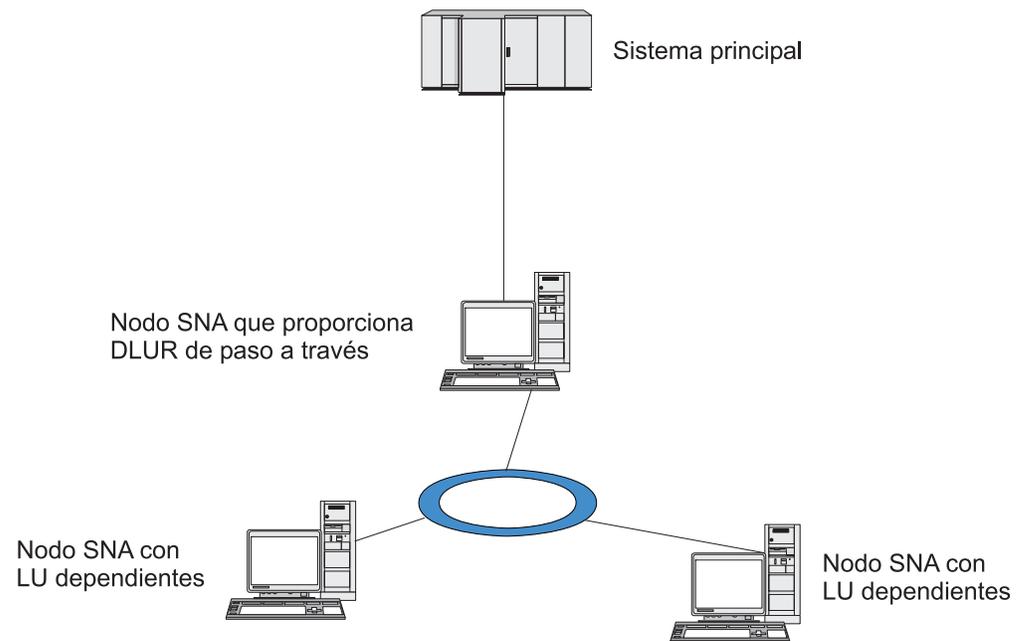


Figura 9. Nodo de Communications Server para Linux que proporciona DLUR

Nota:

1. No puede configurar el DLUR en un nodo LEN.
2. Sólo puede configurar el DLUR de paso a través en un nodo de red o en un nodo de red de ramificación.
3. Si está utilizando Branch Extender, no puede configurar el DLUR en un nodo final de la rama (con un nodo de red de ramificación como su servidor de nodos de red). Sin embargo, puede soportar aplicaciones de LU dependiente desde este nodo configurando el DLUR de paso a través en el nodo de red de ramificación (de modo que el nodo final de la rama no ejecute el DLUR, sino que utilice el DLUR de paso a través en el nodo de red de ramificación).

Las tareas que necesita realizar para configurar el DLUR dependen de si las LU dependientes están en el nodo local o en los nodos en sentido descendente.

Configuración de soporte para el DLUR en el nodo local

Para realizar esta tarea, necesita la información siguiente:

- ID de la PU del nodo local.
- Nombre de PU. (Se trata de un identificador local y no tiene que coincidir con la configuración del sistema principal.)
- Nombre de los DLUS del sistema principal (y el nombre del DLUS de reserva si existe uno).
- Nombre de LU, número de LU y tipo de LU de cada LU en sentido descendente. El número de LU debe coincidir con el número configurado en el sistema principal.

Para configurar el soporte para el DLUR en el nodo local, debe llevar a cabo las tareas de configuración siguientes:

1. Defina el nodo local según se describe en “Configuración del nodo” en la página 80. Si proporciona soporte para DLUR de paso a través para nodos en sentido descendente, defina el nodo como un nodo de red APPN o un nodo de red de ramificación.
2. Configure la conectividad con la red APPN. La conectividad APPN necesita al menos un puerto y una estación de enlace para el tráfico independiente entre el nodo local y el nodo de red APPN adyacente, como se describe en “Configuración de la conectividad” en la página 82.
3. Defina una PU DLUR en el nodo local (la PU DLUR da soporte para conectividad con el sistema principal).

Para configurar la PU DLUR, siga estos pasos desde la ventana Nodo:

- a. Seleccione el menú **Servicios**, el submenú **Conectividad** y a continuación, **Nueva PU DLUR** (o pulse el botón **Nuevo** de la barra de botones y, a continuación, seleccione **PU DLUR**).

Al pulsar en el botón **OK**, Communications Server para Linux muestra el diálogo Configuración de PU DLUR.

- b. Especifique los valores adecuados en los campos del diálogo.
- c. Pulse el botón **OK** para definir la PU DLUR.

La PU DLUR aparece en el panel Conectividad, bajo el elemento DLUR.

4. Para configurar DLUR a fin de que dé soporte a las LU en el nodo local, debe añadir las LU al nodo local. Las LU deben estar configuradas para dar soporte a LUA, tal como se describe en el apartado “Configuración de LUA” en la página 94. Según los requisitos de las aplicaciones de usuario soportadas por las LU, es posible que deba realizar alguna configuración adicional.

Configuración de soporte para el DLUR de paso a través para nodos en sentido descendente

Para realizar esta tarea, necesita la información siguiente:

- Nombre de PU en sentido descendente para cada nodo en sentido descendente o para cada PU del nodo en sentido descendente. (Se trata de un identificador local y no tiene que coincidir con la configuración del sistema principal.)
- Nombre del DLUS del sistema principal.

Para configurar el soporte para el DLUR de paso a través para nodos en sentido descendente, debe llevar a cabo las tareas de configuración siguientes:

1. Defina el nodo local como un nodo de red APPN (consulte “Configuración del nodo” en la página 80).

2. Configure la conectividad con los nodos en sentido descendente. Configure puertos y estaciones de enlace para el tráfico dependiente entre el nodo local y cada nodo en sentido descendente, como se describe en “Configuración de la conectividad” en la página 82. (No es necesario definir una PU DLUR para dar soporte al DLUR de paso a través para nodos en sentido descendente.)
3. Un nodo en sentido descendente puede soportar varias PU. En este caso, cada PU en sentido descendente se asocia a un enlace diferente, por lo que deberá configurar varios enlaces entre el nodo DLUR de Communications Server para Linux y el nodo en sentido descendente y deberá conocer el nombre de PU en sentido descendente de cada enlace.

Configuración del servidor TN

Los programas de emulación 3270 que se comunican por TCP/IP (en lugar de una red SNA) se conocen como programas TN3270 (programas de emulación Telnet 3270).

Los programas TN3270 también pueden incluir soporte para TN3270E (extensiones estándar de Telnet 3270). TN3270E es un protocolo abierto que soporta la emulación de dispositivos 3270 (terminales e impresoras) mediante Telnet. Permite que un cliente Telnet seleccione un dispositivo determinado (especificando el nombre de LU), y proporciona soporte ampliado para varias funciones, incluidas las teclas ATTN y SYSREQ y el manejo de respuestas SNA.

Nota: en esta publicación se utiliza el término TN3270 para la información que es válida para los protocolos TN3270, TN3287 y TN3270E.

El servidor TN de Communications Server para Linux proporciona acceso a sistemas principales 3270 para usuarios TN3270 en otros sistemas. El servidor TN permite a los usuarios TN3270 compartir una conexión de sistema principal con usuarios Communications Server para Linux o con otros usuarios TN3270, en lugar de requerir un enlace directo. Además, el servidor TN permite a los usuarios TN3270 acceder a sistemas principales que no ejecutan TCP/IP.

