IBM Communications Server for AIX

Guida rapida

V64

GC13-4142-04

IBM Communications Server for AIX

Guida rapida

V64

GC13-4142-04

Nota:
Prima di utilizzare queste informazioni ed il prodotto supportato, consultare le informazioni generali riportate in “Note legali”, a pagina 111.

Sesta edizione (maggio 2009)

Questa edizione si applica a IBM Communications Server for AIX, V6.4 (numero programma 5765-E51) e a tutti i successivi rilasci e modifiche, se non diversamente specificato in nuove edizioni o in newsletter di carattere tecnico.

Ordinare le pubblicazioni mediante il rappresentante IBM o gli uffici IBM del proprio paese. Le pubblicazioni non sono disponibili all'indirizzo di seguito riportato.

IBM attende le vostre opinioni. È possibile inviare i propri commenti al seguente indirizzo:

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

È possibile inviare i propri commenti in formato elettronico, mediante una delle seguenti modalità:

- Fax (USA e Canada):
  - 1+919-254-4028
  - Inviare il fax a: ″Attn: Communications Server for AIX Information Development″
- E-mail:
  - comsvrcf@us.ibm.com

Inviando informazioni a IBM, si garantisce a IBM un diritto non esclusivo di utilizzo o distribuzione di tali informazioni nei modi ritenuti più appropriati senza alcun obbligo nei confronti degli utenti.

Indice

Tabelle vii

Figure ix

Benvenuti in IBM Communications Server for AIX xi

Come utilizzare questo libro xi
Roadmap xi
Convenzioni tipografiche xii
Abbreviazioni utilizzate nel presente libro . . . xii
Novità xiii
Funzioni nuove xiv
Funzioni eliminate xiv
Ulteriori informazioni xv

Capitolo 1. Informazioni su IBM Communications Server for AIX 1

IBM Communications Server for AIX - Funzioni e creazione pacchetti 1
IBM Communications Server for AIX V6.4 . . . 1
Funzioni di rete avanzate 6
Funzioni e vantaggi. 11
Blocchi di creazione versatili. 11
Funzionamento client/server 12
Configurazione semplice 12
Ulteriori opzioni di gestione dell'interfaccia utente 13
Migliori prestazioni. 13
Opzioni di sicurezza 14
Flessibilità nella gestione della rete 14
Affidabilità, disponibilità e livello di servizio . . 15
Integrazione, ampliamento e modifica della rete 16

Capitolo 2. Pianificazione della rete e IBM Communications Server for AIX . . 17

Fasi della pianificazione della rete 17
Identificazione dei requisiti funzionali della rete 17
Determinazione della configurazione di CS/AIX 18
Identificazione dei requisiti delle risorse per l'installazione e il funzionamento 18
Indirizzamento IPv4 e IPv6 24
Come garantire la compatibilità tra configurazioni per diverse piattaforme 25
Convenzioni di denominazione. 26

Capitolo 3. Installazione di CS/AIX su server AIX 27

Gestione delle licenze e creazione pacchetti di CS/AIX 27
Meccanismi di gestione delle licenze di CS/AIX 27
Come vengono creati i pacchetti del programma CS/AIX concesso in licenza 29
Preparazione dell'installazione di CS/AIX 31
Installazione delle serie di file DLC (Data Link Control) 31
Visualizzazione dei dettagli di installazione del prodotto 31
Modifica della variabile d'ambiente della lingua 32
Migrazione dai livelli precedenti di CS/AIX . . . 32
Considerazioni 32
Installazione del programma CS/AIX concesso in licenza 33
Modalità di installazione 33
Configurazione di WebSphere Application Server. . 37
Impostazione del certificato di sicurezza di WebSphere Application Server 37
Configurazione di WebSphere Application Server 37
Installazione del file di configurazione del server 38
Procedure successive all'installazione. 38
Funzionamento client/server 38
Visualizzazione di libri in PDF 39
Consultazione delle informazioni sul rilascio corrente 39
Configurazione di SSL per l'utilizzo con il server TN o il programma di reindirizzamento TN . . 39
Configurazione di un server Web per il programma di gestione Web. 40
Host Access Class Library 40
Esecuzione del backup dei file di configurazione di CS/AIX. 40
Ripristino di una copia di backup dei file di configurazione di CS/AIX 41
Reinizializzazione dei file di configurazione . . 42

Capitolo 4. Installazione di IBM Remote API Client su Linux 43

Requisiti hardware e software 43
Requisiti hardware 43
Versione del sistema operativo Linux 44
Java 44
GSKIT (Global Security Kit) 44
Visualizzazione dei dettagli di installazione del prodotto 44
Impostazione della variabile d'ambiente della lingua 44
Installazione di Remote API Client su Linux . . . 45
Impostazione di certificati di sicurezza HTTPS tramite GSKIT 46
Disinstallazione di Remote API Client su Linux . . 47

Capitolo 5. Installazione di IBM Remote API Client su Linux for System z . . . 49

Requisiti hardware e software 49
Requisiti hardware 49
Versione del sistema operativo Linux 49
Java 49
GSKIT (Global Security Kit) 49

Visualizzazione dei dettagli di installazione del prodotto 50
Impostazione della variabile d'ambiente della lingua 50
Installazione di Remote API Client su Linux for System z 50
Impostazione di certificati di sicurezza HTTPS tramite GSKIT 52
Disinstallazione di Remote API Client su Linux for System z 53

Capitolo 6. Installazione di IBM Remote API Client su sistemi AIX 55
Requisiti hardware e software 55
Requisiti hardware 55
Versione del sistema operativo 55
Java 55
GSKIT (Global Security Kit) 55
Modifica della variabile d'ambiente della lingua 56
Installazione di Remote API Client su AIX 56
Installazione di Remote API Client tramite copia dei file sulla stazione di lavoro AIX in uso . . . 56
Installazione di Remote API Client dal CD . . . 57
Impostazione di certificati di sicurezza HTTPS tramite GSKIT 57
Disinstallazione di Remote API Client su AIX . . . 58

Capitolo 7. Pianificazione e installazione di Remote API Client su Windows 59
Requisiti hardware e software 59
Accesso al programma di installazione 60
Installazione di Remote API Client su Windows tramite il programma di installazione. 61
Opzioni avanzate per la configurazione di Remote API Client 64
Installazione del software Remote API Client dalla riga comando. 65
Impostazione di certificati di sicurezza HTTPS tramite GSKIT 67
Personalizzazione del software Remote API Client dopo l'installazione. 68
Reinstallazione del software Remote API Client . . 68
Disinstallazione del software Remote API Client . . 69
Disinstallazione del software Remote API Client dalla riga comando 69
Guida 70

Capitolo 8. Configurazione e utilizzo di CS/AIX 71
Pianificazione della configurazione di CS/AIX. . . 72
Fogli di lavoro per la pianificazione 72
Fogli di lavoro per le attività 73
Utilizzo del programma di gestione Motif 73
Come specificare il percorso ai programmi di CS/AIX 73
Abilitazione di CS/AIX 74
Gestione di CS/AIX con il programma di gestione Motif 74
Configurazione delle funzioni client/server. . . . 79
Configurazione del nodo 80
Configurazione della connettività 81
Configurazione di un collegamento SDLC per il traffico dipendente 82
Configurazione di un collegamento Ethernet per supportare il traffico dipendente e indipendente . 83
Configurazione di un collegamento Enterprise Extender 84
Configurazione delle LU di tipo 0–3 85
Definizione delle LU di tipo 0–3 86
Definizione di un pool di LU 86
Configurazione della comunicazione APPC. . . . 87
Configurazione di una rete APPN semplice. . . 88
Configurazione dell'APPC dipendente 92
Configurazione delle comunicazioni CPI. 93
Configurazione della LUA 93
Configurazione del gateway SNA 94
Supporto di LU in downstream implicite . . . 95
Definizione delle LU in downstream 96
Configurazione DLUR. 97
Configurazione del supporto DLUR nel nodo locale 98
Configurazione del supporto DLUR pass-through per i nodi in downstream. 99
Configurazione del server TN 99
Definizione delle LU 3270 102
Definizione di un pool di LU 102
Configurazione del server TN3270 103
Configurazione del programma di reindirizzamento TN 104
Configurazione del programma di reindirizzamento TN 104
Configurazione di AnyNet 105
Configurazione di APPC over TCP/IP 106
Disabilitazione di CS/AIX 107

Capitolo 9. Risorse informative su CS/AIX e SNA 109
Libreria SNA 109
Informazioni accessibili dalla rete. 109
Letture consigliate 110

Appendice. Note legali 111
Marchi 113

Bibliografia 115
Pubblicazioni relative a CS/AIX, V6.4 115
Redbook IBM 116
Pubblicazioni relative al sistema operativo AIX . . 116
Pubblicazioni relative alla SNA (Systems Network Architecture) 117
Pubblicazioni relative alla configurazione host . . 117
Pubblicazioni relative a z/OS Communications Server 117
Pubblicazioni relative a TCP/IP 117
Pubblicazioni relative a X.25 118
Pubblicazioni relative all'APPC 118
Pubblicazioni relative alla programmazione . . . 118
Altre pubblicazioni relative alle reti IBM 118

Indice analitico. 119

Tabelle

1. Guida introduttiva - Roadmap xi
2. Convenzioni tipografiche xii

Figure

1. Gateway SNA che collega più computer AIX in downstream a un computer host 7
2. Branch Extender 8
3. Server TN 10
4. Finestra Node 76
5. Barra degli strumenti di CS/AIX 78
6. Nodo CS/AIX che comunica direttamente con un host 80
7. Nodi CS/AIX in una rete APPN 81
8. Gateway SNA 94
9. Nodo CS/AIX che fornisce il DLUR 98
10. Nodo CS/AIX configurato per il server TN 100
11. server TN 101
12. Nodo di accesso AnyNet APPC over TCP/IP 106
13. Gateway AnyNet APPC over TCP/IP 106

Benvenuti in IBM Communications Server for AIX

Questo libro presenta IBM Communications Server for AIX, un prodotto software IBM che consente ai server che eseguono il sistema operativo AIX (Advanced Interactive Executive) di IBM di scambiare informazioni con altri nodi in una rete SNA (Systems Network Architecture). Si tratta del prodotto più completo per reti SNA attualmente disponibile per le stazioni di lavoro che eseguono il sistema operativo AIX.

IBM Communications Server for AIX è progettato per essere eseguito su una stazione di lavoro AIX connessa a una o più reti. CS/AIX V6.4 può essere eseguito su qualsiasi sistema IBM RISC System/6000o eServer pSeries supportato dalle versioni 5.2, 5.3 o 6.1 di AIX. In questo libro, l'espressione "stazione di lavoro AIX" indica uno qualsiasi di questi sistemi in cui è installato il sistema operativo AIX.

CS/AIX fornisce blocchi di creazione per rispondere a un'ampia gamma di esigenze e soluzioni legate alle reti. Possono essere utilizzati per scambiare informazioni con i nodi nelle reti SNA, nelle reti TCP/IP (Transmission Control Protocol/Internet Protocol) e nelle reti integrate SNA-TCP/IP.

Come utilizzare questo libro

Questa sezione spiega in che modo le informazioni sono state organizzate e presentate all'interno del libro.

Roadmap

Questo libro è destinato al personale tecnico e di gestione che si occupa della pianificazione delle reti e a chiunque sia interessato a Communications Server per il sistema operativo AIX.

Le informazioni necessarie per iniziare a lavorare con CS/AIX, sono disponibili in Tabella 1.

Tabella 1. Guida introduttiva - Roadmap

Per...	Consultare...
Informazioni su CS/AIX	Capitolo 1, "Informazioni su IBM Communications Server for AIX", a pagina 1
Pianificare l'utilizzo di CS/AIX nella propria rete	Capitolo 2, "Pianificazione della rete e IBM Communications Server for AIX", a pagina 17
Installare CS/AIX sui server AIX	Capitolo 3, "Installazione di CS/AIX su server AIX", a pagina 27
Installare Remote API Client su Linux (32–bit Intel, 64–bit Intel/AMD o pSeries)	Capitolo 4, "Installazione di IBM Remote API Client su Linux", a pagina 43
Installare Remote API Client su Linux for System z	Capitolo 5, "Installazione di IBM Remote API Client su Linux for System z", a pagina 49

Tabella 1. Guida introduttiva - Roadmap (Continua)

Per...	Consultare...
Installare Remote API Client su AIX	Capitolo 6, "Installazione di IBM Remote API Client su sistemi AIX", a pagina 55
Installare Remote API Client su Windows	Capitolo 7, "Pianificazione e installazione di Remote API Client su Windows", a pagina 59
Configurare CS/AIX	Capitolo 8, "Configurazione e utilizzo di CS/AIX", a pagina 71
Reperire informazioni sulla documentazione relativa a CS/AIX e altre pubblicazioni, incluse informazioni online	Capitolo 9, "Risorse informative su CS/AIX e SNA", a pagina 109
Prendere visione delle informazioni su note legali e marchi	"Note legali", a pagina 111

Convenzioni tipografiche

Gli stili tipografici utilizzati nel presente documento sono mostrati nella Tabella 2.

Tabella 2. Convenzioni tipografiche

Elementi particolari	Campione tipografico
Parole evidenziate	**eseguire il back up dei file prima di cancellare**
Titolo del documento	*IBM Communications Server for AIX Administration Guide*
Nome file o percorso	**/usr/spool/uucp/miofile.bkp**
Programma o applicazione	**snaadmin**
Immissione utente	**0p1**
Output del computer	**CLOSE**

Abbreviazioni utilizzate nel presente libro

In questo libro vengono utilizzate le seguenti abbreviazioni:

AIW	APPN Implementers Workshop
AIX	Advanced Interactive Executive
ANR	Automatic Network Routing
API	Application Programming Interface
APPC	Advanced Program-to-Program Communication
APPN	Advanced Peer-to-Peer Networking
ATM	Asynchronous Transfer Mode
BOS	Base Operating System
BrNN	Branch Network Node
CICS	Customer Information Control System
COS	Class of Service
CPI-C	Common Programming Interface for Communications
CSV	Common Service Verb
DB2	DATABASE 2
DDDLU	Dynamic Definition of Dependent LU
DES	Data Encryption Standard
DLC	Data Link Control

DLUR	Dependent LU Requester
DLUS	Dependent LU Server
FDDI	Fiber Distributed Data Interface
FTP	File Transfer Protocol
HPR	High-Performance Routing
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ISO	International Standards Organization
ISR	Intermediate Session Routing
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LEN	Low-Entry Networking
LLC2	Logical Link Control 2
LU	Logical Unit
LUA	Conventional LU Application Programming Interface
MDS-NMVT	Multiple Domain Support—Network Management Vector Transport
MPC	MultiPath Channel
MPQP	Multiprotocol Quad Port
MPTN	Multiprotocol Transport Networking
MS	Management Services
NMVT	Network Management Vector Transport
NOF	Node Operator Facility
OS/2	Operating System/2
OSI	Open Systems Interconnection
PU	Physical Unit
RFC	Request For Comments
RISC	Reduced Instruction Set Computer
RLE	Run-Length Encoding
RTP	Rapid Transport Protocol
SAA	Systems Application Architecture
SAP	Service Access Point
SDLC	Synchronous Data Link Control
SLP	Service Location Protocol
SMIT	Systems Management Interface Tool
SMP	Symmetric Multi-processing
SNA	Systems Network Architecture
SNMP-MIB	Simple Network Management Protocol—Management Information Base
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TN	Telnet
TP	Transaction Program
VT	Virtual Terminal
VTAM	Virtual Telecommunications Access Method
WAN	Wide Area Network

Novità

Communications Server for AIX V6.4 sostituisce Communications Server for AIX V6.3.1.

I rilasci di questo prodotto ancora supportati sono:

- Communications Server for AIX V6.3.1
- Communications Server for AIX V6.3.0

I seguenti rilasci di questo prodotto non sono più supportati:

- Communications Server for AIX Versione 6.1 (V6.1)
- Communications Server for AIX Versione 6 (V6)
- Communications Server for AIX Versione 5 (V5)
- Communications Server for AIX Versione 4, Rilascio 2 (V4R2)
- Communications Server for AIX Versione 4, Rilascio 1 (V4R1)
- SNA Server for AIX, Versione 3, Rilascio 1.1 (V3R1.1)
- SNA Server for AIX, Versione 3, Rilascio 1 (V3R1)
- AIX SNA Server/6000, Versione 2, Rilascio 2 (V2R2)
- AIX SNA Server/6000, Versione 2, Rilascio 1 (V2R1) su AIX 3.2
- AIX SNA Services/6000, Versione 1

Communications Server for AIX V6.4 opera con IBM Remote API Client Versioni 6.4.0, 6.3.1 o 6.3.0.

Funzioni nuove

In questo rilascio, sono state aggiunte a CS/AIX le seguenti funzioni:

- È possibile indicare una corrispondenza tra i tipi di dispositivo TN3270 e i modelli LU che CS/AIX deve richiedere all'host quando questi dispositivi si connettono tramite il server TN di CS/AIX mediante DDDLU. Ciò consente l'utilizzo del modello LU più appropriato per ciascun tipo di dispositivo.
- L'instradamento HPR (High Performance Routing) dispone ora di ulteriori opzioni di configurazione:
  - La modalità progressiva ARB (nota anche come ARB-P), che migliora il controllo del flusso HPR in caso di variazioni del tempo di risposta sui sistemi remoti e virtuali.
  - Un timer di ritardo di commutazione del percorso configurabile, che aiuta ad evitare inutili commutazioni di percorso causate da ritardi transitori nel traffico di rete.
- L'interfaccia APPC include il nuovo verbo CANCEL_CONVERSATION, che consente di deallocare una conversazione anche in presenza di altri verbi ancora in sospeso. Questo verbo opera in maniera analoga alla chiamata Cancel_Conversation (cmcanc) della CPI-C ed è disponibile su AIX, Linux e Windows.
- In IBM Remote API Client for Windows, ora è possibile eseguire i programmi di utilità (l'utilità di configurazione del client **sxclconf**, il client monitor **sxclappl** e l'utilità della riga di comando **tpinst32** per la configurazione di un TP richiamabile) in una qualsiasi delle lingue supportate; l'utente non è vincolato all'utilizzo della lingua impiegata durante l'installazione del client.
- In IBM Remote API Client for Windows, l'utilità di configurazione del client **sxclconf** consente ora di abilitare o disabilitare la registrazione delle eccezioni, la registrazione dei controlli e la traccia (traccia API su tutte le API e traccia client/server sui messaggi tra il client e il server).
- Le applicazioni CPI-C Java sono ora supportate in IBM Remote API Client for Windows, nonché su AIX e Linux.

Funzioni eliminate

La funzione AnyNet APPC over TCP/IP è ancora supportata in questo rilascio, ma solo sui sistemi a 32–bit con interfacce IPv4 e non sui sistemi a 64–bit né con le interfacce IPv6. Nei rilasci futuri non verrà più supportata.

Nella versione 6.4, il driver AnyNet non viene caricato per impostazione predefinita. Per utilizzare AnyNet APPC over TCP/IP, modificare il file **/etc/rc.sna** e seguire i commenti all'inizio del file per abilitare AnyNet.

Ulteriori informazioni

La Bibliografia indica altri libri della libreria CS/AIX, nonché libri contenenti informazioni aggiuntive su SNA, il sistema operativo AIX e altri prodotti correlati.

Capitolo 1. Informazioni su IBM Communications Server for AIX

Questo capitolo spiega in che modo vengono creati i pacchetti di CS/AIX e ne descrive le funzioni, le caratteristiche e i vantaggi.

IBM Communications Server for AIX - Funzioni e creazione pacchetti

CS/AIX V6.4 un software di comunicazione che viene eseguito sul sistema operativo AIX. Comprende le funzioni descritte in "IBM Communications Server for AIX V6.4" e "Funzioni di rete avanzate" a pagina 6.

IBM Communications Server for AIX V6.4

IBM Communications Server for AIX V6.4 consente di connette applicazioni tra reti SNA e TCP/IP. Converte una stazione di lavoro che esegue AIX in un nodo SNA munendola dei relativi protocolli e risorse. La stazione è così in grado di comunicare con altri computer (inclusi i computer host) in una rete SNA. Fornisce, inoltre, funzioni TCP/IP al fine di permettere l'utilizzo di IBM Communications Server for AIX all'interno della propria rete TCP/IP o ai limiti tra la rete TCP/IP e la rete SNA.

CS/AIX offre i seguenti servizi:

Supporto di rete
CS/AIX supporta reti peer-to-peer e di sottoarea:

Reti di sottoarea SNA
Queste reti (note anche come reti mediate dall'host) sono organizzate gerarchicamente, con uno o più computer host che controllano la comunicazione tra computer, gestiscono la rete e forniscono servizi di elaborazione e archiviazione dati ad alta capacità. Tutti gli altri nodi della rete dipendono dal controllo di un host.

È possibile includere i computer AIX in una rete di sottoarea, configurandoli come nodi dipendenti dall'host.

Reti peer-to-peer
Per gli ambienti di elaborazione distribuita, CS/AIX V6.4 supporta le reti APPN e TCP/IP. In queste reti peer-to-peer, i computer AIX mantengono le funzioni di elaborazione e comunicano direttamente l'uno con l'altro come peer. Le reti peer-to-peer sfruttano appieno le funzionalità dei computer AIX, oggi in grado di competere con quelle di costosi computer host.

Una rete APPN è formata dai seguenti tipi di nodi peer:

- Il nodo di rete APPN (che fornisce controllo del traffico, calcolo dinamico dell'instradamento e servizi di selezione, nonché servizi di gestione della rete)
- Il nodo finale APPN (che utilizza i servizi dei nodi di rete APPN per comunicare con i nodi peer)
- Il nodo LEN (che comunica direttamente con i nodi adiacenti o con i nodi configurati per apparire tali).

Nota: In una rete APPN, i computer host possono fungere da nodi peer utilizzando LU 6.2 indipendenti per comunicare con i computer AIX e con altri host all'interno della rete.

Fornire funzioni di sottoarea in una rete APPN
La funzione DLUR (Dependent LU Requester) consente il traffico tra i nodi host e i nodi dipendenti dall'host in una rete APPN.

Opzioni di controllo collegamento dati (DLC, Data Link Control)
A livello di collegamento, CS/AIX offre numerose opzioni di connettività, al fine di agevolare il raggiungimento dei propri obiettivi di costo, sicurezza, velocità e dimensione della rete (per un elenco dettagliato dei tipi di collegamento supportati, consultare "Requisiti di installazione" a pagina 20). Supporta collegamenti dati per diversi tipi di rete:

Local Area Network
Per quanto riguarda la connettività LAN, è possibile installare i collegamenti appropriati per comunicare mediante protocolli Token Ring, Ethernet standard ed Ethernet 802.3 (è possibile fornire un supporto ATM mediante interfaccia LAN emulata su una rete Token Ring o Ethernet).

Wide Area Network
Per quanto concerne la connettività WAN, è possibile selezionare uno dei seguenti collegamenti sincroni per comunicare su linee telefoniche dedicate:

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

CS/AIX supporta, inoltre, Data Link Control X.25 a commutazione di pacchetti (questi tipi di collegamento necessitano di prodotti aggiuntivi, ordinabili separatamente).

Integrazione IP
Se la propria rete backbone aziendale è basata su IP, è possibile utilizzare la funzione Enterprise Extender (HPR/IP) di CS/AIX per integrarla con SNA, consentendo così alle proprie applicazioni SNA di comunicare sulla rete IP.

Supporto LU
Le Logical Unit (LU) sono risorse di rete specifiche per l'applicazione che risiedono in ciascun nodo di una rete SNA. Ciascuna LU funge da interfaccia, che le applicazioni utilizzano per accedere ai collegamenti al fine di comunicare nella rete con applicazioni partner dislocate su altri nodi.

CS/AIX supporta diversi tipi di LU per le diverse classi di applicazioni.

- In una rete di sottoarea, CS/AIX supporta i seguenti tipi di LU dipendenti:
  - LU 0
  - LU 1
  - LU 2
  - LU 3

– LU 6.2

La LU 0 supporta comunicazioni tra programmi primitive, tipicamente utilizzate nelle transazioni POS (Point-Of-Sale) nella vendita al dettaglio e nell'attività bancaria. La LU 2 supporta le applicazioni di emulazione di terminale che consentono al computer AIX di emulare un terminale della famiglia IBM 3270. Gli altri tipi di LU consentono alle applicazioni di partecipare all'elaborazione distribuita o di comunicare con varie stampanti o terminali di visualizzazione interattivi.

CS/AIX supporta sistemi host che utilizzano la DDDLU (Dynamic Definition of Dependent LU), una funzione dell'host che consente di aggiungere le LU dipendenti sul sistema SNA alla configurazione dell'host quando viene stabilito il collegamento di comunicazione tra il sistema SNA e l'host. Con la DDDLU, non è necessario configurare le LU staticamente nell'host (ma si devono comunque definire LU dipendenti sul nodo CS/AIX). Ciò riduce la configurazione iniziale richiesta a livello dell'host e facilita un'eventuale espansione futura.

CS/AIX può comunicare sia con host con supporto DDDLU che con host senza supporto DDLU, senza alcuna differenza in termini di configurazione richiesta. Una volta stabilito il collegamento di comunicazione dal nodo CS/AIX all'host, l'host con supporto DDDLU comunica al nodo di essere in grado di supportare la DDDLU; successivamente, il nodo invia le informazioni richieste per definire le LU dipendenti che utilizzano il collegamento. Se l'host è senza supporto DDDLU, CS/AIX non invia questa informazione e presume che le LU siano già state definite staticamente a livello dell'host.

- La LU 6.2 indipendente supporta il traffico indipendente nelle reti APPN. La LU 6.2 indipendente supporta la gestione autonoma delle reti e delle comunicazioni, nonché l'elaborazione distribuita.

  Inoltre, la funzione DLUR di CS/AIX consente al traffico proveniente dalle LU dipendenti di viaggiare su una rete APPN.

- Il supporto RUI principale fornisce all'applicazione CS/AIX la capacità di gestire i dispositivi LU dipendenti assegnati alla LAN/WAN in downstream come se fosse un mainframe. Questa funzione presenta alcune limitazioni in termini di connettività, ma consente alle applicazioni di trasmettere dati tra dispositivi LU dipendenti, senza la necessità di disporre di un'applicazione di mainframe completa.

Supporto sessioni

Una sessione è un canale logico temporaneo tra LU partner. Normalmente, le applicazioni partner associate a ciascuna LU comunicano durante la sessione. CS/AIX è in grado di supportare migliaia di sessioni. CS/AIX può supportare anche sessioni a ″U″ (note anche come "trasparenza locale/remota"), in cui la LU principale e quella secondaria risiedono nello stesso computer AIX. Ciò consente di sviluppare e testare una coppia di programmi di transazione di origine e di destinazione in un unico computer, senza la necessità di una connessione di collegamento.

I dati trasmessi in una sessione tra due LU partner possono essere compressi, per ridurre la larghezza di banda richiesta.

- Per quanto riguarda le LU 6.2, CS/AIX consente di specificare l'utilizzo della compressione nella configurazione della modalità impiegata dalla sessione. È possibile specificare diversi algoritmi di compressione da utilizzare, ciascuno dei quali fornisce un livello di compressione differente (RLE, LZ9 o LZ10). Inoltre, è possibile indicare differenti livelli

di compressione per i dati trasmessi in direzioni differenti durante la sessione o impostare la compressione in una direzione, ma non nell'altra.

- Per quanto riguarda le LU 0–3, CS/AIX consente di specificare l'utilizzo della compressione nella configurazione della stazione di collegamento o della PU impiegata dalla sessione. La compressione RLE viene utilizzata per la direzione in ingresso, mentre la LZ9 per quella in uscita.

Supporto API

CS/AIX contiene le API (Application Programming Interface) necessarie per lo sviluppo di applicazioni per determinati tipi di LU, per l'elaborazione distribuita, per la gestione della rete e per l'amministrazione dello stesso CS/AIX. In questo rilascio, CS/AIX fornisce una serie di API compatibili con quelle fornite dai membri della famiglia Communications Server in esecuzione su altri sistemi operativi.

Un'API è un'interfaccia che consente a un programma di transazione (Transaction Program, TP) di comunicare con la rispettiva LU di supporto. È formata da una libreria di verbi (detti anche funzioni, chiamate e sottoroutine), da cui il TP seleziona quelli che deve trasmettere alla propria LU per richiedere un'azione, come ad esempio SEND_DATA. A sua volta, la LU elabora i verbi e genera un flusso di dati in base al protocollo appropriato, appone un'intestazione che indica l'indirizzo di destinazione e invia i dati alle LU partner tramite il collegamento.

La Common Programming Interface for Communications (CPI-C) è una delle API più potenti, grazie alla sua portabilità. Introdotta per supportare le LU 6.2 dipendenti e indipendenti, CPI-C rispetta le disposizioni della SAA (Systems Application Architecture) per l'unificazione di piattaforme e sistemi operativi diversi tra loro. CPI-C utilizza un insieme di regole di sintassi comune a tutti i sistemi. È dunque divenuta uno standard.

Oltre all'API CPI-C standard in linguaggio C, CS/AIX include anche un'API CPI-C per le applicazioni Java. Per ulteriori informazioni, consultare *IBM Communications Server for AIX or Linux - CPI-C Programmer's Guide*. Salvo diversa indicazione, nei libri di CS/AIX ogni riferimento a CPI-C include CPI-C Java.

Tra le altre API CS/AIX vi sono inoltre:

- API APPC per comunicazioni peer-to-peer tra applicazioni mediante LU 6.2. L'API può essere anche impostata come non-blocking. Se un TP utilizza verbi di tipo non-blocking, l'API può restituire il controllo al TP prima del completamento dell'azione richiesta. Successivamente, il TP viene informato del completamento dell'azione.
- API LUA per comunicazioni con applicazioni host.
- API CSV (Common Service Verb) per funzioni di utilità quali la conversione dei caratteri e il controllo traccia delle applicazioni.

Inoltre, CS/AIX include le seguenti API proprietarie:

- API MS (Management Services) per le funzioni di messaggistica di rete.
- API NOF (Node Operator Facility) per applicazioni che configurano e gestiscono le risorse CS/AIX.

Le applicazioni che utilizzano le API CS/AIX possono essere compilate e collegate per essere eseguite in modalità a 32 bit o a 64 bit.

Per informazioni dettagliate sull'API, consultare la guida di programmazione dell'API (vedi Bibliografia).

Supporto client/server

I computer che eseguono CS/AIX possono essere configurati per comunicare attraverso protocolli client/server. Quando in una rete vengono utilizzati protocolli client/server, i computer che li utilizzano per comunicare in quella determinata rete vengono collettivamente denominati "dominio."

I computer che eseguono CS/AIX in una configurazione client/server possono utilizzare le seguenti regole:

- Il server contiene un nodo SNA e i componenti di connettività ad esso associati. Il server fornisce la connettività SNA alle applicazioni presenti sul sistema locale o su altri computer del dominio CS/AIX. I server devono essere sistemi AIX.
- Il client API remoto non contiene componenti del nodo SNA, ma può accedervi attraverso il server. Il client può accedere contemporaneamente a uno o più server e, se necessario, può eseguire applicazioni simultanee. I client possono eseguire AIX, Linux o Windows (un computer AIX può essere un server o un client, ma non entrambi; non è possibile installare il server e il client sullo stesso computer).

I server e i client comunicano attraverso il dominio CS/AIX, mediante TCP/IP. In alternativa, possono comunicare tramite HTTPS mediante un server WebSphere che utilizza certificati di sicurezza per autenticare le connessioni dei client. L'HTTPS viene normalmente utilizzato per la connessione dei client su una rete pubblica.

In un dominio con più server CS/AIX, la copia master del file di configurazione del dominio CS/AIX risiede in un unico server. Questo server è noto come server master. È possibile definire gli altri server del dominio come server di backup o lasciarli come server peer. Il file di configurazione del dominio viene copiato nei server di backup— all'avvio o alla modifica della copia master— affinché tutti i server di backup dispongano di una copia delle informazioni più aggiornate. Un server peer ottiene le informazioni relative alla configurazione del dominio dal server master secondo necessità, ma non può fungere da server di backup.

Se il server master non funziona correttamente, il primo server di backup dell'elenco dei server definito per il dominio subentra in qualità di master. Il file di configurazione del domino presente in questo server viene utilizzato come copia master e, se necessario, copiato negli altri server. Al riavvio del server master, quest'ultimo riceve dal server di backup che ha assunto la funzione di master una copia del file di configurazione del dominio e poi subentra in qualità di master.

Supporto per applicazioni distribuite

In un sistema CS/AIX client/server, le applicazioni in esecuzione su Remote API Client cooperano con le risorse di connettività presenti sui server per eseguire una sola attività. Inoltre, le applicazioni in esecuzione su altri computer (non CS/AIX) possono cooperare con le applicazioni dei computer CS/AIX per eseguire un'elaborazione distribuita.

CS/AIX supporta i seguenti tipi di applicazioni distribuite:

- APPC applicazioni (l'APPC è nota anche come LU 6.2)
- Supporto di due note applicazioni di elaborazione distribuita:
  - Customer Information Control System (CICS)
  - DATABASE 2 (DB/2), sviluppato per LU 6.2 (dipendente e indipendente).

CICS e DB2 (un sistema di gestione di database relazionali) sono applicazioni compatibili con SAA e facilmente personalizzabili per qualsiasi ambiente. Le applicazioni CICS e DB2 vengono utilizzate congiuntamente dal 90% delle società elencate in Fortune 500. Si tratta di potenti programmi di transazione in grado di servire migliaia di nodi contemporaneamente. Solitamente, CICS e DB2 vengono utilizzati per accedere a dati provenienti da più ubicazioni, aggiornarli e memorizzarli in un repository centrale.

Host Access Class Library

Host Access Class Library (Host Access API), incluso nel supporto di installazione di CS/AIX, consente di sviluppare applicazioni Java per l'accesso ad applicazioni 3270, 5250 o VT su un sistema host. Fornisce un insieme di metodi e classi di base per lo sviluppo di applicazioni indipendenti dalla piattaforma in grado di accedere alle informazioni dell'host a livello del flusso di dati. Ad esempio, è possibile sviluppare un'interfaccia grafica (cui si accede mediante browser Web) per un'applicazione host esistente basata su caratteri, al fine di agevolarne l'utilizzo.

Funzioni di rete avanzate

La versione base di CS/AIX V6.4 include un insieme di funzioni che aggiungono al prodotto funzionalità di rete avanzate. Tali funzioni includono quanto segue:

- Il gateway SNA connette le LAN alle reti SNA di sottoarea.
- Il supporto della LU principale agevola il controllo dei dispositivi LU dipendenti in downstream in maniera analoga a un'applicazione mainframe host.
- Branch Extender semplifica le grandi reti APPN suddividendo le risorse in differenti ubicazioni (ad esempio in filiali distinte di una grande azienda). Ciò riduce la quantità di informazioni sulla topologia da memorizzare, consentendo al contempo un posizionamento efficiente delle risorse.
- APPC Application Suite fornisce applicazioni appositamente selezionate per l'utilizzo su reti APPN.
- Enterprise Extender (EE, noto anche come HPR/IP) consente il trasporto a livello nativo del traffico SNA sulle reti IP.
- Il server TN fornisce l'accesso host su SNA ai client TN3270 e TN3270E, collettivamente denominati client TN3270.
- Il programma di reindirizzamento TN offre un accesso host TCP/IP pass-through ai client TN3270, TN3270E, TN5250 e VT, collettivamente denominati client Telnet.

Gateway SNA

Un gateway è un dispositivo trasparente per l'utente che connette reti o computer diversi, supportando entrambi gli ambienti connessi. Gli utenti finali possono comunicare come se risiedessero nella stessa rete.

Il gateway SNA consente ai computer CS/AIX di fungere da gateway di collegamento tra più computer in downstream in una rete SNA e una o più unità fisiche (Physical Unit PU) host, come illustrato nella Figura 1 a pagina 7. Per semplificare la connettività host ed eliminare i collegamenti in eccesso, il gateway SNA funge da concentratore di PU—tratta l'insieme dei computer come un'unica PU (che sembra risiedere sul nodo del gateway SNA) e comunica con l'host su un'unica connessione fisica.

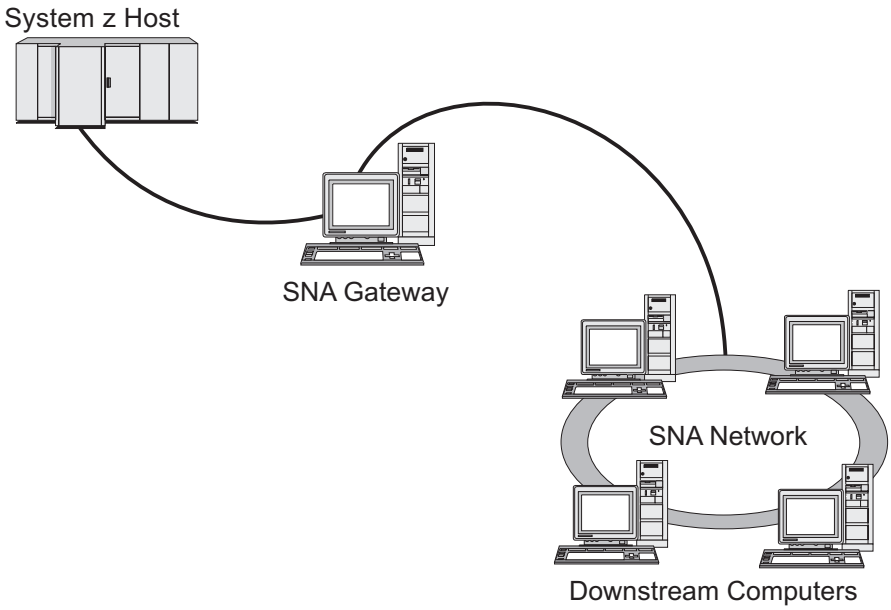

Figura 1. Gateway SNA che collega più computer AIX in downstream a un computer host

Supporto LU principale

Il supporto LU principale consente a un'applicazione AIX di controllare dispositivi LU dipendenti in downstream come se fosse un'applicazione mainframe host.

Generalmente, le applicazioni LUA si connettono ai mainframe host come LU secondarie, consentendo all'applicazione host di controllare la definizione delle sessioni e inviare il BIND per avviare una sessione. CS/AIX può inoltre fungere da LU principale per eseguire il downstream di dispositivi SNA dipendenti su una LAN, utilizzando l'interfaccia RUI principale. Mediante tale interfaccia, un'applicazione può connettere sessioni LU dipendenti in downstream senza che sia necessario un mainframe host.

Per utilizzare le applicazioni LU principali, il nodo deve essere configurato con LU di downstream (o un modello PU di downstream) che abbiano il nome LU host #PRIRUI#. Ciò indica al server che le applicazioni che utilizzano la RUI principale controllano tali PU e le risorse LU ad esse assegnate. Le PU possono essere utilizzate sia con le porte LAN che con le porte WAN. Consultare *IBM Communications Server for AIX o Linux LUA Programmer's Guide* per informazioni sulla programmazione delle applicazioni per l'utilizzo della RUI principale.

Branch Extender

I nodi di una rete APPN hanno la necessità di mantenere le informazioni sulla topologia (ossia sull'ubicazione di altri nodi nella rete e sui reciproci collegamenti di comunicazione) e di inoltrarle alla rete al mutare della topologia. Con l'aumento delle dimensioni della rete, la quantità di informazioni memorizzate e il traffico di rete legato alla topologia possono raggiungere dimensioni notevoli e diventare difficili da gestire.

Questi problemi possono essere evitati suddividendo la rete in sottoreti, affinché ciascun nodo debba mantenere solo le informazioni sulla topologia relative ai nodi della propria sottorete. Tuttavia, ciò comporta un maggiore traffico di rete nel momento in cui si cerca di localizzare le risorse in altre sottoreti.

La funzione Branch Extender di APPN, illustrata nella Figura 2, fornisce una soluzione a questi problemi.

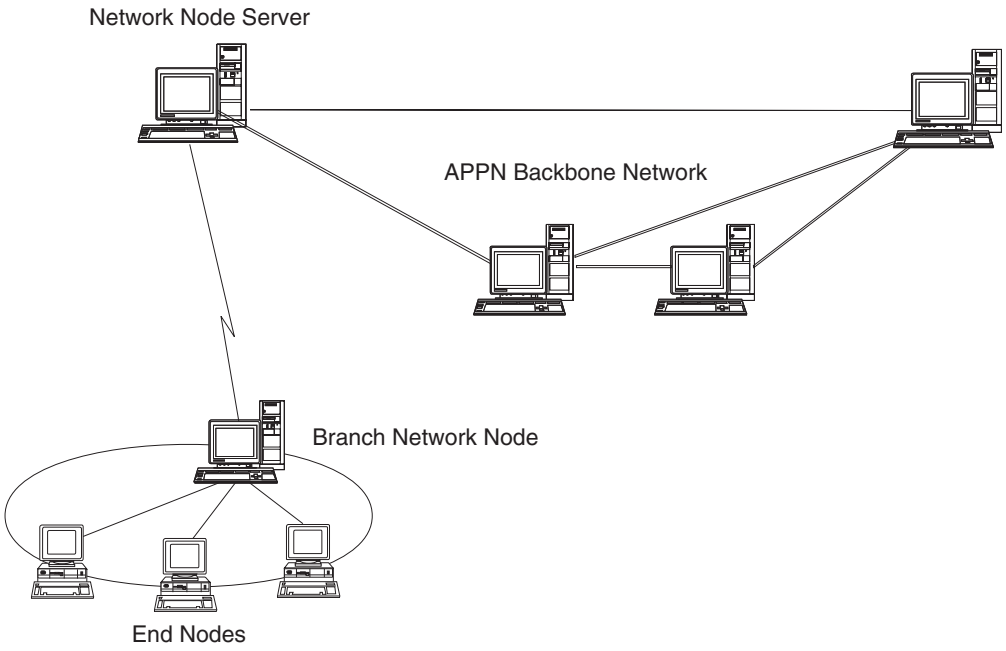

Figura 2. Branch Extender

Come lo stesso nome suggerisce, Branch Extender è progettato per le reti che possono essere suddivise in aree distinte, ad esempio le filiali distinte di una grande azienda. Questa funzione separa le filiali dalla rete backbone APPN principale (ad esempio, la rete della sede centrale di un'organizzazione).

Ciascuna filiale contiene un nuovo tipo di nodo chiamato Branch Network Node (BrNN), collegato a un nodo della rete backbone APPN principale. Il BrNN combina le funzioni di un nodo di rete APPN e di un nodo finale APPN.

- La rete backbone rileva il BrNN come un nodo finale connesso al proprio server nodo di rete (Network Node Server, NNS) all'interno della rete backbone:
  - I nodi della rete backbone non riconoscono i nodi nella filiale, il che riduce la quantità di informazioni sulla topologia da memorizzare.
  - Comparendo come nodo finale, il BrNN non riceve informazioni sulla topologia dalla rete backbone (tali informazioni vengono trasmesse solo tra i nodi di rete).
  - Il BrNN registra tutte le risorse della filiale con il proprio NNS, come se fossero ubicate nello stesso BrNN. Ciò significa che i nodi della rete backbone sono in grado di localizzare le risorse nella filiale senza doverne riconoscere i singoli nodi.
- La rete della filiale rileva il BrNN come un nodo di rete che funge da NNS per i nodi finali della filiale. Ciascun nodo della filiale rileva il resto della rete come se fosse connesso tramite il proprio NNS, analogamente a quanto accade con gli NNS standard.

APPC Application Suite

APPC Application Suite è un insieme di applicazioni che dimostra le funzionalità di elaborazione distribuita delle reti APPN e può essere utile per la verifica della configurazione e l'individuazione di problemi. APPC Application Suite può essere

utilizzato per fornire supporto durante alcune operazioni, ad esempio i trasferimenti di dati, spesso eseguite tramite la rete.

APPC Application Suite contiene le seguenti applicazioni:
- **ACOPY** (APPC COPY)
- **AFTP** (APPC File Transfer Protocol)
- **ANAME** (APPC Name Server)
- **APING** (APPC Ping)
- **AREXEC** (APPC Remote EXECution)
- **ATELL** (APPC TELL)

È possibile accedere a queste applicazioni da un server o da un client AIX o Windows.

Enterprise Extender

Enterprise Extender (noto anche come HPR/IP) fornisce un meccanismo per l'integrazione delle applicazioni SNA con una rete IP.

Le applicazioni SNA sono progettate per utilizzare protocolli SNA per la comunicazione con altre applicazioni SNA tramite reti SNA. Quando vengono installate in una rete TCP/IP che utilizza Enterprise Extender, le applicazioni SNA possono ancora comunicare; la funzione Enterprise Extender fornisce un meccanismo per il trasporto dei protocolli SNA sulla rete IP. In particolare, fornisce una funzionalità APPN HPR (High-Performance Routing) che offre alle applicazioni i vantaggi sia della connettività APPN che della connettività IP.

Enterprise Extender in CS/AIX viene implementato semplicemente come collegamento di comunicazione. Per connettere due applicazioni SNA su IP, occorre definire un collegamento Enterprise Extender in maniera analoga a qualsiasi altro tipo di collegamento quale SDLC o Ethernet.

Server TN

I programmi di emulazione 3270 che comunicano su TCP/IP (piuttosto che su una rete SNA) vengono denominati "programmi TN3270" (programmi di emulazione Telnet 3270).

I programmi TN3270 possono includere anche il supporto per TN3270E (estensioni standard Telnet 3270). TN3270E supporta l'emulazione di dispositivi 3270 (inclusi sia i terminali che le stampanti) che utilizzano Telnet. Consente a un client Telnet di selezionare un determinato dispositivo (specificando il nome LU o il nome di un pool di LU) e fornisce maggiore supporto per differenti funzioni, incluse le chiavi ATTN e SYSREQ e la gestione delle risposte SNA.

Nota: Questa guida utilizza il termine TN3270 per informazioni ugualmente applicabili ai protocolli TN3270, TN3287 e TN3270E.

Il server TN di CS/AIX fornisce l'accesso ai computer host 3270 agli utenti TN3270 che operano su altri computer. Il server TN consente agli utenti TN3270 di condividere una connessione host con CS/AIX o con altri utenti TN3270, invece di richiedere un collegamento diretto. Il server TN consente inoltre agli utenti TN3270 di accedere agli host che non eseguono TCP/IP.

La funzione del server TN di CS/AIX è illustrata nella Figura 3 a pagina 10.

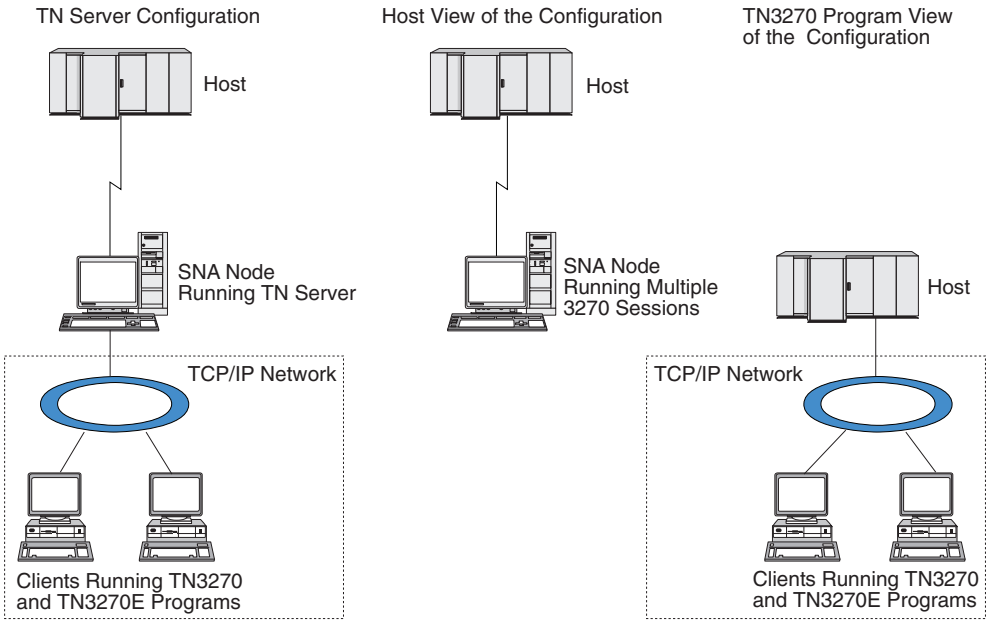

Figura 3. Server TN

La funzione del server TN di CS/AIX fornisce un collegamento tra un utente TN3270 e la LU 3270 di CS/AIX. Tutti i dati provenienti dall'utente TN3270 vengono instradati alla LU. Ciò significa che la configurazione dell'host e dell'utente TN3270 è la stessa che si presenterebbe se fossero direttamente connessi e non necessita del rilevamento dell'instradamento dei dati tramite il server TN.

Il server TN di CS/AIX supporta tutti i programmi di emulazione dei client TN3270 che implementano correttamente i protocolli definiti dalla IETF nelle RFC 1123, 1576, 1646, 1647 e 2355.

Funzioni di sicurezza: Il server TN di CS/AIX supporta la crittografia dati, l'autenticazione del server, l'autenticazione del client e la funzione di accesso rapido Express Logon, tramite software SSL (Secure Sockets Layer):

- La crittografia dati indica che i dati scambiati tra il server TN e l'emulatore TN3270 vengono trasmessi in forma crittografata.
- L'autenticazione del server consente a un client TN3270 di verificare che il server TN al quale è connesso sia quello previsto.
- L'autenticazione del client consente al server TN di verificare che il client TN3270 che si sta connettendo sia quello previsto. Il server TN può anche controllare un elenco di revoche su un server di directory esterno per verificare che l'autorizzazione del client non sia stata revocata.
- Express Logon opera congiuntamente all'autenticazione del client per eliminare la necessità per i client TN3270 di fornire un ID utente e una password durante il collegamento con l'host. Il certificato di sicurezza del client viene utilizzato, invece, per recuperare le informazioni necessarie relative a ID utente e password.

Queste funzioni sono disponibili solo in AIX 4.3.1 e versioni successive e richiedono dei software aggiuntivi oltre al prodotto CS/AIX standard. Per ulteriori informazioni, consultare "Requisiti di installazione" a pagina 20.

Service Location Protocol (SLP): Il server TN di CS/AIX supporta anche SLP (Service Location Protocol) che fornisce funzioni di individuazione dei servizi e bilanciamento del carico. Se si utilizza SLP, ciascun server TN indica:

- le funzioni supportate (in questo caso TN3270)
- il carico corrente; quest'ultimo è basato sulla percentuale di LU host disponibili attualmente in uso, ma può essere calcolato per consentire altre differenze tra server TN.

Un client TN3270 con supporto SLP può quindi selezionare il server "migliore" cui collegarsi (il server con il minor carico, in grado di fornire le funzioni richieste). Per far ciò, interroga direttamente i server TN oppure il directory agent che, a sua volta, raccoglie le informazioni notificate dai server TN.

Un'ampia rete SLP può essere suddivisa in più "ambiti" (solitamente per reparto o area geografica), affinché le informazioni su un server TN siano notificate solo ai client TN3270 e ai directory agent aventi lo stesso ambito del server TN. Ciò consente di controllare l'intervallo di client TN3270 che possono utilizzare i servizi di ciascun server TN.

Nota: Il server su cui viene eseguito il server TN deve supportare l'indirizzamento IPv4, ossia deve avere un indirizzo IPv4 (benché possa avere anche un indirizzo IPv6). Ciò perché SLP utilizza trasmissioni UDP non disponibili in un'installazione che supporta solo IPv6.

Programma di reindirizzamento TN

Il programma di reindirizzamento TN di CS/AIX fornisce servizi pass-through per le sessioni 3270, 5250 o VT su TCP/IP. L'utente Telnet comunica con CS/AIX su una connessione TCP/IP; CS/AIX quindi comunica con l'host su un'altra connessione TCP/IP.

Il programma di reindirizzamento TN di CS/AIX supporta la crittografia dati, l'autenticazione del server e l'autenticazione del client tramite software SSL (Secure Sockets Layer), in maniera analoga al server TN per 3270. Ciò consente l'utilizzo del controllo di sicurezza SSL (Secure Sockets Layer) laddove necessario e non su tutta la connessione utente-host. Ad esempio:

- Se i client si connettono a CS/AIX tramite una LAN TCP/IP in cui il controllo non è richiesto e a un host remoto che invece richiede SSL, è possibile utilizzare SSL sulla connessione TCP/IP tra CS/AIX e l'host. Ciò significa che viene effettuato un controllo di sicurezza unico per tutti i client e che i singoli client non devono fornire informazioni sulla sicurezza.
- Se CS/AIX e l'host sono installati nella stessa ubicazione, mentre i client accedono da siti esterni, è possibile utilizzare SSL sulle connessioni tra client e CS/AIX senza dover installare il software SSL sull'host.

Funzioni e vantaggi

CS/AIX offre una vasta gamma di funzioni e vantaggi, ad esempio consente di semplificare la configurazione, migliorare la diagnostica e aumentare le prestazioni della rete.

Blocchi di creazione versatili

CS/AIX supporta la maggior parte degli ambienti e delle funzioni dei nodi. In qualsiasi tipo di rete, sottoarea o APPN, consente al computer AIX di operare come uno qualsiasi, o come una combinazione, dei seguenti nodi:

- Nodo dipendente dall'host
- Nodo peer (per una descrizione dei nodi peer APPN, consultare l'analisi sulle reti peer-to-peer in "IBM Communications Server for AIX V6.4" a pagina 1)
- Nodo partner (di origine o di destinazione) nelle applicazioni distribuite
- Nodo gateway che interconnette reti SNA
- Nodo gateway che interconnette reti SNA e TCP/IP

Tramite le API di gestione delle reti, il computer AIX può anche essere configurato in modo tale da fungere da punto di ingresso MS (Management Services) per fornire supporto alla gestione delle reti distribuite. A livello di collegamento, il computer AIX può essere connesso a varie LAN e WAN tramite una qualsiasi delle tipologie supportate (descritte in "IBM Communications Server for AIX V6.4" a pagina 1 e "Requisiti di installazione" a pagina 20).

Funzionamento client/server

La configurazione client/server offre i seguenti vantaggi:

- La concentrazione delle risorse SNA nei server diminuisce il carico sui client, migliorando le prestazioni dei client e riducendo al minimo la memorizzazione necessaria per fornire servizi SNA ai client.
- Più utenti possono condividere un unico collegamento dati in macchine diverse, eliminando la necessità di disporre di una connessione di rete SNA fisica su ogni macchina.
- I server multipli possono fornire una connettività ridondante (ad esempio, più server che forniscono accesso allo stesso host). Disporre di più percorsi verso una risorsa SNA consente di bilanciare il carico tra differenti server e offre un backup immediato in caso di errore di un determinato server o collegamento.
- L'utilizzo di pool di LU in più server consente all'amministratore di configurare e aggiungere agevolmente server e utenti.
- Una minore quantità di collegamenti e PU per la connettività host riduce la dimensione della definizione del VTAM dell'host.
- Le utilità di gestione possono essere utilizzate per configurare e gestire sia le risorse dei nodi (relativamente a qualsiasi computer del dominio), sia le risorse condivise. Il supporto client/server offerto dagli strumenti di gestione di CS/AIX consente una gestione trasparente di tutte le risorse del dominio da uno qualunque dei computer del dominio.
- Le applicazioni SNA possono essere connesse su IP (Internet Protocol) tramite TCP/IP e HTTPS per attraversare i firewall e per ragioni di autenticazione e sicurezza.

Configurazione semplice

CS/AIX è progettato con funzionalità e opzioni di configurazione atte a ridurre i tempi di configurazione e la complessità della rete. Ad esempio:

Programma di gestione Motif

Il modo più facile per definire e modificare la configurazione di CS/AIX è utilizzare il programma di gestione Motif (**xsnaadmin**). Questo programma fornisce una GUI da cui è possibile visualizzare e gestire le risorse di CS/AIX. Inoltre, questo programma semplifica la configurazione mostrando solo i campi i cui valori solitamente variano da un'installazione all'altra, utilizzando valori predefiniti per gli altri campi.

Il programma di gestione Motif include schermate della guida che forniscono informazioni riepilogative su SNA e CS/AIX, informazioni di riferimento sulle finestre di dialogo di CS/AIX e una guida per l'esecuzione di attività specifiche.

Programma di gestione Web
CS/AIX include anche un programma di gestione Web che fornisce funzioni analoghe a quelle del programma di gestione Motif. Il programma permette di gestire CS/AIX dal proprio browser senza dover avviare una sessione X o una sessione Telnet nel server CS/AIX ed è particolarmente utile in caso di connessione su collegamenti lenti o inaffidabili.

Configurazione dinamica nelle reti APPN
La configurazione di un nodo o di una rete viene semplificata anche tramite la configurazione dinamica delle reti APPN. Ad esempio, i nodi finali e le applicazioni APPN registrano i dati di configurazione in maniera dinamica per supportare le sessioni LU 6.2, rendendo così facoltativa la configurazione della sessione. Inoltre, con il punto di controllo del nodo che funge da LU locale predefinita, è possibile evitare del tutto la configurazione della LU 6.2.

In assenza di stazioni di collegamento configurate, l'APPN supporta anche la configurazione delle stazioni di collegamento dinamiche.

Ulteriori opzioni di gestione dell'interfaccia utente

Il programma di gestione Motif è l'interfaccia consigliata per la configurazione e la gestione di CS/AIX. Tuttavia, sono disponibili differenti interfacce per CS/AIX, che consentono all'utente di operare con quella più adatta alle proprie apparecchiature, esigenze e preferenze.

Programma di gestione da riga comando
Il programma di gestione da riga comando (**snaadmin**) può essere utilizzato per emettere comandi per la gestione delle singole risorse di CS/AIX. È possibile utilizzare **snaadmin** direttamente dal prompt dei comandi AIX o da uno script shell.

Programma di gestione Web
Il programma di gestione Web consente di gestire CS/AIX dal proprio browser.

System Management Interface Tool (SMIT)
L'interfaccia SMIT è disponibile nella versione grafica Motif per ambienti AIX e Windows e nella versione a caratteri per terminali ASCII. In entrambe le versioni, SMIT visualizza finestre di dialogo per l'immissione agevole di dati di configurazione e dati operativi.

API NOF
L'API NOF di CS/AIX offre le stesse funzioni gestionali del programma di gestione da riga comando, fornendo un'interfaccia adatta ad essere utilizzata all'interno di un programma (invece di uno script di comandi). L'API NOF può essere utilizzata per scrivere le proprie applicazioni di gestione di CS/AIX.

Migliori prestazioni

CS/AIX migliora ulteriormente le prestazioni già elevate delle reti SNA e utilizza classi di servizio. CS/AIX ottimizza anche la velocità della rete mediante la

compressione dei dati SNA per i dati della sessione LU 0–3 e tramite diversi metodi di gestione del traffico che ne bilanciano il flusso in base alle dimensioni della rete:

- Nelle reti APPN, CS/AIX supporta sia l'instradamento HPR (High-Performance Routing) che l'instradamento ISR (Intermediate Session Routing) e fornisce opzioni relative alla rete di connessione. Benché sia efficiente con le piccole reti, l'ISR riduce le prestazioni delle reti più ampie.
- In caso di reti più ampie che utilizzano le opzioni della connettività LAN (ad esempio, Token Ring o Ethernet) o Enterprise Extender, è possibile migliorare l'efficienza delle comunicazioni anche tramite l'opzione della rete di connessione. L'opzione della rete di connessione crea un percorso di comunicazione diretto tra nodi. Ciò consente al traffico di aggirare i nodi di rete intermedi.
- Un altro meccanismo di controllo del traffico, il pacing adattivo a livello sessione, adegua automaticamente la congestione della rete regolando la velocità di invio delle unità di messaggio dalle LU alle LU partner.