Configuración del servidor TN

En la Figura 10 se muestra un nodo Communications Server para Linux que proporciona soporte de servidor TN para clientes TN3270. El nodo de servidor TN y los clientes se comunican a través de la red TCP/IP.

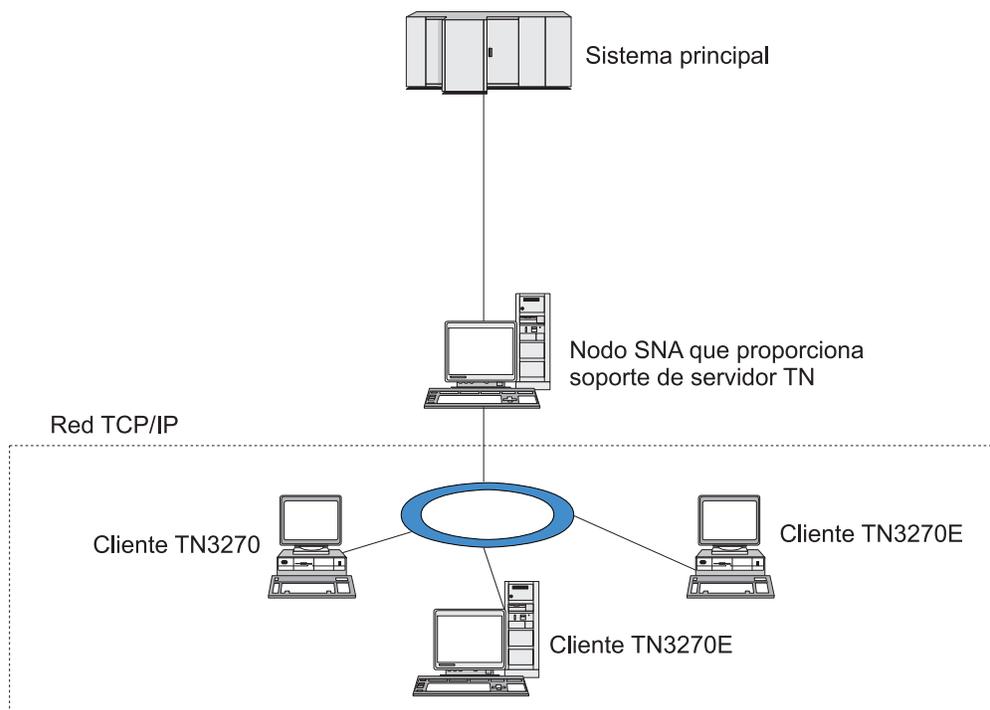


Figura 10. Nodo de Communications Server para Linux configurado para el servidor TN

La función de servidor TN de Communications Server para Linux proporciona una asociación entre un usuario TN3270 y una LU 3270 de Communications Server para Linux. Todos los datos del usuario TN3270 se dirigen a la LU. Esto significa que el sistema principal y el usuario TN3270 están configurados como si estuvieran conectados directamente; ninguno de ellos precisa saber que los datos se dirigen a través del servidor TN.

El servidor TN de Communications Server para Linux TN da soporte a todos los programas de emulación de cliente TN3270 que implementan correctamente los protocolos definidos en los REC de la IETF 1123, 1576, 1646, 1647 y 2355.

Cuando un programa TN3270 se comunica con el servidor TN, Communications Server para Linux identifica el programa por la dirección TCP/IP del sistema en el que se ejecuta el programa TN3270. Communications Server para Linux no puede distinguir entre dos programas TN3270 diferentes utilizados por usuarios diferentes en un mismo sistema. En los manuales de Communications Server para Linux, el término usuario de servidor TN hace referencia al sistema en el que se ejecuta el programa TN3270, no al usuario de ese programa.

Tal como muestra la Figura 11, el sistema principal y el usuario del servidor TN ven la configuración del servidor TN de forma diferente.

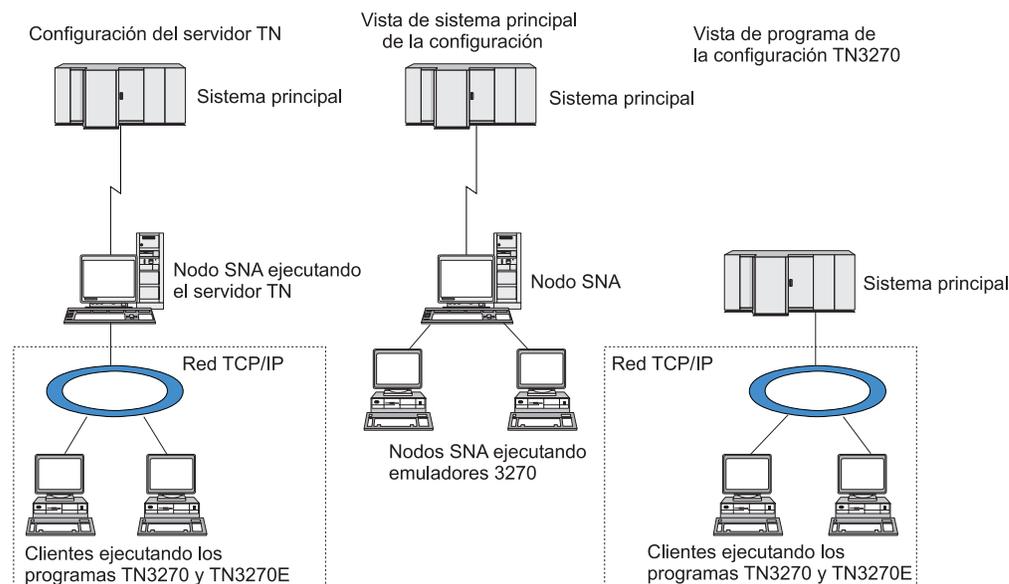


Figura 11. Servidor TN

Cada usuario del servidor TN que se conecta a Communications Server para Linux utilizando la característica del servidor TN3270 se suele configurar para que acceda a una sola LU 3270 y por tanto está restringido a una sola sesión de sistema principal cada vez. Pero también puede configurar un usuario del servidor TN para acceder a una agrupación de unidades LU 3270, en lugar de tener una sola LU 3270 dedicada para cada usuario. Esto permite que los usuarios puedan acceder a tantas sesiones como unidades LU disponibles existan en la agrupación.

Antes de configurar el acceso de servidor TN, debe llevar a cabo las tareas de configuración siguientes:

- Defina el nodo local según se describe en “Configuración del nodo” en la página 80.
- Configure un puerto y una estación de enlace para el tráfico dependiente entre el nodo local y el sistema principal, como se describe en “Configuración de la conectividad” en la página 82.

Para configurar el acceso de servidor TN, debe realizar las tareas de configuración siguientes:

- Defina las LU 3270 en el nodo local que se utilizan para la comunicación con el sistema principal. Para añadir las LU, consulte el apartado “Definición de LU 3270”.
- Si va a utilizar agrupaciones de LU, defínalas tal como se describe en el apartado “Definición de una agrupación de LU” en la página 104.

Definición de LU 3270

Antes de configurar la LU 3270, recopile la información siguiente:

- Nombre de LU (Se trata de un identificador local y no tiene que coincidir con la configuración del sistema principal.)
- Número de LU (o números para un rango de LU)

Configuración del servidor TN

- Tipo de LU (modelo de pantalla 3270 o impresora 3270)
- Nombre de agrupación (si añade la LU a una agrupación)

Para configurar una LU de los tipos 0–3 para una estación de enlace previamente definida, siga estos pasos desde la ventana Nodo:

1. Seleccione la estación de enlace para el sistema principal en el panel Conectividad de la ventana.
2. Pulse el botón **Nuevo**.
3. Seleccione el tipo de LU (**Nueva LU de pantalla 3270** o **Nueva LU de impresora 3270**) en el diálogo que aparece.
Cuando selecciona este elemento y pulsa **OK**, Communications Server para Linux muestra el diálogo LU de tipo 0–3.
4. Especifique los valores adecuados en los campos del diálogo.
5. Pulse **OK** para definir la LU.

La LU aparece en el panel Conectividad de la ventana Nodo, por debajo de la estación de enlace para el sistema principal.

Definición de una agrupación de LU

Para 3270, puede definir agrupaciones de LU para simplificar la configuración de usuario y proporcionar una mayor flexibilidad al establecer sesiones de sistema principal. Por ejemplo, puede definir varias LU 3270 en una sola agrupación de LU y después configurar múltiples clientes TN3270 utilizando esta agrupación de LU. Esto facilita la configuración de las sesiones 3270 y permite a cualquier cliente utilizar cualquier LU de la agrupación.

Nota: puede asignar un cliente TN3270 a una LU o agrupación de LU específica.

- Si asigna el cliente a una LU específica que se encuentra en una agrupación, el cliente utilizará esa LU si está disponible; de lo contrario, utilizará cualquier LU libre de la agrupación, como si lo hubiera asignado a la agrupación de LU en lugar de asignarlo a la LU específica.
- Si desea que el cliente sólo utilice una LU especificada, de modo que la sesión del cliente no se pueda establecer si la LU ya se utiliza, asegúrese de que la LU no se encuentre en una agrupación.

Puede ver las agrupaciones de unidades LU para el nodo Communications Server para Linux local utilizando la ventana Agrupaciones de LU. Esta ventana muestra las agrupaciones de LU configuradas en el sistema local y le permite seleccionar las LU que desee añadir a una agrupación de LU.

Puede añadir los tipos de LU siguientes a una agrupación para que 3270 los utilice (no mezcle LU de distintos tipos en la misma agrupación):

- LU de pantalla 3270
- LU no restringida

Antes de añadir una o varias unidades LU a una agrupación, las LU deben estar definidas en el nodo local.

Para configurar una agrupación de LU, siga estos pasos desde la ventana Nodo:

1. Seleccione **Agrupaciones de LU** en el menú **Ventanas**.
Communications Server para Linux muestra la ventana Agrupaciones de LU.
2. Pulse el botón **Nuevo**.

Communications Server para Linux muestra el diálogo Configuración de una agrupación de LU.

El recuadro de la derecha muestra las LU que no se han asignado todavía a ninguna agrupación. Cualquiera de ellas pueden incluirse en la nueva agrupación.

3. Seleccione las LU que desea añadir a la agrupación y pulse el botón **Nuevo** para mover las LU seleccionadas al recuadro de la izquierda.

Para eliminar una LU del recuadro de la izquierda, selecciónela y pulse el botón **Eliminar**.

4. Pulse **OK** para definir la agrupación de LU.

Todas las LU del recuadro de la izquierda se añaden a la agrupación de LU.

La agrupación aparece en la ventana Agrupaciones de LU.

Configuración del servidor TN3270

Antes de configurar un servidor TN3270, necesita conocer la información siguiente:

- Si el servidor soporta sólo TN3270 o también TN3270E (que incluye soporte TN3270).
- Si un cliente TN3270E puede solicitar una LU determinada.
- Nombres de LU de pantalla e impresora (o nombres de agrupaciones de LU) de cada cliente. (Los nombres de LU de impresora sólo se necesitan si se da soporte a TN3270E.)
- Si sólo se permiten determinados clientes o si desea restringir determinados clientes para LU específicas, necesita el nombre o dirección TCP/IP del cliente.
- Número de puerto TCP/IP del nodo de servidor TN.
- Si es necesario el cifrado de datos SSL, la autenticación de cliente y la autenticación de servidor (esta opción está disponible sólo si ha instalado el software adicional necesario para soportarla).

Para asociar una LU de pantalla y una LU de impresora, necesita también los nombres de esas LU. Un registro de asociación de servidor TN define una asociación entre una LU de impresora y una LU de pantalla, de modo que el protocolo TN3270E puede conectar las dos. No es necesario que defina un registro de asociación si no da soporte a TN3270E o si no da soporte a LU de impresoras.

El registro por omisión de servidor TN define parámetros que se utilizan en todas las sesiones de cliente TN3270. Puede definir un único registro por omisión para cada servidor.

Para configurar el servidor TN3270, siga estos pasos desde la ventana Nodo:

1. Defina un registro de acceso de servidor TN:

- a. Seleccione **Servidor TN** en el menú **Servicios**.

Communications Server para Linux muestra la ventana Servidor TN, que lista todos los registros de acceso de servidor TN configurados en el panel superior y los registros de asociación de servidor TN en el panel inferior.

- b. Seleccione el panel que contiene registros de acceso de servidor TN3270 y pulse el botón **Nuevo**.

Communications Server para Linux muestra el diálogo Acceso de servidor TN.

- c. Especifique los valores adecuados en los campos del diálogo.

- d. Pulse **OK** para definir el registro de acceso de servidor TN. El registro aparece en la ventana Servidor TN.

Configuración del servidor TN

2. Defina un registro de asociación de servidor TN:
 - a. Seleccione el panel que contiene registros de asociación en la ventana Servidor TN y pulse el botón **Nuevo**.
Communications Server para Linux muestra el diálogo Registro de asociación de servidor TN.
 - b. Especifique los valores adecuados en los campos del diálogo.
 - c. Pulse **OK** para definir el registro de asociación de servidor TN. El registro aparece en la ventana Servidor TN.
3. Si necesita forzar respuestas de impresora, especificar un método de keep-alive para todas las sesiones TN3270, especificar el acceso al servidor LDAP externo que contiene una lista de revocaciones utilizada para comprobar la autorización para clientes TN3270 o utilizar SLP (Service Location Protocol) TN3270, utilice el diálogo de parámetros avanzados del servidor TN para hacerlo.

Para obtener más información acerca de la configuración del soporte SSL para el servidor TN, consulte las páginas Web de IBM Communications Server Support en <http://www.ibm.com/software/network/commserver/support/>.

Configuración del redirector TN

La función del redirector TN de Communications Server para Linux proporciona acceso al sistema principal TCP/IP de paso a través para los clientes TN3270, TN3270E, TN5250 y VT, denominados colectivamente clientes Telnet. El usuario Telnet se comunica con Communications Server para Linux a través de una conexión TCP/IP; Communications Server para Linux se comunica entonces con el sistema principal a través de otra conexión TCP/IP. Esto permite utilizar la comprobación de seguridad de SSL (Secure Sockets Layer) donde sea necesario, y no en la conexión completa entre usuario y sistema principal. Por ejemplo:

- Si los clientes se conectan a Communications Server para Linux a través de una LAN TCP/IP en la que no se requiera ninguna comprobación, pero se conectan a un sistema principal remoto que requiere SSL, puede utilizar SSL en la conexión TCP/IP entre Communications Server para Linux y el sistema principal. Esto significa que la seguridad se comprueba una sola vez para todos los clientes y que los clientes individuales no tienen que proporcionar información de seguridad.
- Si Communications Server para Linux está instalado en la misma ubicación que el sistema principal, pero los clientes se conectan desde ubicaciones externas, puede utilizar SSL en las conexiones del cliente con Communications Server para Linux sin tener que instalar el software SSL en el sistema principal.