Opzioni di sicurezza

Con la creazione di reti sempre più complesse e tendenti a un'architettura aperta, i problemi collegati alla sicurezza diventano centrali. Nelle reti SNA che eseguono CS/AIX, è possibile proteggere le proprie risorse definendo vari livelli di sicurezza tramite la configurazione e implementando alcuni tipi di collegamento. Ad esempio:

- In un sistema client/server, è possibile impostare un server WebSphere per fornire l'accesso HTTPS dai client API remoti ai server. Ciò significa che le connessioni dei client vengono autenticate mediante certificati di sicurezza (questa funzione richiede dei software aggiuntivi oltre al prodotto CS/AIX standard. Per ulteriori informazioni, consultare "Requisiti di installazione" a pagina 20).
- Gli utenti LU 6.2 possono definire fino a tre livelli di sicurezza: sessione, risorsa e conversazione. Nell'ordine, il primo garantisce che a una sessione partecipino solo le LU appropriate, la seconda restringe l'accesso a tutte le applicazioni associate ad una determinata LU e l'ultimo restringe l'accesso a una determinata applicazione. È possibile ottenere livelli superiori di sicurezza tramite le routine di crittografia dati.
- A livello di collegamento, la fibra ottica fornisce ulteriore protezione poiché si tratta di un mezzo che (a differenza del cablaggio elettrico) non perde segnali e quindi difficilmente può essere intercettato.
- Il server TN e il programma di reindirizzamento TN di CS/AIX sono in grado di fornire la crittografia dati, l'autenticazione del server e l'autenticazione del client tra il server CS/AIX e i client Telnet o i client TN3270 tramite software SSL (Secure Sockets Layer) (questa funzione richiede dei software aggiuntivi oltre al prodotto CS/AIX standard. Per ulteriori informazioni, consultare "Requisiti di installazione" a pagina 20).

Flessibilità nella gestione della rete

CS/AIX utilizza due tipi di modelli di gestione della rete:

- Multiple Domain Support-Network Management Vector Transport (MDS-NMVT) può fungere da modello di gestione centralizzata, distribuita o gerarchica. È basato su un'architettura punto centrale/punto di ingresso in grado di fornire un elevato livello di flessibilità.

  I punti centrali sono nodi di controllo che gestiscono la rete in base ai dati raccolti dai punti di ingresso (applicazioni di gestione che risiedono in tutti gli altri nodi della rete).

  - Nella gestione centralizzata, un unico punto centrale funge da punto di controllo per tutta la rete.
  - Nella gestione distribuita, più punti centrali condividono la gestione della rete.
  - Nella gestione gerarchica, i punti centrali sono nidificati in base alla funzione.

  MDS-NMVT può pertanto essere adattato alla gestione di una sottoarea, di una rete APPN standard e di reti APPN di notevoli dimensioni.
- Simple Network Management Protocol-Management Information Base (SNMP-MIB), adatto per le reti APPN da TCP/IP, rappresenta un servizio di gestione distribuita basato su un'architettura gestore-agente. Questo modello di gestione è formato da vari componenti: uno o più agenti SNMP, un gestore e un database MIB, tutti disposti solitamente su nodi differenti.
  - Un agente SNMP è un processo in esecuzione nel sistema gestito, del quale monitora lo stato. L'agente aggiorna un database MIB per quel sistema.
  - Il gestore (un'applicazione) interroga l'agente per ricevere informazioni MIB ed elabora la risposta. Il gestore può ricevere anche dati non richiesti (trap SNMP) dall'agente. Il gestore e l'agente comunicano tra loro mediante il protocollo SNMP.

  I gestori della rete APPN possono utilizzare SNMP-MIB APPN per raccogliere informazioni allo scopo di analizzare la rete e correggere gli eventuali problemi.

  CS/AIX utilizza un software agente che supporta MIB APPN. Per ulteriori informazioni su MIB APPN, consultare *IBM Communications Server for AIX Administration Guide* e la home page di IBM AIW all'indirizzo http://www.networking.ibm.com/app/aiwhome.htm.

Affidabilità, disponibilità e livello di servizio

Per garantire l'affidabilità del sistema, CS/AIX fornisce una serie di funzioni di visualizzazione e strumenti di diagnostica.

- Il programma di gestione Motif fornisce strumenti di configurazione e gestione avanzati, tra cui:
  - Aggiornamenti immediati delle informazioni relative alla configurazione
  - Informazioni sullo stato di collegamenti, sessioni e risorse dei nodi
- I comandi query e i comandi di stato forniscono informazioni su:
  - Sessioni LU-LU
  - Sessioni intermedie APPN
  - Collegamenti attivi
  - Database di topologia APPN che memorizzano le informazioni sui collegamenti
- Sono disponibili strumenti diagnostici per aiutare l'utente durante le differenti fasi di configurazione e funzionamento. Essi includono:
  - Strumento di raccolta delle informazioni diagnostiche (**snagetpd**) che consente di raccogliere con facilità le informazioni sul servizio
  - Messaggi di stato e di errore per agevolare la risoluzione di problemi relativi alle routine di configurazione e al funzionamento del sistema
  - Registri per la raccolta di informazioni su errori di rete, malfunzionamenti e controlli
  - Funzioni di traccia per la raccolta e la formattazione di informazioni dettagliate relative ai problemi riscontrati

Altre utilità aiutano l'utente a verificare la connettività dei collegamenti e le comunicazioni tra le applicazioni.

CS/AIX include anche l'API MS (Management Services), utilizzata per sviluppare strumenti per l'invio e la ricezione di avvisi di rete e di dati relativi ai problemi.

Tutti questi strumenti per la diagnosi e la gestione sono completamente integrati nel modello client/server CS/AIX, pertanto è possibile gestire tutto il dominio CS/AIX o raccogliere informazioni diagnostiche da un unico punto della rete.

Integrazione, ampliamento e modifica della rete

Per supportare l'integrazione, l'ampliamento e la modifica della rete, le API di CS/AIX possono essere utilizzate per sviluppare applicazioni per una LU, una piattaforma o un sistema operativo specifici in base alle proprie esigenze aziendali. CPI-C è un'API particolarmente importante, poiché è compatibile con diverse piattaforme e sistemi operativi. Viene utilizzata per sviluppare applicazioni che possono essere eseguite su qualsiasi sistema.

Enterprise Extender fornisce anche un meccanismo per l'integrazione delle reti SNA e TCP/IP.

Capitolo 2. Pianificazione della rete e IBM Communications Server for AIX

Questo capitolo offre una panoramica delle fasi di pianificazione di una rete che esegue CS/AIX. Inoltre, riepiloga le funzioni configurabili per il computer AIX e presenta delle indicazioni per la stima delle risorse richieste per supportare tali funzioni.

Fasi della pianificazione della rete

Questa sezione presenta alcune indicazioni generali per la pianificazione, la configurazione e la gestione delle reti mediante l'utilizzo di varie utilità di CS/AIX e AIX.

La pianificazione di una rete implica il bilanciamento di funzioni, prestazioni, risorse e costi. Benché non esista una sola pianificazione perfetta per una determinata rete, alcune tecniche e indicazioni generali possono aiutare a garantire che la pianificazione risponda alle proprie esigenze. Per pianificare una rete, attenersi alla seguente procedura:

- Stabilire le funzioni che devono essere fornite dalla rete (come ad esempio il trasferimento di file o l'emulazione 3270) e le proprie esigenze in termini di prestazioni.
- Stabilire come deve essere configurato CS/AIX per fornire le funzioni desiderate.
- Stimare le risorse necessarie per installare CS/AIX, soddisfare i propri requisiti in termini di prestazioni e funzionalità e supportare le funzioni di CS/AIX, quindi individuarne i costi.

Identificazione dei requisiti funzionali della rete

Per determinare quali funzioni dovranno essere fornite dalla rete, è necessario porsi le seguenti domande:

- È necessario eseguire applicazioni APPC su una rete TCP/IP?
- La rete deve essere una rete APPN?
- CS/AIX verrà eseguito come sistema client/server? In caso affermativo, i computer opereranno tutti in un unico dominio CS/AIX o è necessario definire due o più domini distinti?
- Sono necessari più server nel dominio CS/AIX per fornire un bilanciamento del carico delle risorse di connettività? In caso affermativo, quale server fungerà da server master per la configurazione? È necessario fornire uno o più server di backup per la configurazione?
- È necessario supportare i client API remoti che si connettono ai server CS/AIX tramite HTTPS?
- Le applicazioni degli utenti verranno eseguite sul server o sui computer client AIX?
- Il server fornirà risorse di connettività per le applicazioni Windows (come ad esempio i programmi di transazioni API) in esecuzione sui client Windows?
- Ciascun server costituisce un endpoint delle sessioni o deve essere uno dei seguenti tipi di gateway?
  - APPN
  - LU 0

  - LU 2
  - Server TN o programma di reindirizzamento TN
- Quali tipi di collegamenti fisici verranno utilizzati dalla rete?
- CS/AIX dovrà supportare IPv4, IPv6 o entrambi i tipi di connessione?

Le risposte a domande di questo tipo consentono di determinare le funzioni CS/AIX richieste dalla rete.

Determinazione della configurazione di CS/AIX

Per stabilire la modalità di funzionamento di CS/AIX, è necessario innanzitutto decidere in che modo il lavoro fluirà nella rete. È necessario considerare le seguenti domande:

- Quali risorse (come ad esempio le applicazioni) devono essere rese disponibili attraverso la rete?
- Quanti utenti devono accedere a risorse remote?
- Con quale frequenza viene effettuato l'accesso a ciascuna risorsa?
- In che modo gli utenti hanno accesso alla rete?
- In che modo le richieste degli utenti verranno instradate nella rete?

CS/AIX può essere configurato per supportare numerose funzioni tra cui:

- Nodo di rete APPN per ISR (Intermediate Session Routing)
- Nodo finale APPN (che comunica in maniera autonoma con i nodi adiacenti, ma utilizza servizi dei nodi di rete APPN per comunicare con i nodi peer non adiacenti)
- Nodo LEN (Low-Entry Network)(che comunica direttamente con i nodi adiacenti o con i nodi configurati per sembrare adiacenti)
- Emulazione del terminale host tramite LU 2
- Utilizzo di LU 0, LU 1, LU 2, LU 3 e LU 6.2 (dipendenti e indipendenti)
- Connessione dal gateway SNA a un host

A seconda delle esigenze, è possibile configurare una o più funzioni per un dato nodo. Ad esempio, è possibile configurare CS/AIX come nodo di rete APPN per la fornitura di servizi di instradamento e ISR ed utilizzare lo stesso nodo per l'instradamento di sessioni LU dipendenti, quali LU 0 e LU 2, da parte del gateway SNA. Analogamente, è possibile configurare CS/AIX perché esegua il server TN e supporti un database condiviso, nonché una connessione LU 6.2 indipendente a MQSeries sull'host.

Identificazione dei requisiti delle risorse per l'installazione e il funzionamento

Per stimare il supporto necessario per le funzioni di CS/AIX, occorre rispondere alle seguenti domande:

- Quali competenze del personale sono necessarie?
- Quale modello di stazione di lavoro AIX è necessario?
- Quale modalità di trasporto si prevede di utilizzare?
- Quali requisiti per l'installazione devono essere selezionati per la configurazione?
- Quanta memoria e spazio di paginazione sono necessari per il funzionamento?
- In base al livello di traffico stimato, qual è il tempo di risposta previsto?

La risposta a queste domande può aiutare l'utente a identificare i tipi di risorsa utilizzati da CS/AIX quando viene configurato per supportare una o più delle numerose funzioni descritte in "Identificazione dei requisiti funzionali della rete" a pagina 17. La risposta a tali domande aiuta inoltre a capire la relazione tra le funzioni di CS/AIX, le risorse di AIX e le risorse di rete.

La modalità di allocazione delle risorse ai nodi determina le prestazioni della rete.

Requisiti del personale

L'installazione, il funzionamento e la messa a punto di CS/AIX richiedono le seguenti figure professionali:

- Amministratori di rete, che pianificano la rete, aggiungono nuovi dispositivi e mantengono o incrementano le prestazioni generali della rete
- Amministratori di sistema, che installano e si occupano della manutenzione di CS/AIX e dell'hardware su cui opera e che configurano i sistemi per la connessione di rete
- Programmatori, che sviluppano applicazioni personalizzate quali i programmi di transazioni o le routine di gestione della rete

Gli amministratori di rete e di sistema devono essere particolarmente esperti dell'hardware su cui opera CS/AIX e del sistema operativo AIX. Devono conoscere le reti cui sono connessi i vari sistemi e comprendere i concetti delle reti SNA in generale. Inoltre, devono avere dimestichezza con quanto segue:

- L'interfaccia Motif o SMIT (System Management Interface Tool) for AIX
- TCP/IP, se prevedono di utilizzare le funzioni client/server, il server TN, Enterprise Extender o AnyNet
- Il sistema operativo Linux, se il sistema CS/AIX include Remote API Client su Linux
- Windows 2000, Windows XP, Windows 2003 Server, Windows Vista o il sistema operativo Windows Server 2008, se il sistema CS/AIX include Remote API Client su Windows
- WebSphere Application Server, se il sistema CS/AIX include client API remoti che si collegano ai server tramite HTTPS

I programmatori che sviluppano applicazioni personalizzate per SNA devono essere esperti di linguaggio C (o Java se utilizzano CPI-C Java) e devono avere dimestichezza con le API disponibili su CS/AIX.

Modelli di IBM eServer pSeries

IBM Communications Server for AIX è progettato per essere eseguito in una stazione di lavoro AIX connessa a una o più reti. CS/AIX V6.4 verrà eseguito su qualsiasi sistema IBM RISC System/6000 o eServer pSeries supportato da AIX Versione 5.2, 5.3 o 6.1 (per AIX V6.1, il server deve essere eseguito nell'ambiente globale, non in una WPAR - partizione del carico di lavoro - del sistema o dell'applicazione).

Le stazioni di lavoro IBM pSeries sono disponibili in numerosi modelli con differenti capacità di memoria, spazio su disco, schede I/O e velocità della CPU. I pacchetti disponibili sono i seguenti:

- Modelli BladeCenter, ad esempio JS20. I modelli BladeCenter sono quelli con minore capacità di memoria, unità disco e schede I/O (ad esempio Ethernet). Sono particolarmente indicati come client o sistemi endpoint.
- Modelli in formato deskside o rack, quali il p5 520. I modelli in formato deskside e rack hanno maggiore capacità di memoria, unità disco e schede I/O.

Sono indicati per server di piccole o medie dimensioni o per ambienti multiutente. Alcuni di questi sistemi possono anche essere suddivisi in partizioni logiche (LPAR) per creare più istanze SO nello stesso hardware.

- Modelli a telaio, quali il p5 590. I modelli a telaio hanno la maggiore capacità di memoria, disco e funzionalità I/O e sono indicati per server di grosse dimensioni o gli ambienti multiutente. Questi modelli possono anche essere suddivisi in partizioni logiche (LPAR).

Per informazioni sulla rispettiva velocità della CPU dei differenti sistemi IBM eServer pSeries, consultare http://www.ibm.com.eserver/pseries.

Mezzi di trasporto

CS/AIX potrebbe dover condividere il mezzo di trasporto sottostante (come ad esempio SDLC o Token Ring) con altri protocolli di comunicazione. Pertanto, i requisiti di larghezza di banda del livello fisico devono soddisfare tutti i protocolli e le applicazioni che condividono il mezzo di trasporto.

Nota: CS/AIX può condividere le schede Token Ring, Ethernet e X.25 con altri protocolli quali il TCP/IP. Potrebbe essere necessario specificare gli indirizzi di punti di accesso al servizio (SAP, Service Access Point) univoci per ciascun protocollo da utilizzare. CS/AIX può anche condividere una scheda MPQP (Multiprotocol Quad Port) , ma non una porta MPQP.

Requisiti di installazione

Le funzioni assegnate a CS/AIX (da "Identificazione dei requisiti funzionali della rete" a pagina 17) determinano anche i requisiti di installazione. Questa sezione fornisce una panoramica delle risorse del computer richieste per l'installazione di CS/AIX. Per ulteriori informazioni, consultare la documentazione fornita con ciascun prodotto (vedere la Bibliografia per un elenco dei libri).

Hardware di collegamento

L'hardware di collegamento è necessario solo sui server e non sui client.

L'installazione di una stazione di lavoro AIX o Power Series in una o più reti richiede che i collegamenti siano conformi al protocollo di comunicazione della rete selezionata. L'hardware di collegamento è formato da una scheda di comunicazione installata nel computer e dal cavo corrispondente per l'attacco alla rete (è necessario anche il software del driver del dispositivo).

Nota:

1. Le schede di comunicazione devono essere installate con i cavi corrispondenti. Ad esempio, affinché il collegamento funzioni, con una scheda Ethernet è necessario un cavo Ethernet.
2. Se si utilizza Enterprise Extender come unico tipo di collegamento o se si utilizza solo la funzione APPC AnyNet over TCP/IP di CS/AIX, le schede elencate in questa sezione non sono necessarie, ma occorre una delle schede richieste da TCP/IP di AIX.

CS/AIX supporta le schede di comunicazione relative ai seguenti protocolli di collegamento:

- Token Ring
- Ethernet (standard o IEEE 802.3)
- SDLC
  - IBM PCI a 2 porte

– IBM MPQP a 4 porte

I seguenti protocolli di collegamento richiedono ulteriori prodotti o funzioni che non sono inclusi in CS/AIX:

- X.25 (richiede il prodotto AIXLink/X.25)
- ATM che utilizza un'interfaccia LAN emulata (Token Ring o Ethernet) su una scheda ATM di IBM AIX
- Frame Relay che utilizza un'interfaccia Token Ring emulata

Per ulteriori informazioni sulle schede verificate con CS/AIX, consultare http://www.ibm.com/software/network/commserver/about/comp_products/adapter_csaix.html. Per eventuali domande sulla scheda o l'hardware più adatti alle proprie esigenze, contattare il rivenditore IBM.

Software: server AIX

Prima di installare ed utilizzare CS/AIX sulla propria stazione di lavoro AIX, quest'ultima deve necessariamente disporre del seguente software:

- Una delle seguenti versioni del sistema operativo di base (BOS, Base Operating System) di AIX:
  - AIX v5.2–ML7 o successivo
  - AIX v5.3–ML3 o successivo
  - AIX 6.1 o successivo
- Supporto DLC adeguato (non necessario per l'installazione, bensì per l'utilizzo di CS/AIX). Per ulteriori informazioni sulle DLC, consultare "Installazione delle serie di file DLC (Data Link Control)" a pagina 31.
- Supporto Motif di livello 1.2 (parte integrante del sistema operativo di base di AIX, necessario se si desidera utilizzare le funzioni SSL (Secure Sockets Layer) del server TN e/o del programma di reindirizzamento TN di CS/AIX o se si desidera utilizzare il programma di gestione Motif).
- Software Java (richiesto se si intende utilizzare CPI-C Java). L'ultimo SDK Java, disponibile all'indirizzo http://www.ibm.com/developerworks/java/jdk, soddisfa tutti i requisiti.

  Installare il pacchetto SDK Java con il comando **installp**.
- L'opzione **bos.64bit** di AIX è un prerequisito se si desidera avviare delle applicazioni tramite le API di CS/AIX in modalità a 64 bit. Questa opzione deve essere non solo installata, ma anche configurata mediante il comando **smit load64bit**, al fine di garantire che venga caricata prima di tentare di avviare le applicazioni a 64 bit. Se si desidera compilare e collegare applicazioni a 64 bit su questo computer, eseguendole tuttavia su un altro computer (ad esempio se si utilizzano due computer distinti per lo sviluppo e la verifica delle applicazioni), l'opzione **bos.64bit** non è necessaria.
- Un server Web che supporta servlet Java (necessari per il programma di gestione Web). IBM HTTP Server (IHS) v6.0.1 è stato testato con CS/AIX.

  Se si intende utilizzare un altro server Web o se si installa uno di questi server Web dopo aver installato CS/AIX, sarà necessario impostare dei collegamenti tra le directory di CS/AIX e quelle del server Web. Per ulteriori informazioni, consultare "Configurazione di un server Web per il programma di gestione Web" a pagina 40 (se uno o più dei server Web summenzionati è già installato, il processo di installazione di CS/AIX imposta automaticamente i collegamenti necessari).

- Un browser Web che supporta Java (necessario per il programma di gestione Web). I seguenti browser Web sono stati testati con CS/AIX:
  - Microsoft Internet Explorer v4 SP1 o successivo
  - Netscape Navigator v4.06 o successivo

WebSphere Application Server (per l'accesso HTTPS)
Se si intende eseguire un sistema client/server in cui i client API remoti si connettono ai server CS/AIX tramite HTTPS, sarà necessario eseguire il WebSphere Application Server per fornire l'accesso HTTPS da questi client ai server.

CS/AIX opera con WebSphere Application Server Version 5, che può essere installato su un computer che esegue qualsiasi sistema operativo supportato da WebSphere (se necessario, può essere installato nello stesso computer AIX in cui si trova il server CS/AIX). Per ulteriori informazioni sull'installazione, consultare la documentazione di WebSphere Application Server. Sarà altresì necessario installare su questo computer un ulteriore plug-in di CS/AIX per poter utilizzare WebSphere con CS/AIX, così come descritto in "Configurazione di WebSphere Application Server" a pagina 37.

Memoria e memorizzazione
Per supportare una gamma completa di configurazioni e servizi, ad una stazione di lavoro che esegue CS/AIX occorrono la memoria minima richiesta dal sistema operativo AIX più 64 MB e 200 MB di spazio libero su disco. Inoltre, durante l'installazione sono necessari 250 MB di memoria temporanea.

I messaggi e i testi della guida vengono forniti in differenti versioni in lingua nazionale. È necessario installare le serie di file relative ad almeno una lingua nazionale ma, se desiderato, è possibile installare più di una lingua. Per ogni lingua occorrono da 2,5 a 4 MB di spazio libero su disco (la dimensione varia in base alla lingua).

Se si decide di installare la documentazione relativa a CS/AIX in formato elettronico (PDF) occorre ulteriore spazio su disco fisso. Anche in questo caso, sono disponibili differenti versioni in lingua nazionale. Per installare i manuali nella lingua Inglese (Stati Uniti) occorrono 28 MB di spazio libero su disco e fino a 17 MB per ogni ulteriore versione linguistica.

Nota: I presenti requisiti non includono i requisiti di memoria e di spazio libero su disco fisso concernenti altri programmi concessi in licenza, applicazioni utente e dati; verificare attentamente tutti i requisiti di sistema, memoria e spazio libero su disco fisso con il rappresentante o il rivenditore IBM autorizzato.

Configurazioni avanzate

Se si prevede di eseguire applicazioni che richiedono più di una configurazione di base, occorre pianificare risorse aggiuntive per il computer.

In generale, i requisiti di memoria e memorizzazione per l'esecuzione di CS/AIX dipendono da numerosi fattori che variano in base alla funzione della stazione di lavoro AIX e al suo ambiente. Tuttavia, partendo dalla regola empirica che le LU, i collegamenti attivi e le sessioni in corso sono gli elementi che consumano maggiormente le risorse dei computer, è possibile stimare la quantità di ulteriore memoria e spazio libero su disco richiesti per supportare le applicazioni più esigenti.

Per ulteriori informazioni sull'utilizzo, l'allocazione e l'ottimizzazione delle risorse rispetto alla funzione del nodo, consultare http://www.ibm.com/software/network/commserver.

Requisiti di memoria e memorizzazione per il funzionamento

Questa sezione descrive i requisiti di memoria e memorizzazione di una stazione di lavoro che esegue CS/AIX.

Buffer di memoria (mbuf)

AIX utilizza i buffer di memoria (mbuf, memory buffer) per consentire la comunicazione tra i sottosistemi di comunicazione e i DLC di AIX. Il pool mbuf è una risorsa condivisa che deve essere gestita a livello di sistema. CS/AIX utilizza gli mbuf per inviare e ricevere dati lungo la rete, ma non è l'unico sottosistema che li utilizza. L'utilizzo della risorsa mbuf da parte di CS/AIX può influenzare le prestazioni di altri sottosistemi, quali TCP/IP, NFS o DCE. Coordinarsi col proprio amministratore di rete per la determinazione dei requisiti mbuf.

Memoria, disco e memoria di paginazione

CS/AIX utilizza la memorizzazione principale — conosciuta anche come memoria principale o memoria ad accesso casuale (RAM, Random Access Memory) —, lo spazio su disco permanente e la memoria di paginazione su disco (nota anche come spazio di paginazione):

- I blocchi di controllo per le risorse SNA — come ad esempio le LU, i collegamenti e le sessioni — consumano memoria principale.
- I buffer di memoria consumano solo memoria principale.
- Le pubblicazioni elettroniche, i file di configurazione e gli eseguibili di CS/AIX consumano spazio su disco permanente.
- I requisiti di spazio di paginazione di applicazioni, sessioni e processi correlati consumano spazio su disco permanente.

I requisiti di memoria e di spazio su disco dipendono da vari fattori che cambiano notevolmente da un ambiente all'altro. I programmi di transazione (TP, Transaction Program) e le sessioni SNA sono gli elementi che consumano più memoria e spazio su disco.

Un TP è un programma che utilizza l'API (Application Programming Interface) per accedere alla rete. Una sessione è un canale logico temporaneo tra due LU su nodi partner. Tale canale viene utilizzato dai TP per comunicare tra loro.

Il consumo di memoria e spazio su disco sono ampiamente influenzati dal numero totale di sessioni, dal numero di sessioni allocate (conversazioni), dall'intensità di traffico delle conversazioni e dal numero di TP utente attivi. I requisiti di memoria vengono influenzati principalmente dall'intensità del traffico dati e dal conseguente impiego di mbuf. I requisiti di spazio su disco derivano dai requisiti di spazio di paginazione dei TP, delle sessioni e dei relativi processi.

Per tutti i tipi di LU, occorre operare una distinzione tra sessione inattiva e sessione allocata. Una sessione inattiva è una sessione attiva non utilizzata da TP. Una sessione allocata è una sessione che supporta una conversazione in corso. Per stimare i requisiti di memoria totali, è necessario stimare l'intensità di traffico e la percentuale del numero totale di sessioni che verrà allocata, in media, in un dato momento. Si può anche scegliere di configurare il sistema affinché gestisca i picchi di richieste. Tali stime variano da un ambiente all'altro.

Se si incrementa il carico della sessione oltre la capacità di memoria del sistema, si incorre nella paginazione.

Processi
CS/AIX richiede almeno 20 processi AIX.

Tempo di risposta

È impossibile stimare il tempo di risposta dei livelli di traffico previsti, a causa dell'elevato numero di condizioni di rete esistenti. Inoltre, poiché il tempo di risposta non può essere espresso con una formula concisa, i risultati migliori si ottengono da dati sperimentali estrapolabili dalla rete.

Per agevolare l'elaborazione delle stime, le pagine Web di IBM Communications Server all'indirizzo http://www.ibm.com/software/network/commserver presentano differenti configurazioni di rete e mostrano inoltre in che modo il tempo di risposta di ciascuna rete sia influenzato da alcuni fattori, quali il modello della stazione di lavoro AIX e il numero di sessioni in corso.

Indirizzamento IPv4 e IPv6

I computer che eseguono CS/AIX V6.4 possono utilizzare gli indirizzi IPv4 o gli indirizzi IPv6, con i seguenti vincoli.

- Tutti i server di un dominio client/server devono utilizzare lo stesso formato di indirizzamento (IPv4 o IPv6).
  - Se i server utilizzano IPv4, anche i client devono utilizzarlo.
  - Se i server utilizzano IPv6, i client possono usare IPv6 o IPv4.
- Per quanto riguarda il server TN, se CS/AIX utilizza IPv4, anche i client TN connessi al server TN devono utilizzarlo. Se CS/AIX utilizza IPv6, i client TN possono utilizzare IPv6 o IPv4. Per impostazione predefinita, il server TN accetta connessioni da entrambi i tipi di client, ma può essere configurato per ascoltare un determinato indirizzo IP (utilizzando il parametro *listen_local_address* nel programma di gestione da riga comando o in un'applicazione NOF) al fine di operare una restrizione verso un unico tipo di connessione client.
- Per quanto riguarda il programma di reindirizzamento TN, se CS/AIX utilizza IPv4, entrambe le connessioni TCP/IP (dal client a CS/AIX e da CS/AIX all'host) devono utilizzare IPv4.

  Se CS/AIX utilizza IPv6, la connessione TCP/IP dal client a CS/AIX segue le stesse regole applicabili al server TN. La connessione da CS/AIX all'host può utilizzare IPv6 o IPv4. Non è necessario che le due connessioni utilizzino lo stesso formato di indirizzamento.
- Se si utilizza SLP, il server TN deve supportare l'indirizzamento IPv4, quindi deve avere un indirizzo IPv4 (benché possa avere anche un indirizzo IPv6). Ciò perché SLP utilizza trasmissioni UDP non disponibili in un'installazione che supporta solo IPv6.
- Per quanto riguarda Enterprise Extender (HPR/IP), le porte ad entrambe le estremità di un collegamento devono utilizzare lo stesso formato di indirizzamento (IPv4 o IPv6).
  - Se CS/AIX utilizza IPv4, può collegarsi solo a sistemi remoti configurati per supportare IPv4.
  - Se CS/AIX utilizza IPv6, può essere configurato in maniera tale da utilizzare IPv4 o IPv6 su un collegamento Enterprise Extender. L'opzione prescelta deve corrispondere alla configurazione a livello del sistema remoto.

  Inoltre, tutti i collegamenti sulla stessa porta Enterprise Extender devono utilizzare lo stesso formato di indirizzamento (IPv4 o IPv6). Per supportare

collegamenti con differenti formati di indirizzamento, è necessario utilizzare porte distinte. Analogamente, tutte le porte Enterprise Extender che risiedono nella stessa rete di connessione devono utilizzare lo stesso formato di indirizzamento.

Per verificare se un server CS/AIX esegue IPv4 o IPv6, utilizzare il comando **ifconfig -a** e cercare l'indirizzo IP o gli indirizzi dell'output. Si tratterà di indirizzi IPv4 decimali puntati, di indirizzi IPv6 esadecimali o di entrambi. Per quanto riguarda Remote API Client su Windows, il comando corrispondente è **ipconfig** (senza opzioni della riga comando). Per modificare il formato di indirizzamento IP del computer, consultare la documentazione del proprio sistema operativo.

Se si sta aggiornando un sistema CS/AIX esistente alla versione 6.4 come descritto in "Migrazione dai livelli precedenti di CS/AIX" a pagina 32 e si desidera anche passare all'indirizzamento IPv6, i due processi possono essere eseguiti in qualsiasi ordine. Tuttavia, le nuove funzionalità di indirizzamento IPv6 non possono essere utilizzate in V6.4 fino al completamento di entrambi i processi.

- Per quanto riguarda un sistema client/server, è necessario passare contemporaneamente tutti i server del dominio da IPv4 a IPv6; non cercare di eseguire un dominio misto di server IPv4 e IPv6.
- Poiché l'aggiornamento a CS/AIX V6.4 richiede anche l'aggiornamento contemporaneo di tutti i server, è possibile decidere di effettuare la modifica all'indirizzamento IPv6 mentre si aggiorna ciascun server. In alternativa, è possibile passare tutti i server a IPv6 prima o dopo l'aggiornamento alla versione 6.4 (scelta consigliata).
- Una volta modificati tutti i server per l'utilizzo dell'indirizzamento IPv6, è possibile modificare i client API remoti affinché utilizzino l'indirizzamento IPv6 come richiesto. I client IPv4 possono continuare a operare con i server IPv6, pertanto non è necessario modificare tutti i client contemporaneamente.

Se si sta installando un nuovo sistema CS/AIX, è possibile impostare solo l'indirizzamento IPv6 su tutti i server e i client, se appropriato, oppure utilizzare in un primo momento l'indirizzamento IPv4 e poi passare a IPv6 (in base ai vincoli summenzionati applicabili ai domini client/server).

Come garantire la compatibilità tra configurazioni per diverse piattaforme

I prodotti SNA in esecuzione su differenti piattaforme — quali IBM Personal Communications, Communications Server for Windows o VTAM NCP su un host — possono funzionare con CS/AIX qualora vengano soddisfatti alcuni requisiti.

In generale, il rilascio corrente di un prodotto di rete SNA può funzionare con CS/AIX nella misura in cui supporta i nodi PU 2.1 e almeno uno dei tipi di collegamento supportati da CS/AIX. Tuttavia, alcuni dei vecchi rilasci (quale VTAM V2) potrebbero non funzionare in maniera affidabile. Le funzionalità di ciascun prodotto di rete sono documentate nel rispettivo manuale per l'utente.

Considerare inoltre i seguenti fattori:

- Se si utilizza una LU 6.2 indipendente e la rete in uso non è una rete APPN, è necessario assicurarsi che le LU partner siano definite nel sistema locale.
- Poiché i valori predefiniti dei timer e delle dimensioni della finestra DLC variano da un dispositivo all'altro, è necessario che i dispositivi remoti utilizzino il valore corretto. Ad esempio, la dimensione della finestra DLC che garantisce

buone prestazioni con un nodo di Communications Server for Windows potrebbe non essere adatta a un nodo 3172. Per ulteriori informazioni sulle prestazioni legate alla dimensione della finestra, consultare le pagine Web di IBM Communications Server all'indirizzo http://www.ibm.com/software/network/commserver.

- Quando si opera in un ambiente eterogeneo (protocolli TCP/IP e SNA sulla stessa LAN) con più segmenti LAN, assicurarsi che i propri dispositivi di interconnessione LAN siano in grado di "instradare" TCP/IP e "collegare" i frame SNA contemporaneamente.

Convenzioni di denominazione

È possibile utilizzare gli ID di rete per segmentare la rete fisica in maniera logica. Inoltre, se si prevede di effettuare connessioni ad altre reti, è fortemente consigliata la registrazione dei propri ID di rete al fine di evitare conflitti tra i nomi delle reti.

I nomi LU e i nomi delle reti possono essere definiti come segue:

Nomi di rete
È possibile definire differenti nomi di rete (ID di rete) per fornire una segmentazione delle reti APPN. La segmentazione limita la dimensione dei database della topologia di rete e la frequenza di trasmissione delle richieste LOCATE effettuate tramite ciascuna rete.

Per garantire l'univocità di un ID di rete, l'amministratore di rete può inserirlo nel registro mondiale della IBM. Il registro della IBM garantisce che ciascun ID di rete sia univoco rispetto a quelli registrati. Gli standard del registro sono coerenti con gli standard OSI (Open Systems Interconnection), inclusi i codici paese OSI, come stabilito dall'ISO (International Organization for Standards).. Per ulteriori informazioni sulla registrazione, consultare *User's Guide for SNA Network Registry*.

Nomi LU
L'uso dei caratteri jolly è consentito per i nomi LU, al fine di ridurre al minimo le ricerche nella rete e nelle definizioni del sistema.

Capitolo 3. Installazione di CS/AIX su server AIX

Questo capitolo descrive come installare CS/AIX sui computer AIX. Inoltre, fornisce istruzioni sulla manutenzione delle proprie informazioni relative alla configurazione di CS/AIX.

Nota:

1. Per installare CS/AIX è necessario disporre di privilegi root.
2. Prima di poter utilizzare CS/AIX, è necessario aggiungere un controllo collegamento dati (DLC, Data Link Control). DLC gestisce la scheda di comunicazione. Per ulteriori informazioni, consultare la descrizione del comando **mkdev** in *AIX Commands Reference* o utilizzare l'opzione **Communications** nel menu **Devices** di SMIT (System Management Interface Tool) (per ulteriori informazioni, consultare *AIX Communications Programming Concepts*).
3. Per quanto riguarda AIX V6.1, il server deve essere eseguito nell'ambiente globale e non in una WPAR (partizione del carico di lavoro) del sistema o dell'applicazione.

Gestione delle licenze e creazione pacchetti di CS/AIX

In questa sezione vengono descritte le modalità di licenza e di creazione pacchetti del prodotto CS/AIX.

Meccanismi di gestione delle licenze di CS/AIX

Con questa sezione si intende fornire al lettore una comprensione avanzata dei meccanismi di gestione delle licenze. Il documento *License Information* di CS/AIX fornisce tutte le clausole e condizioni relative al prodotto. Inoltre, degli scenari campione illustrano ulteriormente la gestione delle licenze per molti dei differenti tipi di connettività e funzionalità offerti da CS/AIX. Per informazioni al riguardo, consultare http://www.ibm.com/software/network/commserver.

CS/AIX include vari componenti, di seguito descritti.

Programma IBM Communications Server for AIX

È necessaria una licenza di programma distinta per ogni macchina o nodo SP su cui è installato uno qualsiasi o la totalità dei componenti.

La gestione delle licenze di CS/AIX include la licenza di programma (server) e le licenze utente.

- Un Utente viene definito come un individuo. È necessario acquistare un'autorizzazione utente per ciascun utente simultaneo che accede a e utilizza CS/AIX, direttamente o indirettamente. Esempio di utilizzo indiretto: se un programma di multiplexing o un server di applicazioni (ad esempio, CICS, DB2, WebSphere o la propria applicazione aziendale) si connette a CS/AIX fornendo l'accesso per più utenti simultanei, occorre una licenza utente per ciascuno di tali utenti.
- Inoltre, per le applicazioni non associate ad utenti effettivi occorre un'autorizzazione utente per ciascuna connessione attiva in upstream o in downstream stabilita con il nodo CS/AIX. In un ambiente APPN, una connessione è un collegamento attivo a un nodo adiacente.

Abilitazione di CS/AIX con una licenza nodelock

CS/AIX utilizza licenze nodelock per abilitare e disabilitare il prodotto (le licenze nodelock sono licenze gestite a livello di un determinato nodo invece che da un server di licenze di rete).

Una licenza nodelock può essere una licenza permanente o una chiave temporanea che concede all'operatore l'utilizzo di CS/AIX per un periodo di tempo circoscritto (ad esempio, per un'offerta promozionale o a scopi dimostrativi). L'acquisto del prodotto CS/AIX include la licenza nodelock permanente che viene installata automaticamente nel file di licenza **nodelock** del sistema durante l'installazione del prodotto.

Se CS/AIX viene installato da un supporto contenente una versione dimostrativa, ad esempio un supporto CD Showcase, viene installato con una chiave temporanea. Per abilitare completamente il prodotto, è necessario acquistare una licenza CS/AIX tramite i canali di vendita IBM tradizionali. Per passare da una chiave temporanea a una licenza permanente, è sufficiente installare la chiave permanente dal supporto di installazione di CS/AIX. Non è necessario reinstallare il prodotto.

Per estrarre la chiave dal CD di installazione di CS/AIX, attenersi alla seguente procedura:

1. Emettere il comando **smit bffcreate** ed utilizzare la finestra di dialogo SMIT visualizzata per estrarre l'immagine LPP dai supporti di installazione. Annotare il nome del file creato, che dovrebbe essere **sna.6.4.0.0.I** o un nome simile.
2. Utilizzare i seguenti comandi per estrarre la chiave dall'immagine LPP:

   cd /tmp
   restore -f /usr/sys/inst.images/installp/ppc/*nome file*
   ./usr/lib/sna/install/license.sna

   Sostituire *nome file* con il nome file annotato nella fase 1.
3. Utilizzare il seguente comando per copiare la chiave nel file **/var/ifor/nodelock**. Assicurarsi di utilizzare l'operatore "append" >> per concatenare la chiave nel file (**non** utilizzare l'operatore > che sovrascrive tutte le chiavi precedenti).

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

Monitoraggio dell'utilizzo delle risorse di CS/AIX

Mentre le licenze di CS/AIX sono basate sugli utenti simultanei del prodotto, è difficile misurare concretamente o notificare il numero di utenti per gli svariati tipi di risorse di comunicazione forniti da CS/AIX. Tuttavia, il monitoraggio dei diversi tipi di risorse potrebbe risultare utile come indicatore di eventuali modifiche nell'uso globale o nei picchi di utilizzo. Se combinate agli scenari di esempio mostrati all'indirizzo http://www.ibm.com/software/network/commserver, queste informazioni possono aiutare a capire meglio quante licenze CS/AIX simultanee occorrono.

CS/AIX monitora l'utilizzo dei seguenti tipi di risorse di comunicazione forniti:

- Applicazioni che utilizzano le API CPI-C o APPC (ad esempio, DB2 o WebSphere)
- Applicazioni che utilizzano l'API LUA (solitamente sviluppata dall'utente)
- Stazioni di collegamento attive (a un host, a un nodo APPN adiacente o a un nodo LEN, a Enterprise Extender o a un client gateway SNA o DLUR in downstream)

- Sessioni Telnet connesse al componente server TN3270E di CS/AIX, che utilizzano o meno la crittografia di dati SSL o l'autenticazione client/server
- Sessioni Telnet connesse al componente programma di reindirizzamento TN di CS/AIX (ad esempio le sessioni VT reindirizzate) per l'utilizzo della crittografia dati SSL o l'autenticazione client/server
- Sessioni di dati SNA attive (sessioni attive di LU di tipo 1, 2 o 3 e sessioni LU 6.2 attive, ad esclusione di quelle utilizzate per il controllo della rete).

L'utilizzo di ciascuna risorsa viene misurato a intervalli periodici, mentre quello di CS/AIX viene rilevato al momento dell'iscrizione in un "file di registrazione dell'utilizzo" disponibile poi per l'analisi e l'uso da parte dell'utente. Ad ogni fase di campionamento, vengono registrati sia l'utilizzo corrente che il picco di utilizzo della risorsa (dall'ultimo riavvio del sistema).

Per ulteriori informazioni sulla registrazione dell'utilizzo, consultare *IBM Communications Server for AIX Diagnostics Guide*.

Come vengono creati i pacchetti del programma CS/AIX concesso in licenza

Il programma CS/AIX concesso in licenza (LPP, Licensed Program Product) è formato da più pacchetti (immagini installabili), ognuno dei quali contiene una o più serie di file. Una serie di file è l'unità installabile più piccola del prodotto. AIX aggiorna le informazioni sul rilascio e sul livello di ciascuna serie di file (vedere il comando **lslpp** di AIX in "Visualizzazione dei dettagli di installazione del prodotto" a pagina 31). Il programma concesso in licenza può contenere anche file di aggiornamento.

Nota: Per informazioni sui requisiti di memoria, consultare "Requisiti di installazione" a pagina 20.

Quando si installa CS/AIX sono necessarie le seguenti serie di file:

pacchetto sna

sna.rte Programma base di CS/AIX.

pacchetto sna.msg.*Lingua*

Catalogo messaggi di CS/AIX, contenente i messaggi e i file della guida finestra di dialogo nella lingua specificata per l'ambiente di runtime. È necessaria la seguente serie di file:

sna.msg.*Lingua* **.rte**

I messaggi e i file della guida della finestra di dialogo per le funzionalità di base di CS/AIX. *Lingua* indica la lingua in cui devono essere visualizzati i messaggi. Selezionare uno dei seguenti identificativi lingua:

Identificativo	Lingua
en_US	Inglese (Stati Uniti)
Ja_JP	Giapponese (PC)
de_DE	Tedesco
es_ES	Spagnolo
fr_FR	Francese
ko_KR	Coreano
pt_BR	Portoghese
zh_CN	Cinese (EUC semplificato)

Identificativo	Lingua
zh_TW	Cinese (tradizionale)

Se si installano più lingue per uno stesso prodotto, assicurarsi di installare prima la lingua preferita (o primaria). Ad esempio, per installare Inglese (Stati Uniti) come lingua primaria, specificare:

sna.msg.en_US.rte

sna.rte è un prerequisito per **sna.msg.***Lingua***.rte**.

Serie di file per il supporto SSL
Le seguenti serie di file sono incluse come supporto per SSL (Secure Sockets Layer) con il server TN o il programma di reindirizzamento TN:

gskta.rte
Certificato AIX e runtime di base SSL.

Funzioni comprese in CS/AIX

Le seguenti funzioni sono fornite come parte integrante di CS/AIX. Si può scegliere di installarle o meno.

sna.xsna
Programma di gestione Motif.

sna.rte, **X11.base.rte** e **X11.Dt.helprun** sono prerequisiti per **sna.xsna**.

sna.wa
Programma di gestione Web.

sna.rte è un prerequisito per **sna.wa**.

sna.lu0
Funzioni LU 0.

sna.rte è un prerequisito per **sna.lu0**.

sna.docs.*Lingua***.data**
Documentazione in linea. *Lingua* indica la lingua in cui devono essere visualizzati i documenti (ad esempio, `fr_FR` per il francese).

sna.man.en_US.rte.data, sna.man.en_US.xsna.data, sna.man.en_US.lu0.data
Pagine del manuale di AIX dedicate ai comandi di CS/AIX.

sna.msg.*Lingua***.snapi, sna.msg.***Lingua***.xsna, sna.msg.***Lingua***.wa**
Messaggi e file della guida della finestra di dialogo per le funzioni opzionali di CS/AIX. L'installazione di queste serie di file è necessaria solo se si stanno installando le serie di file corrispondenti per le funzioni opzionali. *Lingua* indica la lingua in cui devono essere visualizzati i messaggi (ad esempio, `fr_FR` per il francese).

sna.snapi
SNA Application Development Toolkit (SNAPI).

sna.rte è un prerequisito per **sna.snapi**.

sna.rte64
Serie di file per il supporto API a 64 bit.

sna.rte è un prerequisito per **sna.rte64**.

sna.dlcmpc
SNA Channel Data Link.

sna.ecl
Host Access Class Library.

Communications.Bnd
Definizione bundle da utilizzare con Installazione rapida (come descritto in "Modalità di installazione" a pagina 33).

Preparazione dell'installazione di CS/AIX

Prima di installare CS/AIX, è necessario eseguire AIX Versione 5.2, 5.3 o 6.1 (per quanto riguarda AIX V6.1, il server deve essere eseguito nell'ambiente globale, non in una WPAR, partizione del carico di lavoro, del sistema o dell'applicazione). Eseguire queste operazioni:

- Installare e configurare tutti i DLC necessari per la comunicazione sulla rete, come descritto in "Installazione delle serie di file DLC (Data Link Control)" (i DLC devono essere installati e configurati prima dell'utilizzo di CS/AIX, ma possono anche essere installati dopo l'installazione di CS/AIX).
- Se si desidera utilizzare il programma di gestione Web e non è stato ancora installato un server Web adeguato, installarlo ora. I server Web supportati da CS/AIX sono elencati in "Requisiti di installazione" a pagina 20. Seguire le istruzioni di installazione fornite con il software del server Web.
- Per garantire la gestione corretta di messaggi e finestre di dialogo del prodotto, assicurarsi che la variabile d'ambiente `LANG` sia impostata in maniera adeguata, come descritto in "Modifica della variabile d'ambiente della lingua" a pagina 32.

Installazione delle serie di file DLC (Data Link Control)

Per comunicare sulla rete, CS/AIX richiede almeno una serie di file DLC (Data Link Control) di AIX. Segue un elenco di tali serie di file DLC:

- **bos.dlc.token** per stazioni di collegamento Token Ring
- **bos.dlc.ether** per stazioni di collegamento Ethernet standard
- **bos.dlc.8023** per stazioni di collegamento Ethernet 802.3
- **bos.dlc.qllc** per stazioni di collegamento X.25
- **bos.dlc.sdlc** per stazioni di collegamento SDLC

Tutte le serie di file **bos.dlc** sono fornite come parti integranti del pacchetto **bos.dlc.usr** nel sistema operativo AIX di base. I DLC devono essere installati separatamente.

Nota: Per ulteriori informazioni sui DLC di AIX, consultare *AIX Communications Programming Concepts*.

Visualizzazione dei dettagli di installazione del prodotto

È possibile visualizzare la cronologia delle installazioni di CS/AIX (e di alcuni prodotti correlati) immettendo uno dei seguenti comandi:

Immettere:	Per il prodotto:
lslpp -h sna.rte	IBM Communications Server for AIX

Per visualizzare le correzioni PTF (Program Temporary Fixes) applicate ai prodotti dalla rispettiva installazione, immettere il comando con l'indicatore **-ha** invece dell'indicatore **-h**.

Modifica della variabile d'ambiente della lingua

Quando si utilizza CS/AIX, assicurarsi che la variabile LANG non sia impostata su C.

Utilizzare la seguente procedura per visualizzare la variabile LANG in uso o per modificarla:

1. Dal menu principale SMIT, selezionare **System Environments**.
2. Dal menu SMIT successivo, selezionare **Manage Language Environment**.
3. Dal menu SMIT successivo, selezionare **Change/Show Primary Language Environment**.
4. Dal menu SMIT successivo, selezionare **Change/Show Cultural Convention, Language, or Keyboard**.
5. Selezionare la lingua che si desidera utilizzare. Ad esempio, se si stanno utilizzando messaggi in lingua Inglese (Stati Uniti), selezionare en_US.

Migrazione dai livelli precedenti di CS/AIX

Considerazioni

Se si effettua un aggiornamento a CS/AIX V6.4 a partire da una versione precedente di CS/AIX, è necessario tenere conto di quanto segue.

1. Se CS/AIX viene eseguito con una configurazione client/server con due o più server, è consigliabile aggiornare contemporaneamente tutti i server alla versione 6.4 prima di aggiornare i client API remoti.
   - Durante la migrazione dei server non sarà possibile utilizzare il programma di gestione Motif, né il programma di gestione da riga comando su un server di livello precedente per visualizzare e gestire le risorse su un server che esegue la versione 6.4.
   - La Versione 6.3.1.0 e le versioni successive di Remote API Client funzioneranno con un server esistente, ma solo se il sistema operativo presente sul client non è configurato per l'utilizzo di IPv6.
   - Le versioni precedenti di Remote API Client funzioneranno con CS/AIX V6.4.
2. Nella Versione 6.2.3.0 sono state modificate varie strutture dati dell'API NOF affinché accetti i formati di indirizzo più lunghi necessari per gli indirizzi IPv6. Ciò significa che se si utilizza uno qualsiasi dei seguenti verbi e/o indicazioni in un'applicazione NOF esistente creata prima della Versione 6.2.3.0 (anche se non si stanno utilizzano le nuove funzionalità di indirizzamento IPv6), sarà necessario ricompilare l'applicazione affinché lo utilizzi con CS/AIX V6.4.
   - DEFINE_LS, DEFINE_PORT, QUERY_LS, QUERY_PORT se utilizzata con una porta o LS Enterprise Extender (HPR/IP)
   - DEFINE_TN3270_ACCESS, DELETE_TN3270_ACCESS, QUERY_TN3270_ACCESS
   - DEFINE_TN3270_EXPRESS_LOGON, QUERY_TN3270_EXPRESS_LOGON
   - DEFINE_TN3270_SSL_LDAP, QUERY_TN3270_SSL_LDAP
   - DEFINE_TN_REDIRECT, QUERY_TN_REDIRECT_DEF
   - QUERY_LU_0_TO_3 (per qualsiasi tipo LU)
   - TN_REDIRECTION_INDICATION
3. Per utilizzare le nuove funzionalità di indirizzamento IPv6 della versione 6.4, è necessario garantire che i server CS/AIX siano configurati per l'utilizzo dell'indirizzamento IPv6. Per ulteriori dettagli, consultare "Indirizzamento IPv4 e IPv6" a pagina 24.

Installazione del programma CS/AIX concesso in licenza

Una volta installato il software prerequisito, si è pronti per installare CS/AIX. Attenersi alla seguente procedura:

1. Accedere con privilegi root.
2. Installare e configurare il rispettivo DLC di AIX per la scheda di comunicazione selezionata. Per configurare il DLC, utilizzare il comando **mkdev** (descritto in *AIX Commands Reference*) o l'opzione **Communications** sul menu **Devices** di SMIT (descritto in *AIX Communications Programming Concepts*).
3. Installare CS/AIX come descritto in "Modalità di installazione". Selezionare le funzioni che si desidera installare (incluso qualsiasi serie di file di messaggi applicabile) o selezionare `all` per installare CS/AIX includendo tutte le funzioni.

   Se si seleziona una funzione e si sceglie `yes` per il campo *Install requisite software*, il sistema installa anche **sna.rte** (il programma base di CS/AIX).
4. Se per utilizzare il server TN o il programma di reindirizzamento TN con la funzione SSL sono stati installati il certificato AIX e il software runtime di base SSL, è necessario configurare il software SSL dopo aver installato CS/AIX. Per ulteriori informazioni, consultare "Configurazione di SSL per l'utilizzo con il server TN o il programma di reindirizzamento TN" a pagina 39.
5. Personalizzare le informazioni relative alla configurazione di CS/AIX come desiderato (consultare Capitolo 8, "Configurazione e utilizzo di CS/AIX", a pagina 71 o *IBM Communications Server for AIX Administration Guide*).
6. Avviare CS/AIX. Dopo l'installazione, ciò avverrà automaticamente al riavvio della macchina.

   cd /

   sna start

Nota:

1. L'installazione di CS/AIX comporta la riconfigurazione automatica dei driver del dispositivo SNA sul nodo locale. Se CS/AIX v6.1 era già stato installato su AIX 5.3 e ora si sta effettuando l'aggiornamento alla versione 6.4, prima di poter avviare il nodo SNA sarà necessario un riavvio della macchina al termine dell'installazione di CS/AIX. In caso contrario, non sarà necessario riavviare o riconfigurare il kernel prima di avviare CS/AIX.
2. Una volta installato CS/AIX è possibile installare le schede. Non è necessario reinstallare CS/AIX dopo aver aggiunto una scheda, ma quest'ultima non può essere utilizzata finché non viene installato il DLC appropriato.

Modalità di installazione

È possibile installare il programma CS/AIX concesso in licenza con una delle seguenti modalità:

- Installazione rapida
- Sul sistema locale
- Sulla rete (se il nodo locale è un server di rete)

Installazione di CS/AIX mediante Installazione rapida

Il software può essere installato più facilmente utilizzando i bundle software. Un bundle software contiene un elenco di prodotti software indicati per un determinato uso. Le seguenti sezioni mostrano come installare CS/AIX tramite

questa funzione. L'Installazione rapida può essere eseguita dalla console di sistema o in remoto, in X-Windows o da un terminale ASCII.

Installare CS/AIX sul nodo locale come descritto in "Installazione rapida tramite SMIT" o "Installazione rapida tramite CDE (Common Desktop Environment)".

Installazione rapida tramite SMIT:

1. Accedere con privilegi root.
2. Immettere il seguente comando:
   - **smit install_bundle**
3. Premere **PF4** o fare clic sul pulsante **List** su Motif per visualizzare un elenco dei dispositivi di installazione e delle directory relative al supporto di installazione.
4. Selezionare `Media-defined` e premere **Enter**.
5. Selezionare il dispositivo di input e premere **Enter**.

Installazione rapida tramite CDE (Common Desktop Environment):

1. Da Desktop Launch Pad, aprire Tools Application Manager.
2. Aprire la cartella **System_Admin**.
3. Aprire **Easy Install**.
4. Selezionare il proprio dispositivo di input.
5. Selezionare il bundle `Media-defined`.
6. Fare clic sul pulsante **Install/Update**.

Installazione manuale su nodo locale

Installare CS/AIX sul sistema locale come descritto in "Installazione manuale tramite SMIT" o "Installazione manuale tramite Common Desktop Environment" a pagina 35.

Installazione manuale tramite SMIT:

1. Porre il supporto di installazione nell'unità appropriata della stazione di lavoro AIX.
2. Accedere con privilegi root.
3. Assicurarsi che la variabile d'ambiente `LANG` presente sul proprio sistema non sia impostata su `C`. Se si selezionano messaggi in lingua Inglese (Stati Uniti), impostare la variabile `LANG` su `en_US`. Per ulteriori informazioni su come visualizzare o modificare la variabile d'ambiente `LANG`, consultare "Modifica della variabile d'ambiente della lingua" a pagina 32.
4. Immettere il seguente comando nella riga di comando di AIX:

   smit install

   Questo comando richiama SMIT che fornisce un ambiente basato su menu per l'installazione.
5. Selezionare le seguenti opzioni nei menu di installazione di SMIT per eseguire un'installazione standard del software selezionabile e dei relativi aggiornamenti:
   a. **Install and Update Software**
   b. **Install/Update Selectable Software (Custom Install)**
   c. **Install/Update From All Available Software**

   Questa sequenza di selezioni menu è paragonabile al seguente comando di accesso rapido:

smit install_selectable_all

6. Nella successiva finestra di dialogo, selezionare il nome del dispositivo appropriato per il supporto di installazione come dispositivo d'origine per la procedura di installazione (per un elenco dei nomi dei dispositivi, utilizzare **PF4** nell'interfaccia caratteri per SMIT o il pulsante **List** in Motif).
7. Selezionare **sna.rte**, il programma base di CS/AIX, **sna.msg.***Lingua***.rte** (il catalogo messaggi di CS/AIX) e qualsiasi ulteriore funzione e aggiornamento per il programma concesso in licenza (incluso qualunque altra serie di file di messaggi applicabile). Per installare tutte le funzioni sul supporto di installazione, selezionare l'opzione `tutto`.

   L'utilità di installazione visualizza messaggi di stato quando ciascuna parte completa correttamente l'installazione.
8. Per installare il certificato AIX e il software runtime di base SSL per l'utilizzo del server TN o del programma di reindirizzamento TN con la funzione SSL, selezionare anche il certificato AIX e la serie di file di runtime di base SSL.

   L'utilità di installazione visualizza messaggi di stato quando ciascuna parte completa correttamente l'installazione.

   Se è stato installato questo software, è necessario configurare il software SSL dopo aver installato CS/AIX. Per ulteriori informazioni, consultare "Configurazione di SSL per l'utilizzo con il server TN o il programma di reindirizzamento TN" a pagina 39.
9. Personalizzare le informazioni relative alla configurazione di CS/AIX (consultare Capitolo 8, "Configurazione e utilizzo di CS/AIX", a pagina 71 o *IBM Communications Server for AIX Administration Guide*).

Nota:

1. L'installazione di CS/AIX comporta automaticamente la riconfigurazione dei driver del dispositivo SNA sul nodo locale. Se CS/AIX v6.1 era già stato installato su AIX 5.3 e ora si sta effettuando l'aggiornamento alla versione 6.4, prima di poter avviare il nodo SNA sarà necessario un riavvio della macchina al termine dell'installazione di CS/AIX. In caso contrario, non sarà necessario riavviare o riconfigurare il kernel prima di avviare CS/AIX.
2. Per ulteriori informazioni sulla gestione delle licenze utente per CS/AIX, consultare "Meccanismi di gestione delle licenze di CS/AIX" a pagina 27.

Installazione manuale tramite Common Desktop Environment:

1. Porre il supporto di installazione nel drive appropriato della stazione di lavoro AIX.
2. Accedere con privilegi root.
3. Assicurarsi che la variabile d'ambiente `LANG` presente sul proprio sistema non sia impostata su `C`. Se si selezionano messaggi in lingua Inglese (Stati Uniti), impostare la variabile `LANG` su `en_US`. Per ulteriori informazioni su come visualizzare o modificare la variabile d'ambiente `LANG`, consultare "Modifica della variabile d'ambiente della lingua" a pagina 32.
4. Dal Desktop Launch Pad, aprire Tools Application Manager.
5. Aprire la cartella **System_Admin**.
6. Aprire la cartella **Install Manager**.
7. Selezionare il proprio dispositivo di input.

8. Selezionare tutti gli oggetti visualizzati per installare tutto sul supporto oppure espandere e selezionare i singoli oggetti per personalizzare le opzioni di Communications Server for AIX da installare.
9. Fare clic sull'icona **Install** per avviare l'installazione.
10. Personalizzare le informazioni relative alla configurazione di CS/AIX (consultare Capitolo 8, "Configurazione e utilizzo di CS/AIX", a pagina 71 o *IBM Communications Server for AIX Administration Guide*).

Nota:

1. L'installazione di CS/AIX comporta automaticamente la riconfigurazione dei driver del dispositivo SNA sul nodo locale. Se CS/AIX v6.1 era già stato installato su AIX 5.3 e ora si sta effettuando l'aggiornamento a V6.4, prima di poter avviare il nodo SNA sarà necessario un riavvio della macchina al termine dell'installazione di CS/AIX. In caso contrario, non sarà necessario riavviare o riconfigurare il kernel prima di avviare CS/AIX.
2. Per ulteriori informazioni sulla gestione delle licenze utente per CS/AIX, consultare "Meccanismi di gestione delle licenze di CS/AIX" a pagina 27.

Installazione su rete tramite Network Installation Management

Utilizzare questa procedura per installare CS/AIX su una rete:

1. Per informazioni sull'impostazione del server Network Installation e il download dei file nel client, consultare *AIX Version 5.3 Installation Guide and Reference*.
2. Assicurarsi che la variabile d'ambiente `LANG` presente sul proprio sistema non sia impostata su `C`. Se si selezionano messaggi in lingua Inglese (Stati Uniti), impostare la variabile `LANG` su `en_US`. Per ulteriori informazioni su come visualizzare o modificare la variabile d'ambiente `LANG`, consultare "Modifica della variabile d'ambiente della lingua" a pagina 32.
3. Immettere il seguente comando nella riga di comando di AIX:

   smit nim

   Questo comando richiama SMIT che fornisce un ambiente basato su menu per l'installazione.
4. Seguire le istruzioni e rispondere ai prompt sui menu di installazione di SMIT per eseguire un'installazione di rete. Selezionare i file contenenti **sna.rte** e qualsiasi ulteriore funzione e aggiornamento per il programma concesso in licenza. L'utilità di installazione visualizza messaggi di stato quando ciascuna parte completa correttamente l'installazione.