Configuración del redirector TN

Antes de configurar el acceso al redirector TN, debe definir el nodo local tal como se describe en "Configuración del nodo" en la página 80. También necesitará la siguiente información:

- Si sólo se permiten determinados clientes, necesita el nombre o dirección TCP/IP del cliente.
- Número de puerto TCP/IP utilizado por el cliente para conectarse al nodo del redirector TN.
- Nombre o dirección TCP/IP del sistema principal.
- Número de puerto TCP/IP utilizado por el nodo del redirector TN para conectarse al sistema principal.

- Si se requiere el cifrado de datos SSL, la autenticación de cliente y la autenticación de servidor entre el cliente y el nodo del redirector TN (esta opción está disponible sólo si ha instalado el software adicional necesario para soportarla).
- Si se requiere el cifrado de datos SSL entre el nodo del redirector TN y el sistema principal.

El registro por omisión del servidor TN define parámetros que se utilizan en todas las sesiones de cliente de redirector TN. Puede definir un único registro por omisión para el número de puerto TCP/IP de cada cliente.

Para configurar el redirector TN, siga estos pasos desde la ventana Nodo para definir un registro de acceso de redirector TN:

1. Seleccione **Servidor TN** en el menú **Servicios**.

Communications Server para Linux muestra la ventana Servidor TN, que lista todos los registros de acceso de servidor TN3270, configurados, los registros de asociación de servidor TN3270 y los registros de acceso de redirector TN.

2. Seleccione el panel que contiene registros de acceso de redirector TN y pulse el botón **Nuevo**.

Communications Server para Linux muestra el diálogo Acceso de redirector TN.

3. Especifique los valores adecuados en los campos del diálogo.
4. Pulse **OK** para definir el registro de acceso de redirector TN. El registro aparece en el panel Redirector TN de la ventana Servidor TN.

Nota: el nodo SNA debe estar activo para utilizar el redirector TN, aunque no utilice ninguno de los recursos SNA del nodo.

Inhabilitación de Communications Server para Linux

Al inhabilitar el software de Communications Server para Linux, el nodo Communications Server para Linux y los componentes de conectividad asociados al mismo se detienen de forma automática. La inhabilitación de Communications Server para Linux impide también que cualquier otro proceso (por ejemplo, una aplicación LUA) utilice los recursos de Communications Server para Linux de este servidor.

En general, debe detener los servicios individuales a medida que los usuarios terminen de utilizarlos e inhabilitar el sistema solamente cuando no haya ninguna actividad de Communications Server para Linux.

Si necesita inhabilitar Communications Server para Linux mientras hay usuarios activos, comunique a los usuarios que se va a detener Communications Server para Linux y déles tiempo para terminar las actividades antes de inhabilitar el software.

Cuando se inhabilita el software de Communications Server para Linux, a las aplicaciones que utilizan las API APPC, CSV, LUA, NOF o MS se les comunica el código de retorno COMM_SUBSYSTEM_ABENDED y las aplicaciones CPI-C reciben el código de retorno CM_PRODUCT_SPECIFIC_ERROR.

Para inhabilitar el software Communications Server para Linux, indique el siguiente mandato en la solicitud de mandatos de Linux:

```
sna stop
```

Inhabilitación de Communications Server para Linux

Si Communications Server para Linux se inhabilita correctamente, **sna stop** devuelve el código de salida 0. Cualquier otro código de salida indica que se ha producido un error y que el software de Communications Server para Linux no se ha inhabilitado. Consulte la publicación *IBM Communications Server para Linux, Guía de diagnósticos* para obtener más información sobre los valores de códigos de salida.

Inicio automático de Communications Server para Linux

Activación de Communications Server para Linux hasta que su estado sea de pleno funcionamiento consta de varios pasos:

- Habilitación del software de Communications Server para Linux
- Inicialización del nodo SNA
- Activación de los puertos y estaciones de enlace configurados en el nodo.

Cada uno de estos pasos pueden gestionarse por separado y pueden realizarse todos los pasos durante el arranque, si es necesario. El resto de este apartado describe estos pasos y explica cómo controlarlos durante el arranque.

Habilitación de Communications Server para Linux

Communications Server para Linux requiere la carga de varios módulos de kernel para poder funcionar. Estos módulos se cargan al habilitar el software de Communications Server para Linux por primera vez y sólo se descargan cuando se cambia el nivel de ejecución del kernel.

Communications Server para Linux también requiere que una serie de daemons (programas) estén en ejecución. Hasta que estos daemons no estén en ejecución, no puede configurar ni utilizar Communications Server para Linux.

- Para iniciar los daemons y habilitar el software de Communications Server para Linux, emita el mandato **sna start**.
- Para detener los daemons e inhabilitar el software de Communications Server para Linux, emita el mandato **sna stop**.

Inicialización del nodo SNA

Cuando Communications Server para el software de Linux se puede configurar el nodo SNA y sus recursos, normalmente utilizando el programa de administración de Motif `xsnaadmin`. Sin embargo, el nodo no está disponible para su utilización hasta que se inicializa. Puede inicializarlo desde el programa de administración de la línea de mandatos, con el mandato **snaadmin init_node** o desde el programa de administración de Motif `xsnaadmin`.

Activación de puertos y estaciones de enlace

Los puertos y estaciones de enlace se pueden configurar para que se inicien bajo circunstancias diferentes:

- Sólo por la intervención del operador
- Bajo demanda (cuando se inicia una aplicación que utiliza un recurso del enlace)
- Al arrancar el nodo (cuando se emite el mandato **snaadmin init_node** o cuando se inicia el nodo desde el programa de administración de Motif)

El inicio por el operador es el valor por omisión, pero puede cambiarlo por un puerto o un enlace en particular utilizando el programa de administración de la línea de mandatos o el programa de administración de Motif.

Nota: el inicio de un puerto habilita ese puerto para recibir llamadas de otros sistemas, pero no le permite realizar llamadas de salida. El inicio de una estación de enlace significa que Communications Server para Linux intenta ponerse en contacto con el sistema remoto.

Inicio de Communications Server para Linux durante el arranque

Al igual que sucede con otros servicios de Linux, Communications Server para Linux está habilitado para su inicio durante el arranque. Es decir, después de un rearranque se emite por omisión el mandato **sna start** pero no se inicia el nodo SNA.

Esta inicialización se realiza en el script de inicialización para el arranque de Communications Server para Linux, **/etc/rc.d/init.d/snastart**. Tal como es normal para los scripts de arranque, se enlaza con **/etc/rc?.d/init.d/snastart** para los distintos niveles de arranque.

Puede editar **/etc/rc.d/init.d/snastart** para cambiar lo que ocurre en el rearranque. El cambio más normal es añadir la inicialización del nodo. El mandato para ello, **snaadmin init_node**, ya se incluye en el archivo pero como comentario, sólo debe cambiar su condición de comentario. Al incluir este mandato, también inicia la activación de los puertos o las estaciones de enlace que se han configurado para activarse en el arranque del nodo.

Las aplicaciones que utilizan Communications Server para Linux no se deben iniciar hasta después de inicializar el nodo. Si es necesario, puede iniciar estas aplicaciones automáticamente durante el arranque, y añadir otros mandatos **snaadmin** que deba ejecutar durante el arranque, de dos maneras:

- Añada los mandatos al final de **/etc/rc.d/init.d/snastart**, después del mandato **snaadmin init_node**.
- Cree un script **/etc/rc?.d/init.d** con un número mayor que 95, lo que garantiza que se ejecutará después de iniciar Communications Server para Linux y añada los mandatos a ese script.