Nota:

1. Il catalogo messaggi di CS/AIX, **sna.msg.***Lingua***.rte**, si installa automaticamente con CS/AIX quando l'opzione *Include corresponding LANGUAGE filesets?* è impostata su `yes` (opzione predefinita).
2. L'installazione di CS/AIX comporta automaticamente la riconfigurazione dei driver del dispositivo SNA sul nodo locale. Se CS/AIX v6.1 era già stato installato su AIX 5.3 e ora si sta effettuando l'aggiornamento alla versione 6.4, prima di poter avviare il nodo SNA sarà necessario un riavvio della macchina al termine dell'installazione di CS/AIX. In caso contrario, non sarà necessario riavviare o riconfigurare il kernel prima di avviare CS/AIX.

3. Per ulteriori informazioni sulla gestione delle licenze utente per CS/AIX, consultare “Meccanismi di gestione delle licenze di CS/AIX” a pagina 27.

Configurazione di WebSphere Application Server

Se si intende eseguire un sistema client/server in cui i client API remoti si connettono ai server CS/AIX tramite HTTPS, sarà necessario un computer che esegue WebSphere Application Server affinché fornisca un accesso HTTPS da questi client ai server, così come descritto in “Requisiti di installazione” a pagina 20.

Questa sezione descrive come impostare WebSphere per utilizzarlo con CS/AIX:

- Impostazione di un certificato di sicurezza nel server WebSphere da presentare ai client
- Configurazione di WebSphere Application Server per l'utilizzo con CS/AIX
- Installazione del file di configurazione del server sul server WebSphere

Sarà altresì necessario impostare il certificato di sicurezza del client e il file dei dati di rete del client su ciascun client API remoto per accedere a WebSphere Application Server. Per ulteriori informazioni, consultare il capitolo sull'installazione del tipo di client appropriato.

Impostazione del certificato di sicurezza di WebSphere Application Server

Consultare la documentazione di WebSphere Application Server per istruzioni sull'impostazione di un certificato di sicurezza sul server. Si tratta del certificato del server che verrà presentato al client API remoto nel corso del processo di autenticazione durante il tentativo di connessione tramite HTTPS.

Si consiglia di configurare WebSphere in modo che applichi l'autenticazione del client. Per ulteriori informazioni, consultare la documentazione di WebSphere Application Server. Ciò significa che durante il processo di autenticazione WebSphere richiederà i certificati di sicurezza ai client API remoti e accetterà una connessione in entrata da uno di questi client solo se sarà in grado di verificare l'autenticità del suo certificato.

Configurazione di WebSphere Application Server

Per configurare WebSphere Application Server per l'utilizzo con CS/AIX, attenersi alla seguente procedura. Per ulteriori informazioni, consultare la documentazione di WebSphere Application Server.

1. Copiare o trasferire tramite FTP i due file **snahttpsrv.ear** e **snahttpsrv.cfg** dalla directory **ibm-commserver-https** sul CD di installazione di Remote API Client a una directory sul computer in cui è in esecuzione la console di gestione WebSphere o a una directory di rete accessibile da questo computer.

   Se la console di gestione è in esecuzione su Windows, non è necessario copiare i file in quanto è possibile accedervi direttamente dal CD. È sufficiente inserire il CD di installazione di Remote API Client nell'unità CD del computer Windows.
2. Avviare la console di gestione WebSphere.

3. Seguire le indicazioni della documentazione di WebSphere per creare un host virtuale accessibile solo tramite una connessione protetta con SSL. Questo host virtuale verrà utilizzato per il plug-in Java che gestisce le connessioni HTTPS SNA.
4. Dalla barra dei menu, selezionare Applications, Install New Application.
5. Specificare l'ubicazione del file **snahttpsrv.ear**. Fare clic sul pulsante Next.
6. Quando, nelle prime due schermate, verrà richiesto di specificare un nome per l'host virtuale, immettere il nome di quello impostato per l'HTTPS. Per tutti gli altri parametri, è possibile accettare le opzioni predefinite a meno che occorra utilizzare una configurazione specifica di WebSphere. Nelle successive finestre di dialogo, fare clic sul pulsante Next finché non viene sostituito dal pulsante Finish, quindi fare clic su quest'ultimo. La schermata dovrebbe quindi mostrare il messaggio **Application installed successfully**.
7. Fare clic su Save to Master Configuration, quindi sul pulsante Save.
8. Dalla barra dei menu, selezionare Applications, Enterprise Applications.
9. Cercare **SnaHttpTransport** nell'elenco delle applicazioni, fare clic sulla casella di spunta adiacente, quindi sul pulsante Start per avviare l'applicazione (successivamente, quest'ultima verrà avviata automaticamente all'avvio di WebSphere Application Server).
10. Dalla barra dei menu, selezionare Environment, Update Web Server Plugin e fare clic sul pulsante OK. Ciò serve ad aggiornare la configurazione di WebSphere.

Installazione del file di configurazione del server

Per poter operare con CS/AIX, WebSphere Application Server necessita di un elenco dei server CS/AIX ai quali si accederà tramite HTTPS. Creare e installare tale elenco utilizzando la seguente procedura.

1. Nella barra dei menu della console di gestione di WebSphere, selezionare Environment, Manage WebSphere Variables.
2. Cercare la variabile **USER_INSTALL_ROOT** nell'elenco e annotarne il valore (il percorso di una directory nel server WebSphere). L'elenco delle variabili d'ambiente potrebbe estendersi su due o più pagine, pertanto potrebbe essere necessario utilizzare il pulsante Next per scorrere l'elenco.
3. Copiare il file **snahttpsrv.cfg** dall'ubicazione in cui è stato salvato in "Configurazione di WebSphere Application Server" a pagina 37 (o dal CD di installazione) nella directory specificata dalla variabile **USER_INSTALL_ROOT**, quindi modificarlo tramite un editor di testo per includere un elenco di server CS/AIX accessibili dai client API remoti tramite HTTPS. Ciascun server deve essere specificato su una riga distinta del file, in base al seguente formato:

   server=*nomeserver.nomedominio.com*

Procedure successive all'installazione

Questa sezione spiega come eseguire le attività di manutenzione che potrebbero rendersi necessarie dopo l'installazione di CS/AIX.

Funzionamento client/server

Appena installato, CS/AIX funge da server standalone (con tutti i componenti su un unico sistema AIX). Per eseguirlo come server in un dominio client/server, consultare le istruzioni riportate nel capitolo Managing CS/AIX Client/Server Systems in *IBM Communications Server for AIX Administration Guide*.

Visualizzazione di libri in PDF

I manuali inclusi nel supporto di installazione di questo prodotto sono in formato PDF (Portable Document Format). Il formato elettronico consente di cercare, stampare o navigare agevolmente tra le informazioni tramite collegamenti ipertestuali alle informazioni correlate. Semplifica inoltre la condivisione della libreria sul proprio sito, poiché i visualizzatori PDF sono disponibili per numerose piattaforme differenti.

Se si sceglie di installare i manuali PDF durante l'installazione del prodotto, la directory in cui vengono installati è **/usr/share/man/info/***Lingua***/sna**. Il file HTML **SNABOOKS.HTM** contenuto in questa directory fornisce un collegamento ipertestuale a ciascun manuale. I manuali sono inclusi anche nella directory **/DOCS** sul supporto di installazione di CS/AIX.

I manuali PDF possono essere letti tramite qualsiasi visualizzatore PDF, quali Adobe Acrobat su Windows o **xpdf** su Intel Linux.

Consultazione delle informazioni sul rilascio corrente

L'ultimo aggiornamento del file **README** per il prodotto, ubicato nella directory **/usr/lpp/sna**, contiene informazioni su qualsiasi modifica del prodotto successiva alla pubblicazione della libreria di CS/AIX. Consultare il file **README** ogni volta che si ricevono aggiornamenti sul prodotto.

È possibile accedere al file **README** da SMIT, seguendo la seguente procedura:

1. Dopo aver installato CS/AIX V6.4, accedere al menu principale di SMIT per CS/AIX immettendo il seguente comando nella riga di comando:

   smit sna

   Viene così visualizzato il menu principale di SMIT per CS/AIX.
2. Selezionare **Product Information** dal menu principale di SMIT per CS/AIX. SMIT visualizza la finestra di dialogo Product Information.
3. Selezionare una delle opzioni del menu per visualizzare il rispettivo file **README**.

Configurazione di SSL per l'utilizzo con il server TN o il programma di reindirizzamento TN

Se sono stati installati il certificato AIX e il software di runtime di base SSL per poter utilizzare il server TN o il programma di reindirizzamento TN con la funzione SSL, dopo aver installato CS/AIX è necessario configurare il software SSL.

Il software SSL necessita di due componenti:

- Una coppia di chiavi, necessaria per consentire l'esecuzione della crittografia e della decrittografia dei dati.
- Un certificato, necessario per consentire l'autenticazione del server.

Il certificato e la coppia di chiavi formano un record unico in un database keyring, memorizzato nel server CS/AIX che esegue il server TN o il programma di reindirizzamento TN. CS/AIX utilizza il database per implementare SSL.

Per gestire il database keyring, digitare il seguente comando nel prompt dei comandi di AIX:

snakeyman

Il comando **snakeyman** avvia un programma Java. Per ulteriori istruzioni, consultare la guida fornita con questo programma.

Ciascun record contenuto nel database viene identificato da un nome univoco noto come etichetta. Se due o più record devono essere utilizzati su differenti sessioni del server TN o del programma di reindirizzamento TN, è necessario annotarsi le etichette assegnate durante l'impostazione del database; tali etichette vengono utilizzate per individuare il record da utilizzare in ciascuna sessione. È anche possibile impostare uno di questi record come record predefinito, affinché le sessioni utilizzino questo record, salvo esplicita indicazione dell'etichetta di un altro record.

Dopo aver utilizzato **snakeyman** per aggiornare i certificati del server, per utilizzare i certificati aggiornati è necessario uscire dal programma **snakeyman**, quindi arrestare e riavviare il nodo di CS/AIX. Utilizzare i seguenti comandi per arrestare e riavviare il nodo:

snaadmin term_node
snaadmin init_node

Configurazione di un server Web per il programma di gestione Web

Se si utilizza il programma di gestione Web con un server Web non elencato in "Requisiti di installazione" a pagina 20 o se si installa il server Web dopo aver installato CS/AIX, occorre impostare dei collegamenti tra le directory di CS/AIX e le directory del server Web, affinché quest'ultimo possa trovare i file necessari. Utilizzare il comando **ln** per creare i seguenti collegamenti.

- La directory "servlets" del server Web deve essere collegata a **/usr/lib/sna/WebAdmin/Server**.
- La sottodirectory **SnaAdmin** della directory "public HTML" del server Web deve essere collegata a **/usr/lib/sna/WebAdmin/Client**.

Per ulteriori informazioni su come impostare il server Web, consultare il file di testo **/usr/lpp/sna.wa/README** installato insieme al pacchetto del programma di gestione Web di CS/AIX.

Host Access Class Library

Se si sceglie di installare i file dell'Host Access Class Library durante l'installazione del prodotto, la directory in cui vengono installati è **/usr/share/lib/sna/ecl**. Per ulteriori informazioni su questi file, consultare il file **readme.htm** contenuto nella stessa directory.

Esecuzione del backup dei file di configurazione di CS/AIX

CS/AIX esegue un backup automatico dei file del nodo, del dominio, dei dati del dispositivo TN3270 (**tn3270dev.dat**) e della configurazione di TP ogni volta che si effettuano modifiche che influiscono su questi file (utilizzando uno qualsiasi degli strumenti di gestione di CS/AIX). Ad esempio, quando si apporta una modifica che influisce sul file di configurazione del nodo (**sna_node.cfg**), CS/AIX crea un file di backup denominato **sna_node.bk***n*, in cui *n* è 1 o 2:

- La prima volta che si modifica il file, la configurazione esistente viene salvata in **sna_node.bk1**.

- La seconda volta che si modifica il file, la configurazione esistente viene salvata in **sna_node.bk2**, lasciando inalterato il file **sna_node.bk1**.
- La terza volta che si modifica il file, così come tutte volte successive, il file **sna_node.bk1** viene eliminato, **sna_node.bk2** viene rinominato in **sna_node.bk1** e la configurazione esistente viene salvata in **sna_node.bk2**.

Ciò significa che, in qualsiasi momento, non possono essere presenti più di due file di backup per il file di configurazione del nodo. Lo stesso processo viene utilizzato per generare estensioni del nome file per altri file di backup.

Oltre ai backup automatici, nelle seguenti situazioni sarebbe opportuno eseguire il backup dei file di configurazione per proteggersi da eventuali perdite di dati:

- Prima di installare un nuovo livello del sistema operativo AIX
- Prima di installare un nuovo rilascio di CS/AIX
- Dopo aver creato una nuova configurazione

È possibile eseguire un backup dei file di configurazione tramite i seguenti comandi:

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

In questi comandi, *Nomedispositivo* indica il percorso e il nome file del dispositivo che riceverà i dati dai file di cui viene eseguito il backup. Possibilmente, eseguire il backup dei file su un supporto esterno come un dischetto o un nastro.

Ripristino di una copia di backup dei file di configurazione di CS/AIX

Per ripristinare i file di configurazione di CS/AIX di cui è stato effettuato il backup come descritto in "Esecuzione del backup dei file di configurazione di CS/AIX" a pagina 40, attenersi alla seguente procedura:

1. Assicurarsi che CS/AIX non sia attivo. Per stabilire se lo è, immettere il seguente comando:

   snaadmin status_node

   Se CS/AIX è attivo, il comando visualizza informazioni relative allo stato del nodo locale, in caso contrario visualizza un messaggio che indica che CS/AIX non è attivo.

   Se CS/AIX è attivo, immettere il seguente comando per disattivarlo:

   sna stop
2. Immettere i seguenti comandi:

   cd /etc/sna
   restore -x -f *Nomedispositivo*

   In questo comando, *Nomedispositivo* indica il percorso e il nome file del dispositivo utilizzato durante l'esecuzione del backup dei file.

   Questo comando sovrascrive qualsiasi file di configurazione omonimo esistente nella directory **/etc/sna**.

Reinizializzazione dei file di configurazione

Se i file di configurazione di CS/AIX vengono inavvertitamente modificati in maniera tale che le informazioni in essi contenute non possono più essere utilizzate, potrebbe dover essere necessario reinizializzare i file per poter riconfigurare CS/AIX come se fosse stato appena installato. Eseguire la procedura solo se si è certi che le informazioni relative alla configurazione non possono essere recuperate.

Nota: Se si dispone di backup dei file di configurazione validi, è possibile copiare tali file nella directory **/etc/sna** ed utilizzarli per inizializzare il nodo tramite il comando **sna start**.

È possibile reinizializzare i seguenti file di configurazione:

- File di configurazione del nodo **sna_node.cfg**
- File di configurazione del dominio **sna_domn.cfg**
- File di configurazione di TP **sna_tps**
- File del database keyring SSL e file nascosto password

Attenersi alla seguente procedura per reinizializzare i file di configurazione:

1. Chiudere il programma di gestione, se attivo, e disabilitare CS/AIX emettendo il seguente comando:

   sna stop
2. Eseguire il backup dei file di configurazione esistenti, copiando in un'altra ubicazione qualsiasi file oggetto di reinizializzazione.
3. Cancellare i file oggetto di reinizializzazione.
4. Se è stato cancellato il file di configurazione del dominio, emettere il seguente comando per ricrearlo (effettuando una copia del file di configurazione del dominio vuoto fornito con CS/AIX):

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

   Questo comando crea un nuovo file di configurazione del dominio, necessario per avviare CS/AIX.
5. Se è stato cancellato il file database keyring SSL, emettere il seguente comando per ricrearlo (effettuando una copia del file campione fornito con CS/AIX):

   cp -p /usr/lib/sna/samples/ibmcs.* /etc/sna
6. Emettere il seguente comando per riavviare CS/AIX:

   sna start
7. Avviare il programma di gestione Motif:

   xsnaadmin &

   Se il file **sna_node.cfg** non esiste, il programma di gestione richiede la configurazione del nodo. È possibile proseguire, configurando il nodo e le altre risorse così come descritto in Capitolo 8, "Configurazione e utilizzo di CS/AIX", a pagina 71 o *IBM Communications Server for AIX Administration Guide.*

   Se è stato utilizzato un file **sna_node.cfg** valido, il nodo viene inizializzato con il nuovo file di configurazione.

Capitolo 4. Installazione di IBM Remote API Client su Linux

Questo capitolo descrive come installare IBM Remote API Client su Linux, il quale consente a una stazione di lavoro di Linux di eseguire le applicazioni SNA pur non avendo un'installazione stack SNA completa. Remote API Client su Linux può connettersi a uno o più server CS/AIX (o a un server CS di Linux, ma non ad entrambi contemporaneamente) tramite una rete TCP/IP (i server CS di Linux non possono operare nello stesso dominio dei server CS/AIX).

Questo capitolo si applica agli IBM Remote API Client in esecuzione su computer Intel a 32 bit (i686), AMD64/Intel EM64T a 64 bit (x86_64) e pSeries (ppc64). Se si sta installando IBM Remote API Client su un computer System z (s390 / s390x), consultare Capitolo 5, "Installazione di IBM Remote API Client su Linux for System z", a pagina 49.

Il programma di installazione e i rispettivi file, incluso il file README di IBM Remote API Client, si trovano nel CD di installazione, nella directory dedicata al proprio tipo di client:

Tipo di client	Directory sul CD
Intel a 32 bit (i686)	**/ibm-commserver-clients/linux**
AMD64/Intel EM64T a 64 bit (x86_64)	**/ibm-commserver-clients/linux-x86_64**
pSeries (ppc64)	**/ibm-commserver-clients/linux—ppc64**

Si consiglia di leggere il file README di IBM Remote API Client prima di installare il software.

Se si esegue un aggiornamento da una versione precedente di CS/AIX e dei client API remoti, si consiglia di aggiornare tutti i server prima di aggiornare tali client. Per ulteriori informazioni, consultare "Migrazione dai livelli precedenti di CS/AIX" a pagina 32.

Requisiti hardware e software

Requisiti hardware

IBM Remote API Client necessita di un computer supportato da una delle seguenti distribuzioni Linux.

Utilizzare il comando **uname -m** per verificare la classe CPU del computer di destinazione. La seguente tabella mostra l'hardware appropriato per ciascun tipo di client e la risposta del comando **uname -m** per tale hardware.

Tipo di client	Hardware	Risposta del comando uname
Intel a 32 bit	Sistema Intel a 32 bit Pentium II o successivo o sistema basato su Opteron	`i686`
AMD64/Intel EM64T a 64 bit	Sistema x86_64 (AMD64 o Intel EM64T)	`x86_64`
pSeries	Sistema pSeries POWER5 o OpenPower	`ppc64`

Versione del sistema operativo Linux

La versione attuale di IBM Remote API Client è stata testata con le seguenti versioni del sistema operativo Linux. Può essere eseguita ad un livello soddisfacente anche su altre distribuzioni 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)

Per informazioni sui pacchetti opzionali eventualmente richiesti, consultare il file **README** sul CD di installazione.

Java

Se si utilizza l'API CPI-C Java, sarà necessario il software Java. Per ulteriori informazioni, consultare il file **README** sul CD di installazione.

GSKIT (Global Security Kit)

Se il client si connetterà ai server CS/AIX tramite HTTPS, sarà necessario il software GSKIT per consentire l'accesso HTTPS ai server mediante un server WebSphere. Il software GSKIT è incluso nel CD di installazione, ma per installarlo potrebbero essere necessari dei pacchetti aggiuntivi di sistemi operativi Linux; consultare il file **README** sul CD di installazione per informazioni dettagliate sui pacchetti opzionali eventualmente richiesti.

Se, quando si esegue il processo di installazione del client descritto successivamente in questo capitolo, tutti i pacchetti prerequisiti sono già installati, il software GSKIT viene installato automaticamente all'interno di questo processo. In caso contrario, può essere installato successivamente.

Visualizzazione dei dettagli di installazione del prodotto

È possibile visualizzare le informazioni dettagliate relative al client API remoto e ai rispettivi pacchetti software già installati. Per elencare tutti i pacchetti installati, utilizzare il seguente comando:

rpm -q -a

Per visualizzare maggiori dettagli su un pacchetto specifico, utilizzare il seguente comando:

rpm -q -i *nomepacchetto*

nomepacchetto è il nome base del pacchetto installato, ad esempio **ibm-commserver-client**.

Impostazione della variabile d'ambiente della lingua

Utilizzare il seguente comando per modificare la variabile `LANG` per indicare la lingua che si desidera utilizzare:

export LANG=*lingua*

Sostituire *lingua* con l'identificativo della lingua che si desidera utilizzare, che può essere una delle seguenti:

Identificativo	Lingua
en_US	Inglese (Stati Uniti)
ja_JP	Giapponese (PC)
de_DE	Tedesco
es_ES	Spagnolo
fr_FR	Francese
ko_KR	Coreano
pt_BR	Portoghese
zh_CN	Cinese (EUC semplificato)
zh_TW	Cinese (tradizionale)

Installazione di Remote API Client su Linux

Una volta installato il software prerequisito, si è pronti per installare IBM Remote API Client.

Se è già installato un livello precedente di IBM Remote API Client, seguire la procedura descritta nella sezione "Disinstallazione di Remote API Client su Linux" a pagina 47 per eliminarlo prima di installare questo nuovo livello. Qualsiasi informazione relativa alla configurazione verrà lasciata dove si trova, affinché possa essere utilizzata dalla nuova installazione.

1. Accedere con privilegi root.
2. Montare il CD e impostarlo come directory corrente.

   mount /dev/cdrom
   cd /media/cdrom

   Il nome della directory **/media/cdrom** potrebbe essere differente se si ha un'unità DVD. Utilizzare il comando **df** per vedere dove Linux ha montato il CD.
3. Passare alla sottodirectory appropriata del CD ed eseguire lo script shell per installare il client. Il seguente esempio mostra la sottodirectory di **/linux** per un client Intel a 32 bit (i686); se necessario, sostituirla con **/linux-x86_64** o **/linux-ppc64**.

   cd ibm-commserver-clients/linux
   ./installibmcscli

   Lo script shell verificherà alcuni prerequisiti e, se non rispettati, emetterà dei messaggi di avviso. Verrà richiesta la lettura e l'accettazione del contratto di licenza, quindi lo script installerà gli RPM. Se i prerequisiti richiesti sono già installati, lo script installerà anche il software GSKIT.
4. Aggiungere le directory binarie di IBM Remote API Client al proprio PATH. È possibile modificare il proprio profilo affinché questo processo avvenga automaticamente:

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

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

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

   Per le applicazioni CPI-C Java occorre impostare anche la seguente variabile d'ambiente:

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

Per alcune applicazioni potrebbe essere necessario anche impostare la variabile d'ambiente LD_PRELOAD, ma non come modifica generale del proprio profilo:

export LD_PRELOAD=/usr/lib/libpLiS.so

5. Avviare IBM Remote API Client. Dopo l'installazione, ciò avverrà automaticamente al riavvio della macchina. Assicurarsi di essere usciti dalle directory del CD quando si effettua quest'operazione.

   cd /
   sna start

Nota: Prima che IBM Remote API Client possa connettersi ai server tramite HTTPS, è necessario utilizzare il programma di gestione delle chiavi di GSKIT per impostare la configurazione del certificato di sicurezza del client. Per ulteriori informazioni, consultare "Impostazione di certificati di sicurezza HTTPS tramite GSKIT".

Sarà altresì necessario aggiornare il file dei dati di rete del client per specificare i server CS/AIX cui si può collegare il client e il nome del server WebSphere che fornisce supporto HTTPS. Per ulteriori informazioni, consultare la sezione sulla gestione dei client API remoti in *IBM Communications Server for AIX Administration Guide*.

Impostazione di certificati di sicurezza HTTPS tramite GSKIT

Se il client si connetterà ai server CS/AIX tramite HTTPS, dovrà esservi installato il software di gestione delle chiavi GSKIT. Solitamente ciò avviene all'interno dell'installazione del client, posto che i prerequisiti del sistema operativo Linux siano installati come descritto nel file **README** sul CD di installazione. Se GSKIT non è stato installato come parte dell'installazione del client ma ora i prerequisiti sono installati, è possibile installare il software GSKIT eseguendo la seguente procedura.

1. Accedere con privilegi root.
2. Montare il CD e impostarlo come directory corrente.

   mount /dev/cdrom
   cd /media/cdrom

   Il nome della directory **/media/cdrom** potrebbe essere differente se si ha un'unità DVD. Utilizzare il comando **df** per vedere dove Linux ha montato il CD.
3. Passare alla sottodirectory appropriata del CD ed eseguire lo script shell per installare il software GSKIT. Il seguente esempio mostra la sottodirectory di **/linux** per un client Intel a 32 bit (i686); se necessario, sostituirla con **/linux-x86_64** o **/linux-ppc64**.

   cd ibm-commserver-clients/linux
   ./installgskit

Prima che IBM Remote API Client possa connettersi ai server tramite HTTPS, è necessario utilizzare il programma di gestione delle chiavi di GSKIT per impostare la configurazione del certificato di sicurezza del client. Attenersi alla seguente procedura.

1. Eseguire il programma di gestione delle chiavi di GSKIT con il seguente comando:

/opt/ibm/sna/bin/snakeyman

Dall'interfaccia utente del programma di gestione delle chiavi, aprire il file database delle chiavi **/etc/opt/ibm/sna/ibmcs.kdb** che è in formato CMS.

2. La password iniziale per il database delle chiavi è `ibmcs`. Prima di impostare i certificati di sicurezza, **è necessario** modificare questa password per preservare la sicurezza della propria configurazione. Nella finestra di dialogo per la modifica della password, sarà necessario spuntare la casella 'Stash the password to a file?' per assicurarsi che la nuova password venga salvata, in modo tale che il client possa aprire il database delle chiavi.
3. Ottenere una copia del certificato della CA (Certificate Authority) utilizzato per firmare il certificato di sicurezza del server Web e installarla nel database delle chiavi. Per far ciò, selezionare Signer Certificates dall'interfaccia utente del programma di gestione delle chiavi e fare clic su Add.
4. Se il server WebSphere è configurato per richiedere i certificati di sicurezza dei client, il client deve disporre di un certificato emesso da una CA il cui certificato sia presente nel database dei certificati di sicurezza del server Web. Per richiedere un nuovo certificato:
   a. Selezionare Create, New Certificate Request dall'interfaccia utente del programma di gestione delle chiavi e inserire i dati richiesti.
   b. Salvare il certificato, estrarlo in un file e inviarlo alla CA.
   c. Una volta emesso il certificato, memorizzarlo nel database del server Web. Per far ciò, selezionare Personal Certificates dall'interfaccia utente del programma di gestione delle chiavi e fare clic su Receive.

   Come misura temporanea ai fini di una verifica interna, è possibile creare un certificato client autofirmato invece di ottenere un certificato dalla CA. Tuttavia, tale certificato non fornisce il livello di sicurezza richiesto e non deve essere utilizzato in un sistema attivo. Per creare un certificato autofirmato:
   a. Selezionare Create, New Self-Signed Certificate dall'interfaccia utente del programma di gestione delle chiavi e inserire i dati richiesti.
   b. Salvare il certificato ed estrarlo in un file.
   c. Memorizzare il file del certificato in un database del server Web. Per far ciò, selezionare Personal Certificates dall'interfaccia utente del programma di gestione delle chiavi e fare clic su Receive.
5. Al termine della configurazione dei certificati, chiudere il programma di gestione delle chiavi di GSKIT.

Disinstallazione di Remote API Client su Linux

È possibile disinstallare Remote API Client su Linux utilizzando i seguenti comandi.

```
/usr/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
```

Non tutti i pacchetti elencati in questi comandi saranno necessariamente installati su ciascun sistema.

Disinstallazione di Remote API Client su Linux

La disinstallazione di IBM Remote API Client su Linux non eliminerà alcuna informazione relativa alla configurazione personalizzata, affinché possa essere utilizzata da un'installazione successiva.

Capitolo 5. Installazione di IBM Remote API Client su Linux for System z

Questo capitolo descrive come installare IBM Remote API Client su Linux, il quale consente al mainframe System z di eseguire applicazioni SNA pur non avendo un'installazione stack SNA completa. Remote API Client su Linux for System z può connettersi a uno o più server CS/AIX (o CS Linux) tramite una rete TCP/IP.

Si consiglia di leggere il file README di IBM Remote API Client prima di installare il software. Questo file si trova nella directory **/ibm-commserver-clients/linux-systemz** sul CD di installazione.

Se si esegue un aggiornamento da una versione precedente di CS/AIX e dei client API remoti, si consiglia di aggiornare tutti i server prima di aggiornare tali client. Per ulteriori informazioni, consultare "Migrazione dai livelli precedenti di CS/AIX" a pagina 32.

Requisiti hardware e software

Requisiti hardware

IBM Remote API Client necessita di un sistema System z a 31 bit o a 64 bit supportato da una delle distribuzioni Linux elencate in "Versione del sistema operativo Linux".

Utilizzare il comando **uname -m** per verificare la classe CPU. Il risultato deve essere `s390` per un ambiente a 31 bit o `s390x` per un ambiente a 64 bit.

Versione del sistema operativo Linux

La versione attuale di IBM Remote API Client è stata testata con le seguenti versioni del sistema operativo Linux. Può essere eseguito ad un livello soddisfacente anche su altre distribuzioni Linux.

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

Per informazioni sui pacchetti opzionali eventualmente richiesti, consultare il file **README** sul CD di installazione.

Java

Se si utilizza l'API CPI-C Java, sarà necessario il software Java. Per ulteriori informazioni, consultare il file **README** sul CD di installazione.

GSKIT (Global Security Kit)

Se il client si connetterà ai server CS/AIX tramite HTTPS, sarà necessario il software GSKIT per consentire l'accesso HTTPS ai server mediante un server WebSphere. Il software GSKIT è incluso nel CD di installazione, ma per installarlo potrebbero essere necessari dei pacchetti aggiuntivi di sistemi operativi Linux;

consultare il file **README** nella directory **/ibm-commserver-clients/linux-systemz** sul CD di installazione per informazioni dettagliate sui pacchetti opzionali eventualmente richiesti.

Se, quando si esegue il processo di installazione del client descritto successivamente in questo capitolo, tutti i pacchetti prerequisiti sono già installati, il software GSKIT viene installato automaticamente come parte integrante del processo. In caso contrario, può essere installato successivamente.

Visualizzazione dei dettagli di installazione del prodotto

È possibile visualizzare le informazioni dettagliate relative a Remote API Client e ai rispettivi pacchetti software già installati. Per elencare tutti i pacchetti installati, utilizzare il seguente comando:

rpm -q -a

Per visualizzare maggiori dettagli su un pacchetto specifico, utilizzare il seguente comando:

rpm -q -i *nomepacchetto*

nomepacchetto è il nome base del pacchetto installato, ad esempio **ibm-commserver-client**.

Impostazione della variabile d'ambiente della lingua

Utilizzare il seguente comando per modificare la variabile `LANG` per indicare la lingua che si desidera utilizzare:

export LANG=*lingua*

Sostituire *lingua* con l'identificativo della lingua che si desidera utilizzare, che può essere una delle seguenti:

Identificativo	Lingua
en_US	Inglese (Stati Uniti)
ja_JP	Giapponese (PC)
de_DE	Tedesco
es_ES	Spagnolo
fr_FR	Francese
ko_KR	Coreano
pt_BR	Portoghese
zh_CN	Cinese (EUC semplificato)
zh_TW	Cinese (tradizionale)

Installazione di Remote API Client su Linux for System z

Una volta installato il software prerequisito, si è pronti per installare IBM Remote API Client.

Se è già installato un livello precedente di IBM Remote API Client, seguire la procedura descritta nella sezione "Disinstallazione di Remote API Client su Linux for System z" a pagina 53 per eliminarlo prima di installare questo nuovo livello. Qualsiasi informazione relativa alla configurazione verrà lasciata dove si trova, affinché possa essere utilizzata dalla nuova installazione.

1. Copiare o trasferire tramite FTP il file **ibm-commserver-client–6.4.0.0–s390x.tgz** dalla directory **/ibm-commserver-clients/linux-systemz** ubicata sul CD di installazione al sistema Linux System z. Assicurarsi di utilizzare la modalità binaria per copiare o trasferire il file tramite FTP.
2. Accedere al sistema Linux System z come root.
3. Decomprimere il file tar in una directory temporanea vuota:

   mkdir /tmp/ibmcs

   cd /tmp/ibmcs

   tar —xzf ibm-commserver-client–6.4.0.0–s390x.tgz
4. Eseguire lo script shell **installibmcscli**:

   ./installibmcscli

   Questo script shell verifica alcuni prerequisiti e, se non rispettati, emette dei messaggi di avviso. Richiede inoltre all'utente di confermare di aver letto e di accettare i termini della licenza di CS/AIX. È possibile saltare questo messaggio specificando dei parametri aggiuntivi nel comando **installibmcscli**, così come descritto di seguito. Una volta risposto al messaggio, lo script shell installa i pacchetti **rpm**. Se gli opportuni prerequisiti sono già installati, lo script installerà anche il software GSKIT.
5. Aggiungere le directory binarie di IBM Remote API Client al proprio PATH. È possibile modificare il proprio profilo affinché questo processo avvenga automaticamente:

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

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

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

   Se si intende eseguire applicazioni a 64 bit, utilizzare i seguenti comandi:

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

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

   Per applicazioni CPI-C Java impostare anche la seguente variabile d'ambiente:

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

   Per alcune applicazioni potrebbe essere necessario anche impostare la variabile d'ambiente `LD_PRELOAD`, ma non come modifica generale del proprio profilo:

   export LD_PRELOAD=/usr/lib/libpLiS.so
6. Avviare IBM Remote API Client. Dopo l'installazione, ciò avverrà automaticamente al riavvio della macchina. Assicurarsi di essere usciti dalle directory del CD quando si effettua quest'operazione.

   cd /
   sna start
7. Una volta terminata l'installazione, è possibile cancellare il file **tgz** e la directory temporanea creata durante il processo di installazione.

Nota: Prima che IBM Remote API Client possa connettersi ai server tramite HTTPS, è necessario utilizzare il programma di gestione delle chiavi di GSKIT per impostare la configurazione del certificato di sicurezza del client. Per ulteriori informazioni, consultare "Impostazione di certificati di sicurezza HTTPS tramite GSKIT" a pagina 52.

Sarà altresì necessario aggiornare il file dei dati di rete del client per specificare i server CS/AIX a cui si può collegare il client e il nome del server WebSphere che fornisce il supporto HTTPS. Per ulteriori

informazioni, consultare la sezione sulla gestione dei client API remoti in *IBM Communications Server for AIX Administration Guide*.

Impostazione di certificati di sicurezza HTTPS tramite GSKIT

Se il client si connetterà ai server CS/AIX tramite HTTPS, dovrà esservi installato il software di gestione delle chiavi GSKIT. Solitamente ciò avviene all'interno dell'installazione del client, posto che i prerequisiti del sistema operativo Linux siano installati come descritto nel file **README** sul CD di installazione. Se GSKIT non è stato installato durante l'installazione del client ma ora i prerequisiti sono installati, è possibile installare il software GSKIT eseguendo la seguente procedura.

1. Copiare o trasferire tramite FTP il file **ibm-commserver-client–6.4.0.0–s390x.tgz** dalla directory **/ibm-commserver-clients/linux-systemz** ubicata sul CD di installazione al sistema Linux System z. Assicurarsi di utilizzare la modalità binaria per copiare o trasferire il file tramite FTP.
2. Accedere al sistema Linux System z come root.
3. Decomprimere il file tar in una directory temporanea vuota:

   mkdir /tmp/ibmcs

   cd /tmp/ibmcs

   tar —xzf ibm-commserver-client–6.4.0.0–s390x.tgz
4. Eseguire lo shell script **installgskit**:

   ./installgskit
5. Una volta terminata l'installazione, è possibile cancellare il file **tgz** e la directory temporanea creata durante il processo di installazione.

Prima che IBM Remote API Client possa connettersi ai server tramite HTTPS, è necessario utilizzare il programma di gestione delle chiavi di GSKIT per impostare la configurazione del certificato di sicurezza del client. Attenersi alla seguente procedura.

1. Eseguire il programma di gestione delle chiavi di GSKIT con il seguente comando:

   /opt/ibm/sna/bin/snakeyman

   Dall'interfaccia utente del programma di gestione delle chiavi, aprire il file database delle chiavi **/etc/opt/ibm/sna/ibmcs.kdb** che è in formato CMS.
2. La password iniziale per il database delle chiavi è `ibmcs`. Prima di impostare i certificati di sicurezza, **è necessario** modificare questa password per preservare la sicurezza della propria configurazione. Nella finestra di dialogo per la modifica della password, sarà necessario spuntare la casella 'Stash the password to a file?' per assicurarsi che la nuova password venga salvata, in modo tale che il client possa aprire il database delle chiavi.
3. Ottenere una copia del certificato della CA (Certificate Authority) utilizzato per firmare il certificato di sicurezza del server Web e installarla nel database delle chiavi. Per far ciò, selezionare Signer Certificates dall'interfaccia utente del programma di gestione delle chiavi e fare clic su Add.
4. Se il server WebSphere è configurato per richiedere i certificati di sicurezza dei client, il client deve disporre di un certificato emesso da una CA il cui certificato sia presente nel database dei certificati di sicurezza del server Web. Per richiedere un nuovo certificato:
   a. Selezionare Create, New Certificate Request dall'interfaccia utente del programma di gestione delle chiavi e inserire i dati richiesti.
   b. Salvare il certificato, estrarlo in un file e inviarlo alla CA.

c. Una volta emesso il certificato, memorizzarlo nel database del server Web. Per far ciò, selezionare Personal Certificates dall'interfaccia utente del programma di gestione delle chiavi e fare clic su Receive.

Come misura temporanea ai fini di una verifica interna, è possibile creare un certificato client autofirmato invece di ottenere un certificato dalla CA. Tuttavia, tale certificato non fornisce il livello di sicurezza richiesto e non deve essere utilizzato in un sistema attivo. Per creare un certificato autofirmato:

a. Selezionare Create, New Self-Signed Certificate dall'interfaccia utente del programma di gestione delle chiavi e inserire i dati richiesti.
b. Salvare il certificato ed estrarlo in un file.
c. Memorizzare il file del certificato in un database del server Web. Per far ciò, selezionare Personal Certificates dall'interfaccia utente del programma di gestione delle chiavi e fare clic su Receive.

5. Al termine della configurazione dei certificati, chiudere il programma di gestione delle chiavi di GSKIT.

Disinstallazione di Remote API Client su Linux for System z

È possibile disinstallare Remote API Client su Linux for System z utilizzando i seguenti comandi.

```
/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
```

Non tutti i pacchetti elencati in questi comandi saranno necessariamente installati su ciascun sistema.

La disinstallazione di IBM Remote API Client su Linux for System z non eliminerà alcuna informazione relativa alla configurazione personalizzata, affinché possa essere utilizzata da un'installazione successiva.

Capitolo 6. Installazione di IBM Remote API Client su sistemi AIX

Questo capitolo descrive come installare IBM Remote API Client su AIX, il quale consente ad una stazione di lavoro di AIX di eseguire le applicazioni SNA pur non avendo un'installazione stack SNA completa. Remote API Client su AIX può connettersi a uno o più server CS/AIX (o CS Linux) tramite una rete TCP/IP.

Si consiglia di leggere il file README di IBM Remote API Client prima di installare il software. Il file è ubicato nella directory **/ibm-commserver-clients/aix** sul CD di installazione. Se si esegue un aggiornamento da una versione precedente di CS/AIX e dei client API remoti, si consiglia di aggiornare tutti i server prima di aggiornare tali client. Per ulteriori informazioni, consultare "Migrazione dai livelli precedenti di CS/AIX" a pagina 32.

Requisiti hardware e software

Requisiti hardware

IBM Remote API Client necessita di un sistema pSeries supportato da uno dei seguenti sistemi operativi AIX elencati in "Versione del sistema operativo".

Versione del sistema operativo

La versione attuale di IBM Remote API Client è stata testata con le seguenti versioni del sistema operativo:

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

  Il client può essere eseguito nell'ambiente globale o in una WPAR (partizione del carico di lavoro) del sistema o dell'applicazione. Assicurarsi che ogni WPAR in cui viene eseguito il client abbia un nome host univoco che il DNS è in grado di risolvere.

Java

Se si utilizza l'API CPI-C Java, è necessario il software Java. L'ultimo SDK Java, disponibile all'indirizzo http://www.ibm.com/developerworks/java/jdk, soddisfa tutti i requisiti richiesti.

Installare il pacchetto SDK Java con il comando **installp**.

GSKIT (Global Security Kit)

Se il client si connetterà ai server CS/AIX tramite HTTPS, sarà necessario installare il software GSKIT per consentire l'accesso HTTPS ai server mediante un server WebSphere. Per ulteriori informazioni, consultare il file **README** nella directory **/ibm-commserver-clients/aix** sul CD di installazione. Il software GSKIT viene installato nel corso del processo principale di installazione del client, successivamente descritto nel presente capitolo.

Modifica della variabile d'ambiente della lingua

Quando si utilizza Remote API Client, assicurarsi che la variabile LANG non sia impostata su C.

Utilizzare la seguente procedura per visualizzare la variabile LANG in uso o modificarla:

1. Dal menu principale SMIT, selezionare **Ambienti di sistema**.
2. Dal menu SMIT successivo, selezionare **Manage Language Environment**.
3. Dal menu SMIT successivo, selezionare **Change/Show Primary Language Environment**.
4. Dal menu SMIT successivo, selezionare **Change/Show Cultural Convention, Language, or Keyboard**.
5. Selezionare la lingua che si desidera utilizzare. Ad esempio, se si stanno utilizzando i messaggi nella lingua Inglese (Stati Uniti), selezionare en_US.

Installazione di Remote API Client su AIX

Una volta installato il software prerequisito, si è pronti per installare IBM Remote API Client.

Se è già stato installato un livello precedente di IBM Remote API Client, seguire la procedura descritta nella sezione "Disinstallazione di Remote API Client su AIX" a pagina 58 per eliminarlo prima di procedere all'installazione di questo nuovo livello. Qualsiasi informazione relativa alla configurazione verrà lasciata dove si trova, affinché possa essere utilizzata dalla nuova installazione.

Installazione di Remote API Client tramite copia dei file sulla stazione di lavoro AIX in uso

Per installare Remote API Client, attenersi alla seguente procedura.

1. Copiare o trasferire tramite FTP il file **sna.client.6.4.0.0.I** dalla directory **/ibm-commserver-clients/aix** ubicata sul CD-ROM alla stazione di lavoro AIX. Assicurarsi di utilizzare la modalità binaria per copiare o trasferire il file tramite FTP.

   Se il client si connetterà ai server CS/AIX tramite HTTPS, sarà necessario anche copiare o trasferire tramite FTP i due file **gskta.*.I** e **gsksa.*.I** dalla stessa directory sul CD. Questi file contengono il software GSKIT richiesto per l'accesso HTTPS dal client.
2. Accedere alla stazione di lavoro di AIX come root.
3. Installare il client AIX utilizzando **smit** o **installp**. Per istruzioni al riguardo, consultare il file **README** nella directory **/ibm-commserver-clients/aix** sul CD di installazione.
4. Se il client si connetterà ai server CS/AIX tramite HTTPS, installare i file GSKIT seguendo le istruzioni riportate nel file **README**.
5. Una volta completato il processo di installazione, è possibile eliminare il file **sna.client.6.4.0.0.I** e i file GSKIT dalla directory di lavoro.
6. Avviare IBM Remote API Client. Dopo l'installazione, ciò avverrà automaticamente al riavvio della macchina.

   cd /
   sna start

Nota: Prima che IBM Remote API Client possa connettersi ai server tramite HTTPS, è necessario utilizzare il programma di gestione delle chiavi di GSKIT per impostare la configurazione del certificato di sicurezza del client. Per ulteriori informazioni, consultare "Impostazione di certificati di sicurezza HTTPS tramite GSKIT".

Sarà altresì necessario aggiornare il file dei dati di rete del client per specificare i server CS/AIX a cui si può collegare il client e il nome del server WebSphere che fornisce il supporto HTTPS. Per ulteriori informazioni, consultare la sezione sulla gestione dei client API remoti in *IBM Communications Server for AIX Administration Guide*.

Installazione di Remote API Client dal CD

Per installare Remote API Client, attenersi alla seguente procedura.

1. Accedere alla stazione di lavoro di AIX come root.
2. Montare il CD nella stazione di lavoro AIX utilizzando il seguente comando:

   mount -o ro /dev/cd0 /mnt
3. Installare il client AIX utilizzando **smit** o **installp**. Per istruzioni al riguardo, consultare il file **README** nella directory **/ibm-commserver-clients/aix** sul CD di installazione.
4. Se il client si connetterà ai server CS/AIX tramite HTTPS, installare i file GSKIT seguendo le istruzioni riportate nel file **README**.
5. Una volta completato il processo di installazione, smontare il CD utilizzando il seguente comando:

   unmount /mnt
6. Avviare IBM Remote API Client. Dopo l'installazione, ciò avverrà automaticamente al riavvio della macchina. Assicurarsi di essere usciti dalle directory del CD quando si effettua quest'operazione.

   cd /
   sna start

Nota: Prima che IBM Remote API Client possa connettersi ai server tramite HTTPS, è necessario utilizzare il programma di gestione delle chiavi di GSKIT per impostare la configurazione del certificato di sicurezza del client. Per ulteriori informazioni, consultare "Impostazione di certificati di sicurezza HTTPS tramite GSKIT".

Sarà altresì necessario aggiornare il file dei dati di rete del client per specificare i server CS/AIX a cui si può collegare il client e il nome del server WebSphere che fornisce il supporto HTTPS. Per ulteriori informazioni, consultare la sezione sulla gestione dei client API remoti in *IBM Communications Server for AIX Administration Guide*.

Impostazione di certificati di sicurezza HTTPS tramite GSKIT

Prima che IBM Remote API Client possa connettersi ai server tramite HTTPS, è necessario utilizzare il programma di gestione delle chiavi di GSKIT per impostare la configurazione del certificato di sicurezza del client. Attenersi alla seguente procedura.

1. Eseguire il programma di gestione delle chiavi di GSKIT con il seguente comando:

/usr/bin/snakeyman

Dall'interfaccia utente del programma di gestione delle chiavi, aprire il file database delle chiavi **/etc/sna/ibmcs.kdb** che è in formato CMS.

2. La password iniziale per il database delle chiavi è `ibmcs`. Prima di impostare i certificati di sicurezza, **è necessario** modificare questa password per preservare la sicurezza della propria configurazione. Nella finestra di dialogo per la modifica della password, sarà necessario spuntare la casella 'Stash the password to a file?' per assicurarsi che la nuova password venga salvata, in modo tale che il client possa aprire il database delle chiavi.
3. Ottenere una copia del certificato della CA (Certificate Authority) utilizzato per firmare il certificato di sicurezza del server Web e installarla nel database delle chiavi. Per far ciò, selezionare Signer Certificates dall'interfaccia utente del programma di gestione delle chiavi e fare clic su Add.
4. Se il server WebSphere è configurato per richiedere i certificati di sicurezza dei client, il client deve disporre di un certificato emesso da una CA il cui certificato sia presente nel database dei certificati di sicurezza del server Web. Per richiedere un nuovo certificato:
   a. Selezionare Create, New Certificate Request dall'interfaccia utente del programma di gestione delle chiavi e inserire i dati richiesti.
   b. Salvare il certificato, estrarlo in un file e inviarlo alla CA.
   c. Una volta emesso il certificato, memorizzarlo nel database del server Web. Per far ciò, selezionare Personal Certificates dall'interfaccia utente del programma di gestione delle chiavi e fare clic su Receive.

   Come misura temporanea ai fini di una verifica interna, è possibile creare un certificato client autofirmato invece di ottenere un certificato dalla CA. Tuttavia, tale certificato non fornisce il livello di sicurezza richiesto e non deve essere utilizzato in un sistema attivo. Per creare un certificato autofirmato:
   a. Selezionare Create, New Self-Signed Certificate dall'interfaccia utente del programma di gestione delle chiavi e inserire i dati richiesti.
   b. Salvare il certificato ed estrarlo in un file.
   c. Memorizzare il file del certificato in un database del server Web. Per far ciò, selezionare Personal Certificates dall'interfaccia utente del programma di gestione delle chiavi e fare clic su Receive.
5. Al termine della configurazione dei certificati, chiudere il programma di gestione delle chiavi di GSKIT.

Disinstallazione di Remote API Client su AIX

È possibile disinstallare Remote API Client utilizzando i seguenti comandi.

1. Se è in esecuzione, arrestare il software del client utilizzando il seguente comando:

   sna stop
2. Accedere con privilegi root.
3. Eliminare il pacchetto Remote API Client e i pacchetti software associati utilizzando uno dei seguenti comandi.

   Per eliminare il pacchetto tramite **installp**:

   installp —u sna.client

   Per eliminare il pacchetto tramite **smit**:

   smit remove

Capitolo 7. Pianificazione e installazione di Remote API Client su Windows

Questo capitolo descrive come installare IBM Remote API Client su Windows che consente a un PC di eseguire applicazioni SNA pur non avendo un'installazione stack SNA completa sul PC. Remote API Client su Windows può connettersi a uno o più server CS/AIX (o CS Linux) tramite una rete TCP/IP.

Se si esegue un aggiornamento da una versione precedente di CS/AIX e dei client API remoti, si consiglia di aggiornare tutti i server prima di aggiornare tali client. Per ulteriori informazioni, consultare "Migrazione dai livelli precedenti di CS/AIX" a pagina 32.

Esistono due varianti di IBM Remote API Client su Windows che cambiano a seconda dell'hardware specifico e della versione di Windows in uso. Le informazioni contenute in questo capitolo si applicano ad entrambe le varianti, salve le differenze espressamente indicate.

- Il client a 32 bit può essere eseguito su un computer basato su Intel a 32 bit che esegue Microsoft Windows 2000, Windows 2003, Windows XP, Windows Vista a 32 bit o Windows Server 2008 a 32 bit.
- Il client x64 può essere eseguito su computer AMD64 o Intel EM64T che eseguono Microsoft Windows 2003 Server x64 Edition, Windows XP Professional x64 Edition, Windows Vista a 64 bit o Windows Server 2008 a 64 bit.

Le interfacce fornite da IBM Remote API Client su Windows sono ampiamente compatibili con quelle fornite da IBM Communications Server for Windows e dai prodotti Microsoft Host Integration Server.

Il Software Development Kit (SDK) di IBM Remote API Client su Windows è un pacchetto opzionale che consente di utilizzare il client API remoto per sviluppare applicazioni che utilizzano APPC, CPI-C, LUA e le API CSV. Per ulteriori informazioni su tali API, consultare la guida di riferimento per programmatori appropriata. Non è necessario installare questo pacchetto se il client API remoto sarà utilizzato solo per eseguire applicazioni esistenti (e non per svilupparne di nuove).

Requisiti hardware e software

Per eseguire il programma di installazione **Setup** e Remote API Client su Windows, il computer deve soddisfare i seguenti requisiti:

- Deve eseguire uno dei seguenti sistemi operativi. Per informazioni aggiornate sui numeri di versione specifici supportati per ciascuna versione del sistema operativo e su qualsiasi ulteriore requisito applicabile a determinate versioni, consultare le informazioni sul client Windows contenute nel file **README** sul CD di installazione.

  :

  – Per il client Windows a 32 bit:
    - Windows 2000
    - Windows XP
    - Windows 2003

  - Windows Vista a 32 bit
  - Windows Server 2008 a 32 bit
- Per il client Windows x64:
  - Microsoft Windows XP Professional x64 Edition
  - Microsoft Windows 2003 Server x64 Edition
  - Windows Vista a 64 bit
  - Windows Server 2008 a 64 bit

- Deve avere accesso ad uno o più server CS/AIX tramite uno dei seguenti meccanismi:
  - Accesso al server tramite rete TCP/IP
  - Accesso a un server WebSphere che fornisce l'accesso HTTPS ai server CS/AIX.

Nota: A seconda della versione di Windows in uso o delle funzioni specifiche di Remote API Client che si desidera utilizzare, per poter installare e utilizzare Remote API Client su Windows potrebbe essere necessario eseguire ulteriori configurazioni. Per ulteriori dettagli, consultare le informazioni sul client Windows contenute nel file **README** sul CD di installazione.

Accesso al programma di installazione

Remote API Client e il software SDK, il software GSKIT e il programma **Setup** sono inclusi nel CD di installazione in formato Windows, affinché possano essere installati dal CD sul computer Windows. È necessario installare il software Remote API Client su ciascun PC client Windows; in tal modo si installa automaticamente anche il software GSKIT. SDK è necessario solo se il client verrà utilizzato per sviluppare nuove applicazioni tramite le API remote di Windows e non è richiesto se il client verrà utilizzato solo per eseguire applicazioni esistenti.

L'immagine di installazione di Remote API Client su Windows è un file eseguibile ZIP autoestraente, fornito sul CD di installazione.

- Per quanto riguarda il client a 32 bit, il file **i_w32cli.exe** si trova nella directory **/ibm-commserver-clients/windows** sul CD.
- Per quanto riguarda il client x64, il file **i_w64cli.exe** si trova nella directory **/ibm-commserver-clients/win-x64** sul CD.

Questo file può essere copiato su altri PC Windows tramite la rete, affinché l'installazione possa avvenire anche senza accesso diretto al CD di CS/AIX. Quando si utilizza l'eseguibile, quest'ultimo decomprime l'immagine di installazione ed esegue automaticamente il programma **Setup**. Se si desidera semplicemente decomprimere l'immagine di installazione in una directory temporanea, ad esempio per eseguire il programma **Setup** dalla riga comando, caricare l'eseguibile ZIP autoestraente nel proprio programma di decompressione.

La prima volta che si esegue il programma **Setup** su un determinato computer, il programma viene eseguito dalla fonte selezionata. Tale programma gestisce tutto il processo di installazione, imposta una configurazione di base e installa e crea una propria icona. Terminata l'installazione, è possibile utilizzare il programma **Setup** (selezionandolo dal File Manager o selezionando la rispettiva icona)nel caso in cui sia necessario reinstallare il software.

Una volta estratta l'immagine di installazione di Remote API Client in una directory temporanea, è possibile installare il software in uno dei due seguenti modi:

- Eseguire il programma **Setup** tramite Windows, come illustrato in "Installazione di Remote API Client su Windows tramite il programma di installazione". Per installare SDK è necessario utilizzare questo metodo.
- Immettere il comando **setup** dalla riga comando, così come illustrato in "Installazione del software Remote API Client dalla riga comando" a pagina 65. Questo metodo non consente l'installazione di SDK.

Nota: Prima che IBM Remote API Client possa connettersi ai server tramite HTTPS, è necessario aggiornare il file dei dati di rete del client per specificare i server CS/AIX ai quali si può collegare il client e il nome del server WebSphere che fornisce il supporto HTTPS. Per ulteriori informazioni, consultare la sezione sulla gestione dei client API remoti in *IBM Communications Server for AIX Administration Guide*.

Installazione di Remote API Client su Windows tramite il programma di installazione

Eseguire automaticamente il programma **Setup** nell'ambito dell'utilizzo dell'eseguibile ZIP autoestraente **i_w32cli.exe** (per client a 32 bit) o **i_w64cli.exe** (per client x64) oppure manualmente dalla riga comando. Il programma visualizza innanzitutto la schermata Choose Setup Language.

1. Selezionare la lingua da utilizzare per l'installazione e la configurazione di Remote API Client, quindi **OK**.

   Il programma visualizza la schermata Welcome di presentazione del programma **Setup**.
2. Selezionare **Next** per proseguire con l'installazione.

   Il programma visualizza il Contratto di licenza software, da leggere e comprendere.
3. Se si accettano le condizioni di concessione della licenza, selezionare **Accept** per proseguire.

   Il programma chiede di specificare una directory di destinazione in cui installare i file.
4. Inserire la directory di destinazione.

   Il programma chiede di scegliere il tipo di installazione desiderata:

   Standard
   Selezionare questa opzione se non occorre installare SDK. SDK è necessario solo se il client verrà utilizzato per sviluppare nuove applicazioni tramite le API remote di Windows e non è richiesto se il client verrà utilizzato solo per eseguire applicazioni esistenti.

   Developer
   Selezionare questa opzione se è necessario installare SDK, ossia se il client verrà utilizzato per sviluppare nuove applicazioni tramite le API remote di Windows.

   Nota: Per installare SDK è necessario selezionare **Developer**.
5. Scegliere il tipo di installazione.

Il programma richiede successivamente l'immissione del nome della cartella del programma in cui devono essere visualizzate le icone di Remote API Client su Windows.

6. Immettere il nome della cartella.
7. Se la directory System contiene già file **.DLL** con nomi uguali a quelli dei file utilizzati da questo programma **Setup** ma non si tratta di file Remote API Client (ad esempio file di un altro software SNA), il programma chiede di seguire una delle seguenti procedure:
   - Copiare i file **.DLL** di Remote API Client sui file **.DLL** esistenti
   - Copiare i file **.DLL** esistenti in una sottodirectory denominata **OTHERSNA** all'interno della directory di installazione e installare i file **.DLL** di Remote API Client. Questa opzione consente di ripristinare le impostazioni originali precedenti all'installazione di Remote API Client nel caso in cui venissero successivamente disinstallati i file (consultare "Disinstallazione del software Remote API Client" a pagina 69).
   - Annullare l'installazione del software del client.

   Se i file **.DLL** di Remote API Client sono già presenti, il programma **Setup** visualizza un messaggio al riguardo. I nuovi file **.DLL** sovrascriveranno i file **.DLL** esistenti solo se questi ultimi hanno numeri di versione inferiori a quelli dei file **.DLL** del programma **Setup**.
8. A questo punto, il programma **Setup** copia i file dalla fonte specificata e li installa dove appropriato. Durante questo processo, una barra delle informazioni visualizza la percentuale di completamento dell'installazione. I file **.DLL** vengono copiati nella directory System o in una directory equivalente, mentre gli altri file vengono copiati nella directory di destinazione specificata nella fase 2. Durante ciascuna operazione di trasferimento dei file, nel file **setup.log** creato nella directory specificata viene scritto un record. Se uno qualsiasi dei file da sovrascrivere è "di sola lettura" o se uno qualunque dei file non può essere copiato per qualunque altro motivo, i nuovi file vengono eliminati e l'utente riceve un messaggio che lo invita a visionare il file **setup.log**.
9. Se la sorgente da cui viene eseguito il programma **Setup** non contiene tutti i file richiesti, il programma chiede il nome di una directory. Immettere il nome della directory in cui sono ubicati i file.

   Se le informazioni specificate non sono sufficienti per localizzare le copie dei file di Remote API Client, il programma visualizza nuovamente questa schermata.
10. Una volta copiati i file richiesti, il programma **Setup** visualizza la finestra Configuration.

    I valori di configurazione predefiniti vengono presi dal file di configurazione del dominio. Per ulteriori informazioni, consultare *IBM Communications Server for AIX Administration Guide*. Se non si desidera utilizzare questi valori predefiniti, è possibile configurarli come mostrato di seguito:

    Domain
    Specificare il nome del dominio client/server di CS/AIX.

    Se il client utilizza l'indirizzamento IPv6, è necessario configurare le seguenti impostazioni. Se il client utilizza l'indirizzamento IPv4, tali impostazioni sono facoltative.

    Server Name
    La schermata mostra un elenco di non più di nove server a cui il client può connettersi. L'ordine di visualizzazione dei server

nell'elenco corrisponde all'ordine in cui il client li seleziona. Se il client non può connettersi al primo server dell'elenco, prova con il server successivo.

Se il client utilizza l'indirizzamento IPv6, è necessario configurare almeno un server. Se il client utilizza l'indirizzamento IPv4 e si utilizza l'opzione *trasmissioni UDP* non occorre specificare alcun server; se non riesce a contattare alcun server tramite le trasmissioni UDP e si specifica uno o più server, il client proverà a turno con questi.