Nota: Los cambios que realice en el archivo **/etc/rc.d/init.d/snastart** no se guardarán cuando actualice Communications Server para Linux a una versión posterior. Asegúrese siempre de conservar una copia de los cambios, para que pueda volver a aplicarlos después de una actualización.

Capítulo 9. Recursos de información sobre Communications Server para Linux y SNA

Este capítulo describe los recursos de la biblioteca SNA que ofrecen información acerca de la tecnología SNA y los distintos productos de red y los servicios que Linux ofrece. También se indica la información que se encuentra disponible en foros de red.

Biblioteca de SNA

La biblioteca de SNA contiene folletos de marketing, manuales, guías del usuario y guías de aprendizaje que proporcionan información introductoria y detallada sobre los temas siguientes:

- Teoría acerca de SNA
- Productos SNA
- Implementación del producto
- Configuración de sistemas y redes
- Interfaces API y programas de aplicación SNA
- Planificación, rendimiento y ajuste globales
- Diagnóstico de problemas
- Gestión de redes
- Seguridad de redes

Todas las publicaciones de IBM pueden solicitarse al representante IBM, a la sucursal de IBM de su zona o llamando directamente a IBM, en el número 1-800-879-2755 (sólo en Estados Unidos).

Para obtener una lista de las publicaciones más importantes que existen de Communications Server para Linux, consulte la bibliografía al final de este manual.

Para obtener información acerca de publicaciones adicionales, póngase en contacto con el representante de IBM.

Información accesible en red

Para promocionar el intercambio de información, IBM patrocina foros y tablones de anuncios electrónicos. Publica páginas de presentación en Internet y proporciona documentación en línea a la que también se puede acceder en la World Wide Web.

Soporte de productos en IBMLink

El foro IBMLink tiene lugar en redes de propiedad de IBM. Está diseñado para ayudar a los clientes que disponen de productos IBM con licencia en la resolución de problemas técnicos y otros problemas relacionados con su sistema y red. El personal de IBM responde a las preguntas y mantiene debates en línea con los clientes de IBM.

Para obtener más información acerca de IBMLink, utilice <http://www.ibm.link.ibm.com>.

Información en páginas de presentación de IBM

En Internet existen diversas páginas de presentación de IBM que proporcionan acceso a foros. Para obtener ayuda global, se puede utilizar

Información accesible en red

la página de presentación principal de IBM para navegar hasta los centros de información en Internet y la World Wide Web. Puede acceder a la página de presentación principal utilizando <http://www.ibm.com>.

Puede acceder a información acerca del software de red de IBM, incluido Communications Server para IBM, emitiendo <http://www.ibm.com/software/network>. En la dirección <http://www.ibm.com/software/network/commsserver> encontrará información acerca de Communications Server para Linux.

Para obtener información más detallada acerca del soporte de Communications Server para Linux, utilice <http://www.ibm.com/software/network/commsserver/support>.

Información para realizar descargas desde Internet

En la World Wide Web, los usuarios pueden descargar publicaciones Redbook desde <http://www.redbooks.ibm.com>.

En la dirección <http://www.ibm.com/software> puede acceder a información sobre software de IBM, donde puede enlazar con páginas sobre Communications Server para Linux y todos los servidores de software de IBM.

Lectura recomendada

Para los usuarios que deseen profundizar sobre SNA, los manuales siguientes tratan sobre conceptos teóricos de SNA y el uso práctico de Communications Server para Linux. Estos manuales son útiles tanto para usuarios noveles como para usuarios expertos que necesitan un punto de partida para adentrarse en el conocimiento de SNA o un tratamiento en profundidad del tema.

- *Systems Network Architecture: Technical Overview* (GC30–3073)
- *IBM Communications Server para Linux, Guía de administración*

Si está interesado en cuestiones más específicas, consulte la bibliografía para obtener otras referencias o póngase en contacto con el representante local de IBM.

Apéndice. Avisos

La presente información se ha desarrollado para productos y servicios ofrecidos por EE.UU. Es posible que IBM no ofrezca en otros países los productos, servicios o funciones descritos en este documento. Consulte el representante local de IBM para obtener información sobre los productos y servicios que se pueden adquirir actualmente en su zona. Cualquier referencia a un producto, programa o servicio de IBM no pretende afirmar o implicar que pueda utilizarse sólo ese producto, programa o servicio. En su lugar puede utilizarse cualquier producto, programa o servicio funcionalmente equivalente que no vulnere ningún derecho de propiedad intelectual de IBM. Sin embargo, corresponde al usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patente en tramitación que abarquen temas descritos en el presente documento. El suministro de este documento no le otorga ninguna licencia sobre esas patentes. Puede enviar solicitudes de información sobre licencias, por escrito, a esta dirección:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
EE.UU.

Para cualquier consulta sobre licencias relacionada con la información sobre DBCS (juego de caracteres de doble byte), póngase en contacto con el departamento de propiedad intelectual de IBM de su país o envíe su consulta por escrito a la siguiente dirección:

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

El párrafo siguiente no es aplicable al Reino Unido ni a ningún otro país en el que estas disposiciones sean contrarias a la legislación del país:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍA DE NINGÚN TIPO, NI EXPLÍCITA NI IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERACIÓN DE DERECHOS, COMERCIALIZACIÓN O ADECUACIÓN PARA UN FIN DETERMINADO. Algunos estados no permiten la renuncia de garantías expresas ni implícitas en determinadas transacciones, por lo que esta declaración puede no ser aplicable a su caso.

La presente información puede contener inexactitudes técnicas o errores tipográficos. Periódicamente se realizan cambios en la información aquí contenida; estos cambios se incorporarán a las nuevas ediciones de la publicación. IBM puede realizar mejoras y cambios en los productos y programas descritos en esta publicación en todo momento sin previo aviso.

Cualquier referencia en esta publicación a sitios Web no pertenecientes a IBM se proporciona solamente para la comodidad del usuario, y en ninguna manera

constituye un aval de esos sitios Web. Los materiales de estos sitios Web no forman parte de este producto IBM y el riesgo de utilizar estos sitios Web lo asume el usuario.

IBM puede utilizar o distribuir cualquier información que el usuario le proporcione de la manera que IBM considere apropiada, sin contraer ninguna obligación con el usuario.

Los licenciatarios de este programa que deseen tener información sobre él con el fin de permitir: (i) el intercambio de información entre programas creados independientemente y otros programas (incluido el presente programa) y (ii) el uso recíproco de la información que se ha intercambiado, deben ponerse en contacto con:

IBM Corporation
P.O. Box 12195
3039 Cornwallis Road
Research Triangle Park, NC 27709-2195
EE.UU.

Dicha información puede estar disponible, sujeta a los términos y condiciones apropiados, incluido en algunos casos, el pago de una tarifa.

IBM ofrece el programa bajo licencia que se describe en esta información y todo el material bajo licencia disponible para él, conforme a los términos del contrato de cliente de IBM, el acuerdo internacional de licencia de programas de IBM o cualquier acuerdo equivalente entre las partes.

Los datos de rendimiento contenidos en este manual se determinaron en un entorno controlado. Por tanto, los resultados obtenidos en otros entornos operativos pueden variar significativamente. Algunas mediciones se pueden haber realizado en sistema a nivel de desarrollo y no es seguro que estas mediciones serán las mismas en los sistemas disponibles normalmente. Además, algunas mediciones se pueden haber calculado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deben verificar los datos aplicables para su entorno específico.