- Per aggiungere un nuovo server all'elenco, utilizzare il pulsante **Add**.
- Per eliminare un server dall'elenco, selezionare il server e utilizzare il pulsante **Remove**.
- Per spostare un server su o giù nell'elenco, selezionare il server e utilizzare i pulsanti di scorrimento accanto all'elenco.

Se il client si trova nella stessa rete privata dei rispettivi server e vi accede tramite TCP/IP, ciascun server viene identificato semplicemente dal suo nome server.

Se il client accede ai suoi server tramite HTTPS, è necessario identificare ciascun server specificando il nome del server WebSphere che fornisce il supporto HTTPS e il nome del server CS/AIX nel seguente formato:

nomeserverweb **:** *nomeserver1*

Ciò presuppone che WebSphere sia impostato per utilizzare la porta predefinita 443 per le connessioni HTTPS. Se il proprio amministratore di rete ha configurato WebSphere per l'utilizzo di un numero di porta differente, includere il numero della porta nel seguente formato:

nomeserverweb **:** *numeroporta* **:** *nomeserver1*

Per ulteriori dettagli sulla configurazione di WebSphere affinché supporti le connessioni HTTPS, consultare "Configurazione di WebSphere Application Server" a pagina 37.

UDP broadcasts

Specificare se questo client utilizzerà le trasmissioni UDP per connettersi a un server. Quando questa opzione è selezionata, il client invia trasmissioni UDP tramite la rete, al fine di localizzare una connessione server invece che di cercare di connettersi direttamente a un server specifico.

L'impostazione predefinita prevede l'utilizzo di trasmissioni UDP. Per modificare questa impostazione, fare clic sulla casella.

Se il client utilizza l'indirizzamento IPv6, le trasmissioni UDP non sono supportate. Disattivare l'opzione per l'utilizzo delle trasmissioni UDP e specificare almeno un *Nome server*.

Le seguenti impostazioni sono facoltative:

Advanced

Per fornire ulteriori valori in sostituzione dei valori predefiniti dal programma **Setup**, fare clic sul pulsante **Advanced** in fondo alla finestra. Il programma **Setup** visualizza la finestra Advanced Options che contiene le impostazioni avanzate per la configurazione del client Windows. Le impostazioni predefinite di questi parametri sono

appropriate per la maggior parte degli utenti, quindi non sarà probabilmente necessario modificare le impostazioni di questa finestra di dialogo.

Per ulteriori informazioni su questi parametri, consultare "Opzioni avanzate per la configurazione di Remote API Client".

Per ulteriori informazioni su qualsiasi impostazione o parametro di configurazione, fare clic su **Help**.

11. Una volta compilata la finestra Configuration, fare clic su **OK**. Se la schermata non è stata compilata in maniera appropriata, il programma **Setup** visualizza un messaggio.
12. Una volta completata l'installazione, viene visualizzata la finestra Finish. È possibile selezionare una delle seguenti azioni, o entrambe, da eseguire alla chiusura del programma di installazione:

    View README file
    Visualizzare il file **README**.

    Start client
    Iniziare ad eseguire questo client CS/AIX.

    Selezionare **Finish** per chiudere il programma di installazione.

Opzioni avanzate per la configurazione di Remote API Client

La finestra Advanced Options consente di configurare alcuni parametri avanzati di Remote API Client. La maggior parte degli utenti non ha bisogno di modificare questi parametri, ma, se necessario, le impostazioni predefinite possono essere adeguate.

LAN access time-out
Specificare per quanto tempo, in secondi, la connessione del client a un server può rimanere inattiva prima che venga chiusa. Se questa casella di spunta non è selezionata, non è stato specificato alcun timeout di accesso LAN (e quindi verrà utilizzato un timeout infinito). Se si spunta la casella, è possibile inserire un valore di timeout, in secondi, nel campo adiacente. Il valore minimo è `60` (che indica 60 secondi); se si lascia la casella vuota o si specifica un valore inferiore a `60`, il client API remoto utilizza il valore minimo `60`.

Max. broadcast attempts
Specificare il numero massimo di volte per cui il client può cercare di connettersi a un server tramite trasmissione. Se la finestra Advanced Options è aperta, viene visualizzato il valore predefinito `5`. Il valore di questa casella viene utilizzato solo se la casella di spunta delle trasmissioni UDP della finestra principale Configuration è selezionata.

Reconnect time-out
Specificare quanto tempo, in secondi, il client deve attendere prima di tentare di riconnettersi a un server dall'arresto di quest'ultimo. Se la finestra Advanced Options è aperta, viene visualizzato il valore predefinito `200`.

Per ulteriori informazioni su questi parametri, premere **Help**.

Una volta compilata la finestra Advanced Options, fare clic su **OK**. Se la schermata è stata compilata in maniera adeguata, il programma **Setup** ritorna alla finestra

Configuration. Se si installa un nuovo client API remoto, ritornare alla fase 11 a pagina 64. In caso contrario, fare clic sul pulsante **OK** della finestra di dialogo Configuration per completare la configurazione.

Installazione del software Remote API Client dalla riga comando

Nota: Per installare SDK, è necessario utilizzare il programma **Setup**, così come illustrato in "Installazione di Remote API Client su Windows tramite il programma di installazione" a pagina 61. Non è possibile installare SDK dalla riga comando.

Una volta estratta l'immagine di installazione di Remote API Client in una directory temporanea, è possibile installare il software Remote API Client dalla riga comando invece che utilizzando il programma **Setup** tramite Windows. Nella riga comando, immettere il comando **setup** con una o più opzioni. È possibile immettere queste opzioni in maiuscolo o in minuscolo e farle precedere da / (barra) o da - (trattino). Se un parametro, quale *cartella*, è una stringa che contiene uno spazio, è necessario inserire la stringa tra virgolette.

Una volta immesso il comando **setup**, il programma **Setup** chiede qualsiasi informazione non sia già stata inclusa nella riga comando e visualizza messaggi di conferma in corrispondenza delle varie fasi dell'installazione. Se non si desidera ricevere richieste dal programma **Setup**, utilizzare l'opzione **-accept -s** per eseguire il programma in modalità non presidiata, accettando i termini del Contratto di licenza software.

Le opzioni del comando **setup** sono le seguenti:

-? Visualizzare un elenco delle opzioni della riga comando. Corrisponde all'opzione **-h**.

-h Visualizzare un elenco delle opzioni della riga comando. Corrisponde all'opzione **-?**.

-accept -s
Eseguire l'installazione in modalità non presidiata, accettando i termini del Contratto di licenza software. Il Contratto è disponibile nella sottodirectory **License** dell'immagine di installazione di Windows.

L'opzione **-s** deve essere l'ultima della riga comando e occorre accertarsi di aver indicato il nome del dominio (utilizzando l'opzione **-i**), nonché qualsiasi altro parametro si desideri specificare. Se l'installazione viene eseguita in modalità non presidiata non viene richiesto alcun parametro, né vengono visualizzati messaggi di conferma. Qualsiasi argomento della riga comando successivo a **-s** viene ignorato.

-f2 Specificare il nome del percorso completo del file di registrazione dell'installazione creato durante l'installazione in modalità non presidiata (tramite l'opzione **-s**).

Se non si specifica questa opzione, il file viene creato come **setup.log** nella directory da cui si esegue il programma di installazione. Se si esegue l'installazione in modalità non presidiata dall'unità CD, è necessario specificare questa opzione per garantire che il file venga creato nel proprio computer (non potendo essere creato nell'unità CD).

-k*cartella*
Specificare la cartella del programma.

-p*directory*
Specificare la directory di installazione.

-i*dominio*
Specificare un nome dominio per questo client. Questo parametro è obbligatorio; non esistono valori predefiniti.

-w*directory*
Specificare la directory di origine contenente i file del software del client CS/AIX nel caso in cui sia ubicata su un dischetto o su un CD. In caso contrario, utilizzare l'opzione **-v**.

-v*server*
Specificare il server da cui devono essere scaricati i file del software del client. È possibile specificare il nome del server o l'indirizzo TCP/IP. Se si copiano i file di origine da un dischetto o da un CD, utilizzare l'opzione **-w** invece dell'opzione **-v**.

-l*server*
Specificare un server da includere nell'elenco dei server ai quali può avere accesso questo client.

Se il client si trova nella stessa rete privata dei rispettivi server e vi accede tramite TCP/IP, ciascun server viene identificato semplicemente dal proprio nome server.

Se il client accede ai propri server tramite HTTPS, è necessario identificare ciascun server specificando il nome del server WebSphere che fornisce il supporto HTTPS e il nome del server CS/AIX nel seguente formato:

nomeserverweb **:** *nomeserver1*

Ciò presuppone che WebSphere sia impostato per utilizzare la porta predefinita 443 per le connessioni HTTPS. Se il proprio amministratore di rete ha configurato WebSphere per l'utilizzo di un numero di porta differente, includere il numero della porta nel seguente formato:

nomeserverweb **:** *numeroporta* **:** *nomeserver1*

Per ulteriori dettagli sulla configurazione di WebSphere affinché supporti le connessioni HTTPS, consultare "Configurazione di WebSphere Application Server" a pagina 37.

-o Sovrascrivere i file **.DLL** esistenti. Se i file **.DLL** di Remote API Client sono già presenti, il programma **Setup** li sovrascrive anche se hanno un numero di versione superiore a quello dei file **.DLL** del programma **Setup**.

-y Salvare i file **.DLL** esistenti. Se i file **.DLL** di Remote API Client sono già presenti nelle directory richieste, il programma **Setup** copia i file **.DLL** esistenti in una sottodirectory della directory di installazione e poi installa i file **.DLL** di Remote API Client. Le copie nella sottodirectory garantiscono, in caso di disinstallazione del software Remote API Client, che il processo venga completato.

-n Annullare l'installazione se vengono trovati i file **.DLL** di Remote API Client.

-a*timeout*
Specificare il timeout di accesso LAN in secondi. Indica per quanto tempo la connessione del client a un server può rimanere inattiva prima di esser chiusa. Il valore `0` indica nessun timeout.

-b*numero massimo trasmissioni*
Specificare il numero massimo di tentativi di trasmissione UDP. Una trasmissione UDP è un tentavo del client di connettersi a uno qualsiasi dei server del dominio invece che a un server specifico. Il valore `0` indica che non vengono effettuati tentativi di trasmissione.

-j*timeout di riconnessione*
Specificare quanto tempo, in secondi, il client deve attendere prima di tentare di riconnettersi a un server dall'arresto di quest'ultimo.

Di seguito viene mostrata una riga comando di esempio per l'installazione di Remote API Client:

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

In questo esempio:

- Il client è installato nel dominio **my_domain**.
- Il client ha accesso a due server nella stessa rete privata del client e non utilizza trasmissioni UDP per contattare qualsiasi altro server. Se perde il contatto con un server, attende 30 secondi prima di riconnettersi.
- L'installazione viene eseguita in modalità non presidiata, scrivendone le informazioni di registrazione dell'installazione nel file **C:\instrapi.log** sul client.
- Le copie esistenti dei file **.DLL** di Remote API Client vengono salvate in una sottodirectory prima dell'installazione dei nuovi file.

Impostazione di certificati di sicurezza HTTPS tramite GSKIT

Prima che IBM Remote API Client possa connettersi ai server tramite HTTPS, è necessario utilizzare il programma di gestione delle chiavi di GSKIT per impostare la configurazione del certificato di sicurezza del client. Attenersi alla seguente procedura.

1. Eseguire il programma di gestione delle chiavi di GSKIT, ossia *dirinstall***snakeyman.exe**. *dirinstall* rappresenta la directory in cui è stato installato il software del client, ossia **C:\IBMCS\w32cli** (per client a 32 bit) o **C:\IBMCS\w64cli** (per client a 64 bit), a meno che non sia stata specificata un'ubicazione differente durante l'installazione del client.

   Dall'interfaccia utente del programma di gestione delle chiavi, aprire il file database delle chiavi *diristall***ibmcs.kdb** che è informato CMS.
2. La password iniziale per il database delle chiavi è `ibmcs`. Prima di impostare i certificati di sicurezza, **è necessario** modificare questa password per preservare la sicurezza della propria configurazione. Nella finestra di dialogo per la modifica della password, sarà necessario spuntare la casella 'Stash the password to a file?' per assicurarsi che la nuova password venga salvata, in modo tale che il client possa aprire il database delle chiavi.
3. Ottenere una copia del certificato della CA (Certificate Authority) utilizzato per firmare il certificato di sicurezza del server Web e installarla nel database delle chiavi. Per far ciò, selezionare Signer Certificates dall'interfaccia utente del programma di gestione delle chiavi e fare clic su Add.
4. Se il server WebSphere è configurato per richiedere i certificati di sicurezza dei client, il client deve disporre di un certificato emesso da una CA il cui certificato sia presente nel database dei certificati di sicurezza del server Web. Per richiedere un nuovo certificato:

a. Selezionare Create, New Certificate Request dall'interfaccia utente del programma di gestione delle chiavi e inserire i dati richiesti.
b. Salvare il certificato, estrarlo in un file e inviarlo alla CA.
c. Una volta emesso il certificato, memorizzarlo nel database del server Web. Per far ciò, selezionare Personal Certificates dall'interfaccia utente del programma di gestione delle chiavi e fare clic su Receive.

Come misura temporanea ai fini di una verifica interna, è possibile creare un certificato client autofirmato invece di ottenere un certificato dalla CA. Tuttavia, tale certificato non fornisce il livello di sicurezza richiesto e non deve essere utilizzato in un sistema attivo. Per creare un certificato autofirmato:

a. Selezionare Create, New Self-Signed Certificate dall'interfaccia utente del programma di gestione delle chiavi e inserire i dati richiesti.
b. Salvare il certificato ed estrarlo in un file.
c. Memorizzare il file del certificato in un database del server Web. Per far ciò, selezionare Personal Certificates dall'interfaccia utente del programma di gestione delle chiavi e fare clic su Receive.

5. Al termine della configurazione dei certificati, chiudere il programma di gestione delle chiavi di GSKIT.

Personalizzazione del software Remote API Client dopo l'installazione

Qualsiasi impostazione personalizzata può essere modificata in qualunque momento successivo all'installazione iniziale, eseguendo il programma **Configuration Utility**, appartenente al gruppo di programmi di CS/AIX. Il programma visualizza la stessa finestra Configuration visualizzata nel processo di installazione iniziale. È possibile modificare le informazioni di qualsiasi campo, seguendo la procedura descritta in "Installazione di Remote API Client su Windows tramite il programma di installazione" a pagina 61.

Se i file SDK non sono stati installati durante l'installazione iniziale e ora si desidera aggiungerli, eseguire nuovamente il programma di installazione e selezionare il tipo di installazione **Developer**.

Reinstallazione del software Remote API Client

È possibile reinstallare il software Remote API Client in qualsiasi momento, ad esempio se si desidera aggiornare il software.

Per far ciò, eseguire il programma di installazione come precedentemente descritto, seguendo le istruzioni indicate in "Installazione di Remote API Client su Windows tramite il programma di installazione" a pagina 61 o "Installazione del software Remote API Client dalla riga comando" a pagina 65. Il programma **Setup** visualizza l'ubicazione da cui sono stati copiati i file del software del client durante l'installazione iniziale. Fare clic su **OK** per ricevere nuove copie dei file da questa stessa ubicazione. Se si fa clic su **OK**, il programma **Setup** copia i file e ritorna alla schermata Options.

Nota: Se si reinstalla il software Remote API Client in modalità non presidiata (come descritto in "Installazione del software Remote API Client dalla riga comando" a pagina 65), potrebbe dover essere necessario riavviare il computer per completare l'installazione. Ciò avviene poiché alcuni file del programma potrebbero essere in uso durante il processo di installazione (ad esempio se Remote API Client è in esecuzione) e quindi potrebbero non poter essere sostituiti dai nuovi file. In questo caso, i nuovi file vengono

copiati in una directory temporanea per essere poi rispostati automaticamente al successivo riavvio del computer.

Per verificare se è necessario riavviare il computer, utilizzare un editor di testo quale **Blocco note** per visualizzare il contenuto del file di registrazione dell'installazione una volta terminato il processo di installazione. Il file di registrazione dell'installazione è denominato **setup.log** e viene creato nella directory da cui si esegue il programma di installazione, a meno che non si utilizzi l'opzione della riga comando **-f2** per specificare un nome file e un percorso differenti.

Alla fine del file, il testo `Result Code` sotto il titolo `Response Result` dovrebbe essere seguito da uno o due valori `0` (zero) o `-12`. Se il valore è `0`, non è necessario riavviare il computer, se il valore è `-12`, riavviare il computer prima di tentare di utilizzare il client Windows.

Disinstallazione del software Remote API Client

È possibile disinstallare il software Remote API Client in qualsiasi momento, utilizzando l'opzione **Installazione applicazioni** del Pannello di controllo di Windows. Una volta confermato il completamento del processo di disinstallazione, Windows effettua le seguenti operazioni:

- Elimina tutti i file installati.
- Se durante l'installazione iniziale sono stati salvati dei file **.DLL** in una sottodirectory, ripristina i file nella loro ubicazione originale.
- Se vuota, cancella la sottodirectory in cui sono stati memorizzati i file **.DLL** salvati.
- Se la cartella Program e la directory creata sono vuote, le rimuove.
- Se la disinstallazione avviene correttamente, elimina il file **setup.log** contenente tutte le eliminazioni e i trasferimenti di file.
- Visualizza un messaggio che comunica che la disinstallazione è avvenuta correttamente o che l'utente deve controllare il file **setup.log** poiché parte dell'installazione non è stata eseguita correttamente.

Il pulsante **Esci** riporta l'utente a Windows.

Disinstallazione del software Remote API Client dalla riga comando

Invece di utilizzare l'opzione **Installazione applicazioni** del Pannello di controllo di Windows, è possibile disinstallare il software Remote API Client dalla riga comando. Utilizzare il seguente comando:

dirinstall\sxcluninst -y

- *dirinstall* è la directory in cui è stato installato il software del client, ossia **C:\IBMCS\w32cli** (per client a 32 bit) o **C:\IBMCS\w64cli** (per client a 64 bit), a meno che non sia stata specificata un'ubicazione differente durante l'installazione del client.
- L'opzione **-y** funge da conferma, al fine di evitare l'utilizzo accidentale del comando.

Il programma di disinstallazione si completa senza messaggi e senza bisogno di ulteriori immissioni da parte dell'utente.

Guida

È possibile accedere alla guida in qualsiasi momento, premendo il tasto **F1**. Anche le finestre Configuration e Advanced Options dispongono del pulsante **Help**.

Capitolo 8. Configurazione e utilizzo di CS/AIX

Il modo più facile per definire e modificare la configurazione di CS/AIX è utilizzare il programma di gestione Motif (**xsnaadmin**). Questo programma fornisce una GUI da cui è possibile visualizzare e gestire le risorse SNA sul nodo locale. Si possono utilizzare anche altri strumenti di gestione quali il programma di gestione Web o la gestione da riga comando, ma si consiglia l'utilizzo del programma Motif.

Il programma di gestione Motif include schermate della guida che forniscono informazioni riepilogative su SNA e CS/AIX, informazioni di riferimento sulle finestre di dialogo di CS/AIX e una guida per l'esecuzione di attività specifiche. Per ciascuna attività (ad esempio la configurazione del nodo) o tipo di comunicazione (quali TN3270 e APPC), il programma guida l'utente nell'impostazione della configurazione delle risorse richieste.

Il programma di gestione Motif permette di impostare tutti i parametri richiesti per le configurazioni CS/AIX standard. Per quanto riguarda i parametri avanzati, il programma di gestione Motif fornisce i valori predefiniti. È necessario fornire solo le informazioni essenziali relative alla configurazione che consentono di impostare le comunicazioni SNA in maniera semplice e veloce.

Il programma di gestione Motif può essere utilizzato anche per gestire il sistema CS/AIX in esecuzione. Il programma di gestione consente di eseguire e applicare le modifiche alla configurazione mentre CS/AIX è attivo e fornisce un accesso agevole alle informazioni di stato riguardanti le risorse del nodo.

Il programma di gestione Motif visualizza automaticamente le informazioni di stato relative alle risorse di CS/AIX. La maggior parte di queste informazioni viene mostrata nella finestra Node (consultare "Gestione di CS/AIX con il programma di gestione Motif" a pagina 74). Inoltre, è possibile controllare alcune risorse — quali nodi e stazioni di collegamento — tramite i pulsanti **Start** e **Stop** della finestra Node. Altre risorse vengono sempre avviate e arrestate automaticamente, pertanto non necessitano di un controllo manuale.

Nota:

1. Per definire o modificare le risorse di CS/AIX è necessario appartenere al gruppo di accesso `sistema`.
2. Per utilizzare il programma di gestione Motif, è necessario disporre di un LFT (Low-Function Terminal) o di un X-terminal. In caso contrario è possibile utilizzare l'interfaccia SMIT (System Management Interface Tool) o il programma di gestione Web che fornisce funzionalità analoghe a quelle del programma Motif. Per ulteriori informazioni, consultare *IBM Communications Server for AIX Administration Guide*.
3. Per ulteriori informazioni sull'interfaccia utente del programma di gestione Motif, inclusi i pulsanti e le icone visualizzati nelle rispettive finestre, consultare le schermate della guida del programma o *IBM Communications Server for AIX Administration Guide*.
4. Le finestre e le finestre di dialogo del programma di gestione Motif potrebbero differire da quelle mostrate in questa guida a seconda delle scelte operate in una determinata finestra di dialogo.

Per ulteriori informazioni sugli altri strumenti di gestione di CS/AIX, incluse la gestione Web, la gestione da riga comando e le applicazioni NOF, consultare *IBM Communications Server for AIX Administration Guide*, *IBM Communications Server for AIX Administration Command Reference* o *IBM Communications Server for AIX NOF Programmer's Guide*.

Pianificazione della configurazione di CS/AIX

Prima di apportare qualsiasi modifica alla configurazione è molto importante effettuare un'attenta pianificazione. Le modifiche apportate possono causare disturbi non solo agli utenti del proprio nodo locale, ma potenzialmente anche agli utenti di tutta la rete.

Potrebbe essere utile tracciare un diagramma delle modifiche apportate alla topologia della rete. Se si aggiungono o si eliminano connessioni ad altri nodi, tracciare un disegno che mostri sia il proprio nodo che gli altri nodi. È possibile utilizzare il programma di gestione Motif per raccogliere le informazioni relative alla configurazione di tutte le connessioni esistenti e aggiungere tali informazioni al proprio diagramma.

Quando si aggiungono nuove risorse al proprio diagramma, si vede facilmente se queste replicano le risorse esistenti o se i nomi sono in conflitto. Analogamente, il diagramma può aiutare a decidere quali risorse debbano essere eliminate e ad evitare di cancellare quelle essenziali.

Se si configura un sistema CS/AIX client/server con più di un nodo, assicurarsi di includere nel diagramma tutti i nodi di CS/AIX e le rispettive risorse di connettività. Successivamente, è possibile configurare ciascun nodo singolarmente, così come descritto nel presente capitolo, eseguendo una configurazione analoga a quella di un nodo standalone.

Una volta determinate le modifiche da effettuare, raccogliere le informazioni necessarie relative alla configurazione. Per guidare l'utente nella raccolta delle informazioni relative alla configurazione di funzioni specifiche di CS/AIX, è possibile utilizzare i fogli di lavoro per le attività forniti nella guida in linea del programma di gestione Motif o i fogli di lavoro per la pianificazione forniti in *IBM Communications Server for AIX Administration Guide*.

Questo capitolo fornisce istruzioni per la configurazione delle funzioni disponibili in CS/AIX più frequentemente utilizzate. Per ciascuna attività di configurazione, questa guida indica inoltre le informazioni da raccogliere prima di configurare la risorsa.

Nota: La guida non fornisce descrizioni dettagliate delle informazioni relative alla configurazione da immettere nelle finestre di dialogo di CS/AIX. Per ulteriori informazioni sui campi di una particolare finestra di dialogo, consultare la guida in linea relativa a quella determinata finestra di dialogo del programma di gestione Motif o dell'interfaccia SMIT.

Fogli di lavoro per la pianificazione

Prima di iniziare a configurare le risorse di CS/AIX, raccogliere tutti i dati relativi alla configurazione delle nuove risorse. Per registrare tutte le informazioni relative a una determinata funzione o applicazione da supportare, utilizzare i fogli di lavoro per la pianificazione forniti in *IBM Communications Server for AIX Administration Guide*.

Sarà probabilmente necessario raccogliere le informazioni relative alla configurazione da differenti fonti, quali gli amministratori di rete, gli amministratori dell'host, i programmatori dell'applicazione e gli utenti finali.

Se si cerca di connettersi a un altro nodo, l'amministratore di quel nodo è un contatto principale. L'amministratore di un nodo può comunicare i nomi, gli indirizzi e le caratteristiche di tutte le risorse di quel nodo. Spesso, sarà necessario garantire che nel nodo locale e nel nodo remoto vengano immessi parametri di configurazione corrispondenti.

Fogli di lavoro per le attività

Le schermate della guida in linea del programma di gestione Motif contengono fogli di lavoro per le attività che forniscono una guida su specifiche attività di configurazione. I fogli di lavoro per le attività contengono puntatori per tutte le schermate della guida concernenti le finestre di dialogo che verranno utilizzate per immettere le informazioni relative alla configurazione. Inoltre, possono essere utilizzati per navigare nella guida e vedere esattamente quali dati devono essere raccolti.

I fogli di lavoro per le attività fanno riferimento anche a guide più dettagliate su ogni singola finestra o finestra di dialogo da utilizzare per immettere le informazioni relative alla configurazione. Queste schermate della guida illustrano ciascun campo da compilare o selezionare.

Utilizzo del programma di gestione Motif

Prima di utilizzare il programma di gestione Motif, si potrebbe desiderare di aggiungere al proprio file **.login** o **.profile** delle informazioni relative al percorso per consentire al sistema di trovare i programmi eseguibili (consultare "Come specificare il percorso ai programmi di CS/AIX"). Inoltre, per poter utilizzare il programma di gestione occorre prima abilitare il software di CS/AIX (consultare).

Per informazioni su come richiamare il programma di gestione Motif e per una panoramica sull'utilizzo del programma, consultare "Gestione di CS/AIX con il programma di gestione Motif" a pagina 74.

Come specificare il percorso ai programmi di CS/AIX

Per eseguire i programmi di CS/AIX, è necessario specificare il percorso alla directory contenente l'eseguibile dei programmi di CS/AIX. È possibile specificare il percorso aggiungendo la directory alla propria variabile d'ambiente `PATH` prima di eseguire i programmi per la prima volta o includendo il nome della directory ogni volta che si eseguono i programmi.

Il programma di gestione Motif è memorizzato nella directory **/usr/bin/X11** e gli altri programmi sono memorizzati nella directory **/usr/bin**. Se si aggiungono queste directory alla definizione della variabile d'ambiente `PATH` nel proprio file **.login** o **.profile**, CS/AIX localizza i programmi automaticamente. In alternativa, è possibile specificare il nome della directory quando si esegue il programma, come illustrato nei seguenti esempi:

/usr/bin/sna start

/usr/bin/X11/xsnaadmin

Le righe di comando d'esempio mostrate in questo manuale partono dal presupposto che le directory siano state aggiunte alla propria variabile d'ambiente PATH e che non siano stati inclusi i nomi delle directory.

Abilitazione di CS/AIX

Prima di poter configurare o gestire il nodo locale, è necessario che CS/AIX venga abilitato sul sistema locale. Così come con qualsiasi applicazione X/Motif, potrebbe anche essere necessario impostare la variabile d'ambiente DISPLAY al fine di indicare un server X adeguato.

Solitamente, CS/AIX viene abilitato automaticamente al termine dell'installazione del software. Se CS/AIX è stato disabilitato, è possibile riabilitarlo immettendo il seguente comando nel prompt dei comandi di AIX:

sna start

Nota: Quando si utilizza il comando **sna start**, il software di CS/AIX utilizza la directory da cui è stato emesso come directory di lavoro corrente e mantiene uno o più descrittori file aperti in quella directory. Ciò significa che non sarà possibile smontare il file system che contiene quella directory mentre il software di CS/AIX è in esecuzione. Per evitare problemi, avviare il software di CS/AIX da una directory su un file system che non deve essere smontato; ad esempio, si potrebbe utilizzare cd / per modificare la directory root prima di utilizzare il comando **sna start**.

Quando si installa CS/AIX, l'utilità di installazione aggiorna automaticamente il file di avvio **/etc/inittab** per aggiungere una voce a **/etc/rc.sna** comprendente il comando **sna start**. Ciò garantisce che CS/AIX venga avviato automaticamente all'avvio del sistema. Se non si desidera che CS/AIX venga avviato automaticamente, è possibile eliminare questa riga o impostarla come commento, quindi seguire le istruzioni riportate in questa sezione per abilitare manualmente il software di CS/AIX.

CS/AIX scrive messaggi al dispositivo di errore standard (solitamente la schermata del proprio terminale) per indicare che è in corso l'inizializzazione e comunicare se l'inizializzazione è stata completata correttamente.

Gestione di CS/AIX con il programma di gestione Motif

Per utilizzare il programma di gestione Motif per CS/AIX, accertarsi innanzitutto che CS/AIX venga inizializzato come descritto in "Abilitazione di CS/AIX" (potrebbe anche essere necessario impostare la variabile d'ambiente DISPLAY per indicare un server X adeguato).

Per avviare il programma di gestione Motif in background, emettere il seguente comando:

xsnaadmin &

CS/AIX visualizza la finestra Domain. Questa finestra mostra tutti i nodi definiti e consente di avviare e arrestare i nodi. Fare doppio clic su qualsiasi nodo richiami la finestra Node per quel nodo, come mostrato in Figura 4 a pagina 76.

La finestra Node mostra informazioni sul nodo e le rispettive risorse. Se il nodo non è ancora stato configurato, il programma di gestione ne richiede la configurazione come descritto in "Configurazione del nodo" a pagina 80.

Nota: Questa guida utilizza il termine finestra per descrivere le finestre Motif che visualizzano informazioni sulle risorse di CS/AIX. Una finestra può contenere una o più sezioni o riquadri. Una finestra di dialogo è una finestra Motif in cui è possibile immettere delle informazioni.

La finestra Node mostra gran parte delle informazioni necessarie e offre un accesso agevole a qualsiasi altro elemento. Visualizza inoltre tutte le risorse chiave presenti sul nodo locale.