La información referente a productos que no son de IBM se ha obtenido de los proveedores de esos productos, de sus anuncios publicados o de otras fuentes disponibles públicamente. IBM no ha probado estos productos y no puede confirmar la precisión del rendimiento, la compatibilidad ni otras cuestiones relacionadas con productos que no son de IBM. Las preguntas sobre las posibilidades de los productos que no son de IBM deben dirigirse a los proveedores de esos productos.

Esta información contiene ejemplos de datos e informes utilizados en las operaciones comerciales diarias. Para ilustrarlas lo máximo posible, los ejemplos incluyen nombres de personas, compañías, marcas y productos. Todos esos nombres son ficticios y cualquier parecido con nombres y direcciones de una empresa comercial real es mera coincidencia.

LICENCIA DE COPYRIGHT: Esta información contiene programas de aplicación de ejemplo en lenguaje fuente, que muestran técnicas de programación en varias plataformas operativas. Puede copiar, modificar y distribuir estos ejemplos de programas según desee, sin efectuar ningún pago a IBM, con la finalidad de desarrollar, utilizar, comercializar o distribuir programas de aplicación conformes a la interfaz de programas de aplicación de la plataforma operativa para la cual se

escribieron los programas. Estos programas de ejemplo no se han probado exhaustivamente bajo todas las condiciones. Por lo tanto, IBM no puede garantizar ni afirmar la fiabilidad, servicio o función de estos programas. El usuario puede copiar, modificar y distribuir estos programas de ejemplo en cualquier forma, sin pago alguno a IBM, con el fin de desarrollar, utilizar, comercializar o distribuir programas de aplicación que se ajusten a las interfaces de programación de aplicaciones de IBM.

Cada copia o cualquier porción de estos programas de ejemplo o cualquier trabajo derivado debe incluir una nota de copyright, de la manera siguiente: ® (nombre de su empresa) (año). Fragmentos de este código se derivan de ejemplos de programas de IBM Corp. ® Copyright IBM Corp. 2000, 2005, 2006, 2007, 2008, 2009. Reservados todos los derechos. .

Marcas registradas

IBM, el logotipo de IBM e ibm.com son marcas registradas de International Business Machines Corp., registradas en muchos países. Otros nombres de productos y servicios pueden ser marcas registradas de IBM o de terceros. Puede encontrar una lista actualizada de marcas registradas de IBM en la sección "Copyright and trademark information" de la Web www.ibm.com/legal/copytrade.shtml.

Adobe es una marca registrada de Adobe Systems Incorporated en Estados Unidos y/o en otros países.

Intel y Pentium son marcas registradas de Intel Corporation o sus subsidiarias en Estados Unidos y otros países.

Java y todas las marcas registradas y logotipos basados en Java son marcas registradas de Sun Microsystems, Inc. en Estados Unidos y/o en otros países.

Linux es una marca registrada de Linus Torvalds en los Estados Unidos y/o en otros países.

Microsoft y Windows son marcas registradas de Microsoft Corporation en los Estados Unidos y/o en otros países.

UNIX es una marca registrada de The Open Group en los Estados Unidos y/o en otros países.

Otras empresas, productos o nombres de servicios pueden ser marcas registradas de terceros.

Bibliografía

Las siguientes publicaciones de IBM ofrecen información acerca de los temas descritos en esta biblioteca. Las publicaciones se dividen en las siguientes grandes áreas temáticas:

- Communications Server para Linux, versión 6.4
- SNA (Arquitectura de red de sistemas)
- Configuración del sistema principal
- z/OS Communications Server
- Transmission Control Protocol/Internet Protocol (TCP/IP)
- X.25
- APPC (Comunicación avanzada programa a programa)
- Programación
- Otros temas de redes de IBM

Se proporcionan descripciones breves sobre los manuales de la biblioteca de Communications Server para Linux. Para otros manuales, sólo se muestra el número de pedido.

Publicaciones de Communications Server para Linux versión 6.4

La biblioteca de Communications Server para Linux comprende los siguientes manuales. Además, se proporcionan versiones en copia software de estos documentos en el CD-ROM. Para obtener más información sobre cómo acceder a los archivos de copia de software contenidos en el CD-ROM, consulte *IBM Communications Server para Linux, Guía de iniciación rápida*. Para instalar en el sistema estos manuales en copia software, necesitará de 9 a 15 MB de espacio de disco duro (según la versión de idioma que instale).

- *IBM Communications Server para Linux, Guía de iniciación rápida* (GC10-9852 y GC10-9856)

Este manual es una introducción general a Communications Server para Linux, que incluye información sobre las características de red soportadas, la instalación, la configuración y el funcionamiento. Existen dos versiones de este manual:

GC10-9852 es para Communications Server para Linux en las plataformas i686, x86_64 y ppc64.

GC10-9856 es para Communications Server para Linux en System z.

- *IBM Communications Server para Linux, Guía de administración* (SC10-9853)
Este manual proporciona una visión general de SNA y Communications Server para Linux e información sobre la configuración y el funcionamiento de Communications Server para Linux.
- *IBM Communications Server for Linux Administration Command Reference* (SC31-6770)
Este manual proporciona información sobre los mandatos de SNA y Communications Server para Linux.
- *IBM Communications Server for AIX or Linux CPI-C Programmer's Guide* (SC23-8691)

Este manual ofrece información para programadores expertos en “C” o Java sobre cómo escribir programas de transacciones SNA utilizando la API de comunicaciones de CPI de Communications Server para Linux.

- *IBM Communications Server for AIX or Linux APPC Programmer’s Guide* (SC23-8692)

Este manual contiene la información necesaria para desarrollar programas de aplicación mediante APPC (comunicación avanzada programa a programa).

- *IBM Communications Server for AIX or Linux LUA Programmer’s Guide* (SC23-8690)

Este manual contiene la información necesaria para desarrollar aplicaciones utilizando la interfaz de programas de aplicación de LU (LUA) convencional.

- *IBM Communications Server for AIX or Linux CSV Programmer’s Guide* (SC23-8689)

Este manual contiene la información necesaria para desarrollar programas de aplicación utilizando la interfaz de programas de aplicación (API) de CSV (Common Service Verbs).

- *IBM Communications Server for AIX or Linux MS Programmer’s Guide* (SC23-8596)

Este manual contiene la información necesaria para desarrollar aplicaciones utilizando la API de MS (Management Services).

- *IBM Communications Server for Linux NOF Programmer’s Guide* (SC31-6778)

Este manual contiene la información necesaria para desarrollar aplicaciones utilizando la API de NOF (Node Operator Facility).

- *IBM Communications Server para Linux, Guía de diagnósticos* (SC11-3348)

Este manual proporciona información sobre la resolución de problemas en redes SNA.

- *IBM Communications Server for AIX or Linux APPC Application Suite User’s Guide* (SC23-8595)

Este manual proporciona información sobre las aplicaciones APPC utilizadas con Communications Server para Linux.

- *IBM Communications Server for Linux Glossary* (GC31-6780)

Este manual ofrece una completa lista de términos y definiciones utilizados en la biblioteca de Communications Server para Linux.

Publicaciones de SNA (arquitectura de red de sistemas)

Los manuales siguientes contienen información sobre las 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)

Publicaciones de configuración de sistema principal

Los manuales siguientes contienen información sobre la configuración de sistemas principales:

- *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)

Publicaciones de z/OS Communications Server

Los siguientes manuales contienen información sobre 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)

Publicaciones sobre TCP/IP

Los manuales siguientes contienen información sobre el protocolo de red 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)

Publicaciones sobre X.25

Los manuales siguientes contienen información sobre el protocolo de red X.25:

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

Publicaciones de APPC

Los manuales siguientes contienen información sobre APPC (comunicación avanzada programa a programa):

- *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)

Publicaciones sobre programación

Los manuales siguientes contienen información sobre programación:

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

Otras publicaciones de redes de IBM

Los siguientes manuales contienen información sobre otros temas relacionados con 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

A

- activación de puertos y estaciones de enlace 108
- adaptadores de comunicaciones 21
- agrupación de unidades LU
 - configuración 87
 - definición 86
 - ver 87
- alertas 15
- alias, definición para LU asociada 91
- almacenamiento de paginación 23
- almacenamiento en disco 23
- almacenamiento en disco fijo 22
- almacenamiento principal 23
- añadir un recurso 77
- API
 - para la administración de Communications Server para Linux 13
 - soporte 4
 - tipos de Communications Server para Linux 4
- API de NOF 13
- aplicaciones asociadas 6
- APPC
 - Application Suite 6, 9
 - configuración 87
 - en línea 112
 - LU 6.2 dependiente 93
 - LU 6.2 independiente 20
 - soporte de aplicaciones distribuidas 6
- APPC (comunicación avanzada programa a programa) 6
- APPC Application Suite 9
- APPN
 - aplicaciones para 6, 9
 - APPN 1
 - configuración 88, 89
 - configuración dinámica 13
 - direccionamiento 13
 - funciones de subárea 2
 - LU independiente 3
 - nodo final 1
 - red de conexión 13
 - segmentación de redes 25
 - soporte de DLUR 2
 - soporte de sistema principal para 2
- archivo snastart 74, 109
- ayuda
 - programa de administración de Motif 12

B

- bibliotecas de clases de acceso a sistema principal 34
- botones de la barra de herramientas 78
- Branch Extender 8

C

- cliente 5
- cliente Remote API Client
 - requisitos de hardware de Linux para System z 47
 - requisitos de hardware para AIX 53
 - requisitos de hardware para Linux 41
 - requisitos de software de Linux para System z 47
 - requisitos de software para AIX 53
 - requisitos de software para Linux 42
- cliente Remote API Client de Linux
 - información detallada sobre los paquetes existentes 42
- cliente Remote API Client de Linux para System z
 - información detallada sobre los paquetes existentes 48
- cliente Remote API Client de Windows
 - instalación con el programa setup 61
 - instalación desde la línea de mandatos 65
 - instalar 60
- cliente/servidor
 - configuración 79
- comodines 92
- componentes, gestión 76
- compresión de datos de sesión LU 3
- concentración de PU 95
- concentrador de PU 7
- conectividad
 - configuración 82
 - opciones 2
- configuración 18
 - archivos 37, 38
 - comunicación APPC 87
 - conectividad 82
 - copia de seguridad 37
 - DLUR 98
 - ejemplos 80, 81, 99, 102
 - información complementaria de CPI-C 93
 - LU 6.2 90, 93
 - LU asociadas para un nodo LEN 90
 - LU de tipo 0-3 85
 - LU en sentido descendente para pasarela SNA 95
 - LU implícita en sentido descendente 97
 - modificar 77
 - nodo 80
 - nodo remoto 91
 - planificación 72
 - puerto 83
 - registros de asociación de servidor TN 105
 - valores por omisión de servidor TN 105
 - valores por omisión del redirector TN 107

- configuración (*continuación*)
 - ver 77
- configuración de LU 6.2
 - independiente 90
- configuración de LU implícita en sentido descendente 97
- configuración del puerto 83, 84, 85
- configuración dinámica 13
- configuraciones avanzadas, requisitos de memoria y almacenamiento 22
- control de acceso al medio (MAC) 84
- control síncrono de enlace de datos (SDLC) 82
- convenios de denominación 25
- copia de seguridad
 - archivos de configuración 37
 - restauración 38
- corriente de datos 4
- CPI-C
 - API 4
 - configuración 93
 - interoperatividad 15
- CPI-C (CPI-Communications) 4
- CPI-C (interfaz común de programación para comunicaciones) 4

D

- DDDLU (definición dinámica de LU dependientes) 3
- definición de LU local 90
- definición dinámica de LU dependientes (DDDLU) 3
- desinstalación de Communications Server para Linux 39
- desinstalación de un cliente Remote API Client de AIX 56
- desinstalación de un cliente Remote API Client de Linux 46
- desinstalación de un cliente Remote API Client de Linux para System z 51
- detener un recurso 77
- diálogo 75
- diálogo de puerto IP 85
- Dirección IPv4 23
- Dirección IPv6 23
- direccionamiento de sesiones intermedias (ISR) 13
- directorio de los programas ejecutables de Communications Server para Linux 73
- DLC
 - configuración 84, 85
 - configuración del puerto 82
- DLUR
 - configuración 98
 - configuración de PU 100
 - descripción 2
 - nodo local 100
 - soporte para nodos en sentido descendente 100
- DLUS 98

documentación de Communications Server para Linux 34
documentación en línea 111
documentación en línea de Communications Server para Linux 34
dominio 5

E

en línea
APPC 112
ayuda 12
documentación 111
foros 111
grupos de debate 111
Enterprise Extender
configuración de enlace 84
diálogo de puerto 85
visión general 9
estación de enlace
activación 108
definir en puerto 83
Ethernet
configuración de enlace 83
SAP, diálogo 84

F

Formatos de dirección IP 23
foros en línea 111
funciones 4
Funciones de la gestión avanzada de energía del PC 28
funciones de software 6

G

Gestión avanzada de energía 28
Gestión de energía 28
grupos de debate, en línea 111
GSKIT
cliente Remote API Client de AIX 53, 56
cliente Remote API Client de Linux 42, 44
cliente Remote API Client de Linux para System z 48, 50
cliente Remote API Client de Windows 67

H

habilitación de Communications Server para Linux
en el sistema local 74
habilitación del software de Communications Server para Linux 108
HACL 34
hardware
enlace 20
hardware de enlace 20
herramientas de resolución de problemas 15
hojas de tareas 73

hojas de trabajo de planificación 73
HPR
comparado con ISR 13
HPR/IP 9
HTTPS
cliente Remote API Client de AIX 56
cliente Remote API Client de Linux 44
cliente Remote API Client de Linux para System z 50
cliente Remote API Client de Windows 67
configurar 34
requisitos 21

I

igual
red 1
información de release 36
inhabilitación de Communications Server para Linux 107
inicialización del nodo SNA 108
iniciar un recurso 77
inicio automático de Communications Server para Linux 108
activación de puertos y estaciones de enlace 108
habilitación del software de Communications Server para Linux 108
inicialización del nodo SNA 108
inicio en tiempo de re arranque 109
inicio de Communications Server para Linux
automáticamente al arrancar el sistema 74
inicio de Communications Server para Linux durante el arranque 109
instalación 33
cliente Remote API Client de AIX 54, 55
cliente Remote API Client de Linux 43
cliente Remote API Client de Linux para System z 49
información detallada sobre los paquetes existentes 28
pasos previos 28
tareas de mantenimiento posteriores 36
instalación cliente/servidor 36
instalación de Communications Server para Linux 33
instalación de un cliente Remote API Client de AIX 54, 55
instalación de un cliente Remote API Client de Linux 43
instalación de un cliente Remote API Client de Linux para System z 49
installibmcs 33
installibmcsdocs 33
Interconexión de sistemas abiertos (OSI) 26
interfaz de programación de aplicaciones (API) 4

ISO (Organización internacional para la estandarización) 26
ISR (direccionamiento de sesiones intermedias) 13

J

Java
cliente Remote API Client de AIX 53
cliente Remote API Client de Linux 42
cliente Remote API Client de Linux para System z 47

L

LAN (red de área local) 2
lectura recomendada 112
LEN, nodo
configuración de LU asociada 90
descripción 1
identificación de nodo remoto 84
llamadas 4
local/remota, transparencia 3
LU
agrupación 94, 95, 103, 104
asociada, definición 90
configuración 90, 93, 104
convenios de denominación 26
sentido descendente 96, 98
soporte 2
LU 3270
definición 103
para servidor TN 10, 102
LU 6.2 dependiente 93
LU asociada
alias 91
configuración 90, 91
definición mediante comodines 92
nodo remoto 92
LU de tipo 0-3 85, 86
LU en sentido descendente
configuración 98
ejemplos de hardware 96
pasarela SNA 95

M

MAC (control de acceso al medio) 84
mandatos de consulta 15
mandatos de estado 15
MDS-NMVT (soporte de dominio múltiple-transporte de vectores de gestión de la red) 14
medios de transporte 19
memoria de acceso aleatorio (RAM) 23
memoria de kernel 22
memoria principal 23
migración desde niveles anteriores de Communications Server para Linux 29, 30
modificar la configuración 77
múltiples servidores en un dominio 5

N

necesidades funcionales 17
nodo
 comunicación con sistemas principales 80
 configuración 80
 en configuración APPN 81
 inicialización 108
 local 100
 remoto 90, 91
 sentido ascendente 99
 sentido descendente 100
nodo de red de ramificación 8
nodo en sentido ascendente 99
nodo en sentido descendente 99
nodo LEN 84
nodo remoto
 configuración 90, 91
 configuración de LU asociada 92
Nombre de servidor 63

O

opciones de control de enlace de datos 2
opciones de interfaces 13
opciones de seguridad 14
Organización internacional para la estandarización (ISO) 26
OSI (Interconexión de sistemas abiertos) 26

P

parámetro Dominio 62
parámetro Intentos de difusión máx. 64
parámetro Tiempo de espera de acceso a LAN 64
parámetro Tiempo de espera de reconexión 64
Parámetros de difusiones UDP 63
pasarela
 definición 6
 pasarela SNA 6
pasarela SNA
 configuración 95
 visión general 6
PDF, visualización de manuales 36
petionario de LU dependientes (DLUR) 2
planificación, hojas de trabajo 73
planificación de compatibilidad 25
problema
 datos 15
 herramientas de diagnóstico 15
procedimientos
 instalar el cliente Remote API Client para Windows 61, 65
procedimientos posteriores a la instalación 36
proceso distribuido
 entorno 1
 soporte de aplicación 6
programa bajo licencia 32
 cliente Remote API Client de AIX 54
 cliente Remote API Client de Linux 43

programa bajo licencia (*continuación*)
 cliente Remote API Client de Linux para System z 49
programa de administración
 API de NOF 13
 línea de mandatos 13
 Motif 12, 14
programa de administración a través de la línea de mandatos 13
programa de administración de Motif
 ayuda 12
 descripción 12
 posibilidades de gestión 14
 utilizar 71
programa de transacciones (TP) 4
programa xsnaadmin 12, 71
programas TN3270 101
PU (unidad física) 7
puerto
 activación 108
punto de acceso a servicio (SAP) 19, 83
punto de entrada 14
punto focal 14

R

RAM (memoria de acceso aleatorio) 23
recurso
 definición 77
 detener 77
 elementos 78
 gestión 76
 información 111
 iniciar 77
 requisitos 18
 suprimir 77
recursos de información 111
red
 alertas 15
 convenios de denominación 25
 de igual a igual 1
 gestión 14
 información disponible a través de 111
 planificación 17, 18, 25
 soporte 1
 subárea 1
red de área amplia (WAN) 2
red de área local (LAN) 2
red de conexión 13
red de conexión, configuración 84
redirector TN
 configuración 106
 configuración de registro de acceso 107
 configuración de valores por omisión 107
 visión general 11
requisitos
 HTTPS 21
 instalación 20
 memoria y almacenamiento 22
 personal y aptitudes 19
 sistema operativo 20
 software 20, 21
 WebSphere Application Server 21
requisitos de almacenamiento 22

requisitos de aptitudes 19
requisitos de hardware
 cliente Remote API Client de AIX 53
 cliente Remote API Client de Linux 41
 cliente Remote API Client de Linux para System z 47
 cliente Remote API Client de Windows 59
 servidor 20
requisitos de instalación 20
requisitos de memoria 22
 configuraciones avanzadas 22
 tipos de almacenamiento 23
requisitos de personal 19
requisitos de sistema operativo 20
requisitos de software 20, 21
requisitos de Remote API Client de AIX 53
 cliente Remote API Client de Linux 42
 cliente Remote API Client de Linux para System z 47
 cliente Remote API Client de Windows 59
ritmo, nivel de sesión 13
ritmo adaptable a nivel de sesión 13
rpm 19
RUI primaria 3

S

SAA (Systems Application Architecture) 4
SAP (punto de acceso a servicio) 19, 83
SDLC 2
 configuración 83
 para tráfico dependiente 82
SE Linux 20
Seguridad mejorada de Linux 20
servidor 5
 adición 80
 eliminación 80
 requisitos de hardware para Linux 20
servidor de configuración 79
 adición 80
 eliminación 80
servidor de reserva 5
servidor de unidades lógicas dependientes (DLUS) 98
servidor igual 5
servidor maestro 5
servidor maestro de reserva 79
servidor Telnet 9
servidor TN
 configuración 101
 configuración de registro de acceso 105
 configuración de registros de asociación 105, 106
 configuración de valores por omisión 105
 soporte de varias sesiones 103
 usuario 102
 visión general 9
sesión
 direccionamiento 13

- sesión (*continuación*)
 - forma de U 3
 - ritmo 13
 - soporte 3
- sesiones en forma de U 3
- sistema en sentido descendente 96
- sistema principal
 - en red APPN 2
 - en red de subárea 1
 - soporte de LU 2
- SNA
 - biblioteca 111
- snaadmin, programa 13
- software de cliente
 - actualizar 69
 - desinstalar 69, 70
 - personalizar 68
 - volver a instalar 69
- software SDK
 - cliente Remote API Client de Windows 60
- soporte de cliente/servidor 5
- soporte de dominio múltiple-transporte de vectores de gestión de la red (MDS-NMVT) 14
- SSL (Secure Sockets Layer)
 - autenticación de cliente 105, 107
 - autenticación de servidor 37, 105, 107
 - cifrado de datos 36, 105, 107
- start, mandato 74
- stop, mandato 107
- subrutinas 4
- suprimir un recurso 77
- Systems Application Architecture (SAA) 4

- ver la configuración 77
- verbos 4
- versión, dirección IP 23
- vía de acceso de los programas ejecutables de Communications Server para Linux 73

W

- WAN (red de área amplia) 2
- WebSphere Application Server
 - configurar 34
 - requisitos 21

T

- tareas de preinstalación 28
- TN3270
 - programas 9
 - servidor 9
- TP (programa de transacciones) 4
- transparencia local/remota 3

U

- unidad física (PU) 7
- unidad lógica (LU) 2, 98
- usuario TN3270 10, 102

V

- variable de entorno de idioma 29, 54
 - cliente Remote API Client de Linux 43
 - cliente Remote API Client de Linux para System z 48
- ventana 75
- ventana de configuración, cliente Remote API Client de Windows
 - parámetros 62
 - parámetros avanzados 64
- ventana Nodo 76
- ventanas de recursos, botones 78



Número de Programa:

GC10-9852-03