Se si configura un sistema CS/AIX client/server con più di un nodo, seguire le istruzioni di questo capitolo per configurare ogni nodo individualmente (ritornando alla finestra Domain per selezionare il nodo successivo).

Dal menu **Windows** della finestra Node è possibile accedere ad altre finestre, tra cui:

- Finestra LU Pools
- Finestra CPI-C Destination Names

Il menu **Services** della finestra Node offre uno strumento rapido per l'aggiunta di risorse e un aiuto per le attività di configurazione e gestione. Il menu **Diagnostics** porta alle finestre di dialogo Logging e Tracing.

Finestra Node

Figura 4 a pagina 76 offre un esempio della finestra Node. La barra del titolo mostra il nome del sistema AIX.

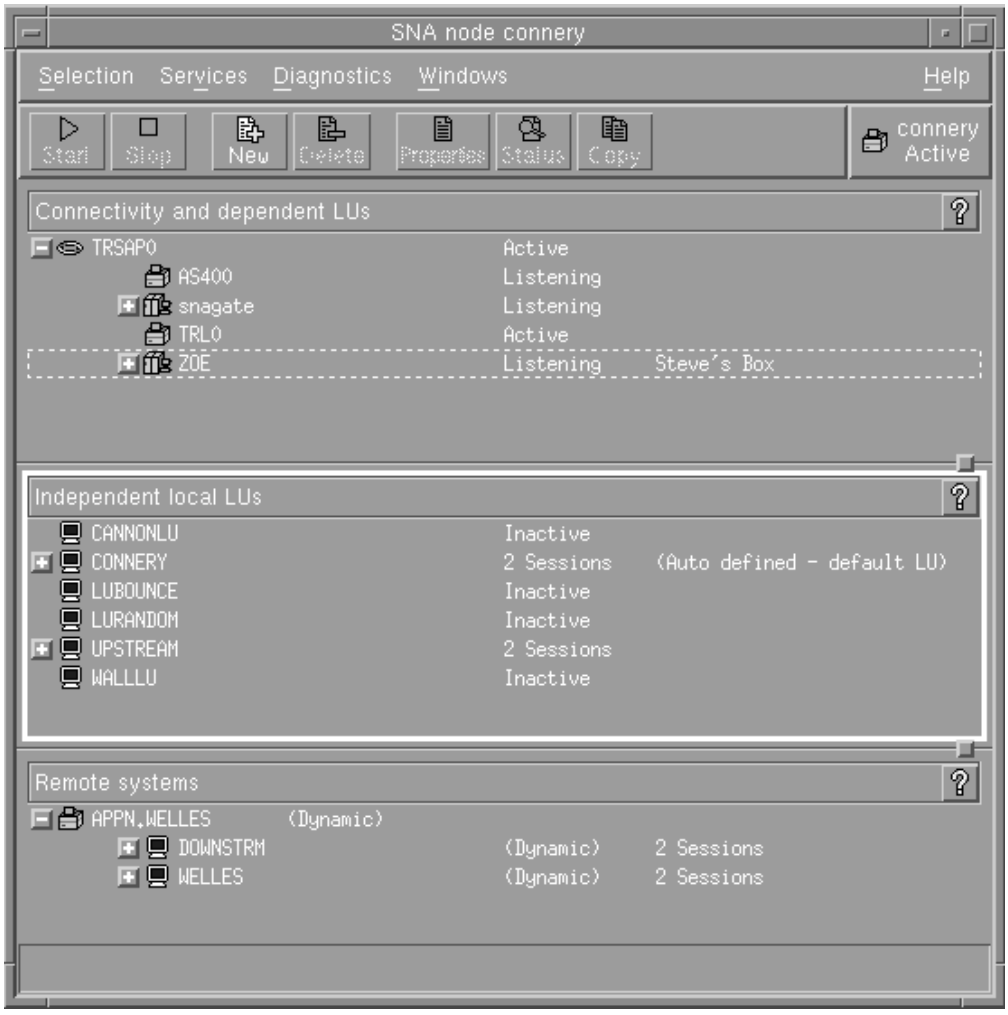

Figura 4. Finestra Node

Dalla finestra Node è possibile configurare e gestire tutte le risorse e i componenti del nodo di CS/AIX.

- Porte
- Stazioni di collegamento
- LU di tipo 0-3 e LU dipendenti di tipo 6.2
- PU interne DLUR
- LU locali indipendenti
- Nodi remoti
- LU partner

Tutte queste risorse possono essere aggiunte, eliminate, modificate e gestite dalla finestra Node. La disposizione delle risorse nella finestra mostra le relazioni tra le risorse e consente di controllare quali risorse vengono visualizzate.

Porte, LU locali e nodi remoti vengono sempre visualizzati. La finestra Node visualizza ogni stazione di collegamento al di sotto della sua porta principale e ogni LU dipendente al di sotto della sua stazione di collegamento principale. Mostra inoltre le LU partner al di sotto delle LU locali e dei nodi remoti.

La finestra Node contiene sezioni distinte per i differenti tipi di risorse relative al nodo:

- La casella Node posta nell'angolo in alto a destra della finestra Node indica se il nodo è `Active` o `Inactive`.
- Il riquadro superiore della finestra Node (Connectivity) elenca le risorse di connettività relative al nodo, incluse le porte, le stazioni di collegamento o le PU su ciascuna porta e le LU dipendenti su una specifica stazione di collegamento o PU. Questa finestra mostra informazioni sullo stato corrente di ciascuna risorsa.
- Il riquadro centrale (Independent Local LU) mostra le LU indipendenti definite sul nodo locale. Questa finestra visualizza inoltre informazioni sulle sessioni che utilizzano una particolare LU e qualsiasi record definisca l'ubicazione di una LU partner tramite la stazione di collegamento utilizzata per accedervi.
- Il riquadro inferiore (Remote Systems) visualizza informazioni sui nodi remoti e le LU partner. Mostra inoltre informazioni sulle sessioni per ogni nodo remoto o LU partner.

È possibile selezionare uno qualsiasi di questi riquadri, facendo clic sul riquadro stesso. Inoltre, è possibile selezionare risorse specifiche all'interno di un riquadro, facendo clic sulla riga della risorsa. Per visualizzare o modificare la configurazione di una voce, fare doppio clic sulla voce (per accedere alle informazioni relative alla configurazione di determinate risorse è possibile utilizzare i pulsanti e i menu della finestra).

Per ciascuna voce elencata, le rispettive risorse sono nidificate all'interno delle informazioni relative alla voce stessa. Ad esempio, le stazioni di collegamento sono raggruppate sotto la porta a cui appartengono. È possibile fare clic sul pulsante **Expand** (+) posto accanto a una voce per visualizzarne le risorse non visualizzate attualmente o fare clic sul pulsante **Contract** (−) per nasconderne le risorse.

Le seguenti attività di gestione possono essere svolte dalla finestra Node:

Avviare o arrestare una risorsa
Selezionare la risorsa e fare clic sul pulsante **Start** o **Stop** (in alternativa, è possibile selezionare **Start item** o **Stop item** dal menu **Selection**).

Aggiungere una risorsa per una voce
Selezionare la voce e fare clic sul pulsante **New** (o selezionare **New** dal menu **Selection**). Ad esempio, per aggiungere una stazione di collegamento per una porta, selezionare la porta e fare clic sul pulsante **New**.

Eliminare una risorsa
Selezionare la risorsa e fare clic sul pulsante **Delete** (o selezionare **Delete** dal menu **Selection**).

Visualizzare o modificare la configurazione di qualsiasi risorsa
Selezionare la risorsa e fare clic sul pulsante **Properties** (o selezionare **Properties** dal menu **Selection**).

Ricevere informazioni sullo stato di qualsiasi risorsa
Selezionare la risorsa e fare clic sul pulsante **Status** (o selezionare **Status** dal menu **Selection**).

Copiare la configurazione di qualsiasi risorsa
Selezionare la risorsa e fare clic sul pulsante **Copy** (o selezionare **Copy** dal menu **Selection**).

Inoltre, è possibile selezionare attività di configurazione specifiche per il nodo dal menu **Services**, controllare la registrazione (per il dominio) e la traccia (per il nodo) dal menu **Diagnostics** e visualizzare o modificare le risorse del dominio selezionando una delle voci del menu **Windows**.

Voci delle risorse

La disposizione delle risorse nella finestra mostra le relazioni tra tali elementi.

Se ad una voce sono associate una o più voci secondarie, accanto ad essa viene visualizzato il simbolo **Expand** (+) o **Contract** (–):

- Il simbolo **Expand** indica che le voci secondarie associate sono nascoste. Per visualizzarli, è possibile fare clic sul simbolo **Expand** o premere il tasto **+** sulla tastiera numerica.
- Il simbolo **Contract** indica che vengono visualizzate le voci secondarie. Per nasconderle, fare clic sul simbolo **Contract** o premere il tasto **–** della tastiera numerica.
- Se accanto alla voce non c'è nessun simbolo, ad essa non è associata alcuna risorsa secondaria.

Ad esempio, una stazione di collegamento è associata a una determinata porta. Nel riquadro Connectivity della finestra Node, la stazione di collegamento viene visualizzata al di sotto della sua porta principale insieme a tutte le altre stazioni di collegamento associate a quella porta. La porta viene sempre visualizzata, ma è possibile scegliere se visualizzare o nascondere l'elenco di stazioni di collegamento associate. Analogamente, è possibile espandere le stazioni di collegamento con un elenco di LU associate per visualizzare le LU o ridurle per nasconderle.

Una risorsa principale deve sempre essere configurata prima delle rispettive risorse secondarie e l'eliminazione della risorsa principale comporta anche l'eliminazione di tutte le rispettive risorse secondarie.

Pulsanti della barra degli strumenti

Le finestre delle risorse includono dei pulsanti della barra degli strumenti per agevolare l'esecuzione delle funzioni più comuni. La Figura 5 mostra una barra degli strumenti di CS/AIX.

Figura 5. Barra degli strumenti di CS/AIX

Non tutti i pulsanti vengono visualizzati nelle barre degli strumenti di ciascuna finestra delle risorse. Se l'operazione di un pulsante non è valida per la voce attualmente selezionata (o se un'operazione richiede la selezione di una voce, ma nessuna voce è selezionata), il riquadro del pulsante viene visualizzato in grigio e la funzione non può essere selezionata (facendo clic sul pulsante non si ottiene alcun effetto). Nelle finestre delle risorse possono essere visualizzati i seguenti pulsanti:

Start Avvia la voce selezionata.

Stop Arresta la voce selezionata.

New Aggiunge una nuova voce alla risorsa.

Delete Elimina le risorse selezionate.

Properties
Apre la finestra di dialogo della voce selezionata per visualizzare o modificare la configurazione della voce.

Status Visualizza lo stato corrente della voce selezionata.

Copy Copia la voce selezionata. Facendo clic su questo pulsante si apre una finestra di dialogo i cui campi riproducono la configurazione della voce selezionata. Per aggiungere una nuova risorsa, compilare i campi della finestra di dialogo (immettendo il nome della nuova voce).

Numerose risorse, quali le porte e le stazioni di collegamento, non possono essere modificate mentre sono attive. Tuttavia, è possibile visualizzare i parametri di una risorsa attiva selezionando la risorsa e facendo clic sul pulsante **Properties** per aprirne la finestra di dialogo. Una volta terminato, fare clic sul pulsante **Close**.

Configurazione delle funzioni client/server

Questa sezione è rilevante solo se CS/AIX è stato installato per essere eseguito in un ambiente client/server (con più nodi CS/AIX nella stessa rete).

In un ambiente client/server, è possibile contrassegnare un server come server di configurazione; CS/AIX conserva un elenco di tali server. Il primo server elencato corrisponde al server master, mentre tutti gli altri sono server di backup. I server vengono elencati in ordine, affinché il secondo server elencato (il primo server di backup) subentri qualora il server master non sia disponibile, il terzo (il secondo server di backup) subentri qualora né il master, né il primo server di backup siano disponibili e così via.

Se uno qualsiasi dei nodi del dominio è attivo, il primo server di configurazione disponibile nel dominio (ossia il primo server che può essere contattato e il cui software CS/AIX sia in esecuzione) assume il ruolo di server master. Se il master corrente diventa non disponibile (perché non può essere contattato, probabilmente per un errore della rete, o perché il software SNA in esecuzione è stato arrestato), il primo server di configurazione disponibile dell'elenco diventa il nuovo master.

CS/AIX può essere eseguito senza un master. Ciò avviene se non si riesce a contattare nessuno dei server dell'elenco dei server di configurazione. In tal caso, le risorse del nodo possono essere visualizzate e configurate solo sui server contattabili.

Nota: Non è possibile indicare direttamente quale nodo debba fungere da server master: il server master viene selezionato in base all'ordine in cui i nodi vengono aggiunti all'elenco dei server di configurazione. Se si desidera spostare un server in cima all'elenco, eliminare tutti gli altri nodi dall'elenco e riaggiungerli.

Nella finestra Domain del programma di gestione Motif, è possibile aggiungere un server di configurazione selezionando **Make configuration server** dal menu **Selection**. Il server viene aggiunto in fondo all'elenco e diventa il server master solo se non è disponibile nessuno degli altri server di configurazione. Per eliminare un server, selezionare **Remove configuration server** dal menu **Selection**.

Nota: Non è possibile eliminare un server se si tratta dell'unico server elencato su cui è in esecuzione il software di CS/AIX, poiché in questo caso non vi sono altri server che possano subentrare in qualità di server master. Nella configurazione client/server è necessario almeno un server master abilitato.

Per ulteriori informazioni sulla configurazione e sulla gestione del sistema CS/AIX client/server, consultare *IBM Communications Server for AIX Administration Guide*. Questo manuale fornisce anche informazioni sulla configurazione avanzata client/server, incluso come spostare i client e i server in differenti domini CS/AIX e come configurare i dettagli di funzionamento del client.

Configurazione del nodo

Il primo passo per la configurazione di CS/AIX in un sistema è la configurazione del nodo locale. La configurazione del nodo offre le informazioni di base di cui necessita il nodo per comunicare in una rete SNA. Per poter definire la connettività o altre risorse del nodo è necessario innanzitutto configurare il nodo stesso.

Se il nodo è già stato configurato, è possibile utilizzare le procedure descritte in questa sezione per modificare la configurazione del nodo, che dev'essere tuttavia arrestato prima di apportare tali modifiche.

Prima di configurare il nodo, decidere se configurarlo come nodo APPN o come nodo non APPN. Questa decisione dipende dalle funzionalità degli altri nodi SNA con cui si comunica.

La Figura 6 mostra un nodo CS/AIX che comunica direttamente con un computer host.

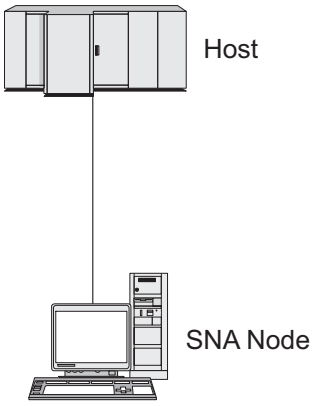

Figura 6. Nodo CS/AIX che comunica direttamente con un host

Se l'host non supporta l'APPN, configurare il nodo CS/AIX come un nodo LEN. Se l'host supporta l'APPN, è possibile configurare il nodo CS/AIX come un nodo della rete APPN o come un nodo finale APPN (se CS/AIX utilizza la rete SNA solo per comunicare con l'host, probabilmente si desidererà configurare il nodo CS/AIX come nodo finale o come BrNN).

Per vedere vari nodi CS/AIX in una rete APPN, consultare Figura 7 a pagina 81.

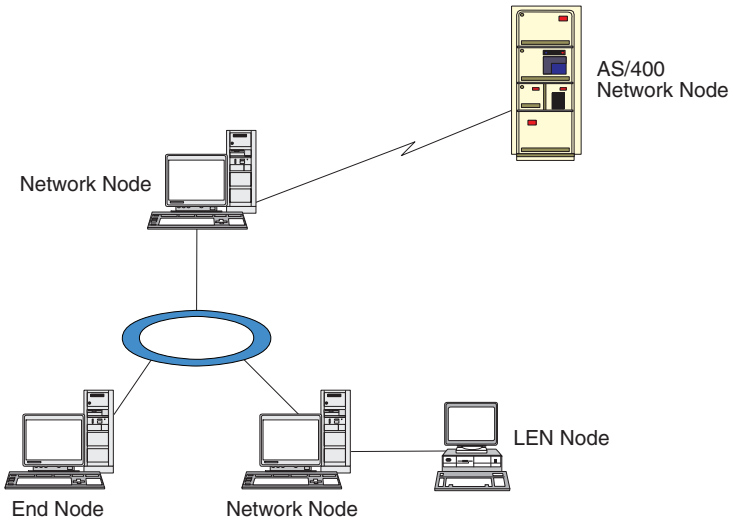

Figura 7. Nodi CS/AIX in una rete APPN

Se il nodo locale appartiene a una rete APPN, configurarlo come nodo della rete APPN qualora debba fornire servizi di instradamento APPN ad altri nodi. Se altri nodi forniscono servizi di instradamento, configurare il nodo locale come nodo finale APPN. Se il nodo locale comunica solo con un nodo connesso direttamente (di qualsiasi tipo esso sia), configurare il nodo come nodo LEN.

Prima di iniziare la configurazione del nodo, raccogliere le seguenti informazioni:

- Tipo di supporto APPN (nodo di rete, BrNN, nodo finale o nodo LEN).
- Nome del punto di controllo (e alias, se differente). Consultare il proprio responsabile della pianificazione della rete per determinare tale nome.
- ID nodo predefinito (il valore predefinito può essere sovrascritto durante la configurazione di un singolo collegamento di comunicazione).

Per configurare il nodo, eseguire quanto segue dalla finestra Node:

1. Selezionare **Configure node parameters** dal menu **Services** o fare doppio clic sulla casella Node nell'angolo in alto a destra della finestra Node. CS/AIX visualizza la finestra di dialogo Node Parameters.
2. Specificare il livello di supporto APPN, il nome del punto di controllo e, se necessario, l'ID del nodo predefinito.
3. Fare clic sul pulsante **OK** per definire il nodo. Una volta definito il nodo, CS/AIX definisce automaticamente una LU predefinita attribuendole lo stesso nome del punto di controllo.

   Per terminare senza salvare i valori immessi, fare clic sul pulsante **Cancel**.

Configurazione della connettività

Affinché un nodo CS/AIX possa comunicare con altri nodi, è necessario configurare la connettività con almeno un nodo adiacente. È possibile configurare un collegamento di connessione affinché supporti il traffico dipendente, il traffico indipendente o entrambi.

Nel proprio computer possono essere installate schede che supportano uno o più protocolli di collegamento. La maggior parte delle informazioni da immettere per

la configurazione della connettività dipende dal protocollo di collegamento in uso. Per un elenco dei protocolli di collegamento supportati da CS/AIX, consultare “Requisiti di installazione” a pagina 20.

Per configurare un collegamento, è necessario definire una porta e (nella maggior parte dei casi) una stazione di collegamento. Se si utilizza il programma di gestione Motif, il sistema configura automaticamente un controllo collegamento dati (DLC, Data Link Control) durante il processo di configurazione della porta. Inoltre, è possibile definire la porta come appartenente a una rete di connessione.

I collegamenti necessari per la configurazione dipendono dal risultato desiderato e dal fatto che la rete sia una rete APPN. Le informazioni richieste dipendono dal protocollo di collegamento e dal tipo di collegamento (per il traffico dipendente, per il traffico indipendente o per entrambi).

A titolo esemplificativo, questa sezione illustra come configurare i seguenti tipi di collegamento:

- Collegamento che supporta il traffico dipendente con un sistema host tramite linea SDLC.
- Collegamento che supporta sia il traffico dipendente sia quello indipendente in una rete APPN tramite il protocollo di collegamento Ethernet. Questo esempio definisce inoltre una rete di connessione sulla porta Ethernet.
- Collegamento Enterprise Extender in una rete APPN (notare che i collegamenti Enterprise Extender supportano solo il traffico indipendente).

Per altri protocolli di collegamento, consultare *IBM Communications Server for AIX Administration Guide* o la guida in linea del programma di gestione Motif.

Configurazione di un collegamento SDLC per il traffico dipendente

Per una porta SDLC (Synchronous Data Link Control) sono necessarie le seguenti informazioni:

- Nome della porta SNA (solitamente si può usare quello predefinito). Occorre fornire anche il numero del dispositivo SDLC.
- Eventuale attivazione automatica della porta all’avvio del nodo.
- Tipo di linea (linea commutata in uscita, linea commutata in entrata o linea dedicata).
- Ruolo del collegamento (primario, secondario, negoziabile, multidrop primario, o multi-PU secondario).
- Indirizzo di interrogazione (solo per una linea commutata in entrata o per una porta non primaria). Per altri tipi di porta, configurare l’indirizzo di interrogazione sulla stazione di collegamento.

  Per le linee commutate in entrata e le linee dedicate, occorrono anche la codifica (NRZ o NRZI) e le impostazioni del duplex (half o full). Per altri tipi di porta, configurare la codifica e le impostazioni del duplex sulla stazione di collegamento.
- Tipo di collegamento fisico (per identificare il tipo di modem).
- Stringa di composizione del numero (necessaria solo per una linea commutata in entrata). Per una linea commutata in uscita, configurare la stringa di composizione del numero sulla stazione di collegamento.

Per una stazione di collegamento SDLC, sono necessarie le seguenti informazioni aggiuntive:

- Metodo di attivazione (tramite amministratore, all'avvio del nodo o su richiesta).
- Tipo di traffico supportato (per questo esempio, solo dipendente).
- Ruolo del nodo remoto (per questo esempio, host).

Per configurare il collegamento SDLC, eseguire quanto segue dalla finestra Node:

1. Configurare la porta:
   a. Selezionare il riquadro Connectivity della finestra.
   b. Selezionare **New port** dal sottomenu **Connectivity** del menu **Services** (o fare clic sul pulsante **New** nella barra dei pulsanti).
   c. Nella successiva finestra di dialogo, selezionare il tipo di protocollo dal menu delle opzioni, quindi scegliere di definire una porta.

      Se si fa clic sul pulsante **OK**, CS/AIX visualizza la finestra di dialogo SDLC Port.
   d. Immettere i valori appropriati nei campi della finestra di dialogo.
   e. Fare clic sul pulsante **OK** per definire la porta.

      La porta viene visualizzata nel riquadro Connectivity della finestra Node.
2. Definire una stazione di collegamento nella porta:
   a. Assicurarsi di aver selezionato la porta a cui deve essere aggiunta la stazione di collegamento nel riquadro Connectivity della finestra Node.
   b. Selezionare **New link station** dal sottomenu **Connectivity** del menu **Services** (o fare clic sul pulsante **New** nella barra dei pulsanti).
   c. Fare clic sul pulsante **OK**.

      CS/AIX visualizza la finestra di dialogo SDLC Link Station.
   d. Immettere i valori appropriati nei campi della finestra di dialogo.
   e. Fare clic sul pulsante **OK** per definire la stazione di collegamento.

      La stazione di collegamento viene visualizzata sotto la porta a cui appartiene nel riquadro Connectivity della finestra Node.

Configurazione di un collegamento Ethernet per supportare il traffico dipendente e indipendente

Questo esempio mostra come configurare un collegamento Ethernet che supporta sia il traffico dipendente sia quello indipendente in una rete APPN. Inoltre, definisce una rete di connessione sulla porta Ethernet.

Per una porta Ethernet, sono necessarie le seguenti informazioni:

- Nome della porta SNA (solitamente si può usare quello predefinito). In caso di più schede di rete Ethernet, occorre fornire anche il numero della scheda Ethernet. È necessario, inoltre, specificare il numero del punto di accesso al servizio (SAP, Service Access Point) locale (solitamente `04`).
- Indicazione sull'attivazione automatica della porta all'avvio del nodo.
- Nome della rete di connessione (deve essere lo stesso su tutte le porte della stessa rete di connessione).

Per una stazione di collegamento Ethernet, sono necessarie le seguenti informazioni aggiuntive:

- Metodo di attivazione (tramite amministratore, all'avvio del nodo o su richiesta).

- Tipo di traffico supportato (per questo esempio, sia dipendente che indipendente).
- Nome del punto di controllo del nodo remoto (necessario solo per un nodo LEN).
- Tipo di nodo remoto (nodo di rete, nodo finale o rileva).
- Ruolo del nodo remoto (per questo esempio, gateway SNA in downstream o DLUR pass-through).
- Per configurare una stazione di collegamento selettiva, sono necessari l'indirizzo MAC (Medium Access Control) e il numero SAP (solitamente `04`) della stazione remota. Se non si forniscono informazioni sull'indirizzo e nel campo *Activation* si specifica `By administrator`, la stazione di collegamento è una stazione di collegamento di ascolto non selettiva.

Per configurare il collegamento Ethernet, eseguire quanto segue dalla finestra Node:

1. Configurare la porta:
   a. Selezionare il riquadro Connectivity della finestra.
   b. Selezionare **New port** dal sottomenu **Connectivity** del menu **Services** (o fare clic sul pulsante **New** nella barra dei pulsanti).
   c. Nella successiva finestra di dialogo, selezionare il tipo di protocollo dal menu delle opzioni, quindi scegliere di definire una porta.

      Se si fa clic sul pulsante **OK**, CS/AIX visualizza la finestra di dialogo Ethernet SAP.
   d. Immettere i valori appropriati nei campi della finestra di dialogo.
   e. Fare clic sul pulsante **OK** per definire la porta.

      La porta viene visualizzata nel riquadro Connectivity della finestra Node.
2. Definire una stazione di collegamento nella porta:
   a. Assicurarsi di aver selezionato la porta a cui deve essere aggiunta la stazione di collegamento nel riquadro Connectivity della finestra Node.
   b. Selezionare **New link station** dal sottomenu **Connectivity** del menu **Services** (o fare clic sul pulsante **New** nella barra dei pulsanti).
   c. Fare clic sul pulsante **OK**.

      CS/AIX visualizza la finestra di dialogo Ethernet Link Station.
   d. Immettere i valori appropriati nei campi della finestra di dialogo.
   e. Fare clic sul pulsante **OK** per definire la stazione di collegamento.

      La stazione di collegamento viene visualizzata sotto la porta a cui appartiene nel riquadro Connectivity della finestra Node.

Configurazione di un collegamento Enterprise Extender

Questo esempio mostra come configurare un collegamento Enterprise Extender in una rete APPN. I collegamenti Enterprise Extender supportano solo il traffico LU indipendente.

Per una porta Enterprise Extender, sono necessarie le seguenti informazioni:

- Nome della porta SNA (solitamente si può usare quello predefinito). In caso di più schede di rete che eseguono l'IP, occorre fornire anche il nome dell'interfaccia IP da utilizzare (ad esempio `eth0`).
- Indicazione sull'attivazione automatica della porta all'avvio del nodo.

Per una stazione di collegamento Enterprise Extender, sono necessarie le seguenti informazioni aggiuntive:

- Metodo di attivazione (tramite amministratore, all'avvio del nodo o su richiesta).
- Tipo di nodo remoto (nodo di rete, nodo finale o rileva).
- Per configurare una stazione di collegamento selettiva, è necessario il nome host IP o l'indirizzo IP della stazione remota. Se non si forniscono queste informazioni e nel campo *Activation* si specifica `By administrator` la stazione di collegamento è una stazione di collegamento di ascolto non selettiva.

Per configurare il collegamento Enterprise Extender, eseguire quanto segue dalla finestra Node:

1. Configurare la porta:
   a. Selezionare il riquadro Connectivity della finestra.
   b. Selezionare **New port** dal sottomenu **Connectivity** del menu **Services** (o fare clic sul pulsante **New** nella barra dei pulsanti).
   c. Nella successiva finestra di dialogo, selezionare il tipo di protocollo dal menu delle opzioni, quindi scegliere di definire una porta.

      Se si fa clic sul pulsante **OK**, CS/AIX visualizza la finestra di dialogo IP Port.
   d. Immettere i valori appropriati nei campi della finestra di dialogo.
   e. Fare clic sul pulsante **OK** per definire la porta.

      La porta viene visualizzata nel riquadro Connectivity della finestra Node.
2. Definire una stazione di collegamento nella porta:
   a. Assicurarsi di aver selezionato la porta a cui deve essere aggiunta la stazione di collegamento nel riquadro Connectivity della finestra Node.
   b. Selezionare **New link station** dal sottomenu **Connectivity** del menu **Services** (o fare clic sul pulsante **New** nella barra dei pulsanti).
   c. Fare clic sul pulsante **OK**.

      CS/AIX visualizza la finestra di dialogo IP Link Station.
   d. Immettere i valori appropriati nei campi della finestra di dialogo.
   e. Fare clic sul pulsante **OK** per definire la stazione di collegamento.

      La stazione di collegamento viene visualizzata sotto la porta a cui appartiene nel riquadro Connectivity della finestra Node.

Configurazione delle LU di tipo 0–3

Per supportare le applicazioni utente che utilizzano le LU di tipo 0–3, è necessario configurare le LU dipendenti. Prima occorre effettuare la seguente configurazione:

- Configurare il nodo come descritto in "Configurazione del nodo" a pagina 80.
- Configurare un collegamento per supportare il traffico delle LU dipendenti, come descritto in "Configurazione della connettività" a pagina 81.

  Se si dispone di un collegamento in upstream ad un altro nodo che utilizza un gateway SNA o se si utilizza il DLUR non è necessario configurare un collegamento diretto all'host. Per ulteriori informazioni, consultare "Configurazione del gateway SNA" a pagina 94 e "Configurazione DLUR" a pagina 97.

Per supportare le comunicazioni con un sistema host, occorre configurare le LU dipendenti di tipo 0–3. Le informazioni contenute in questa sezione possono essere

utilizzate per definire una LU che supporti LUA, DLUR o la concentrazione PU. È possibile anche definire una gamma di LU al fine di configurare più LU dello stesso tipo in un'unica operazione.

Inoltre, è possibile definire un pool di LU da utilizzare secondo necessità, assegnando una LU a un pool durante la definizione della LU o assegnando le LU precedentemente definite a un pool.

Definizione delle LU di tipo 0–3

Prima di configurare le LU 3270, raccogliere le seguenti informazioni:

- Nome LU (si tratta di un identificativo locale e non deve necessariamente corrispondere alla configurazione dell'host).
- Numero LU (o numeri LU, nel caso di un intervallo di LU).
- Tipo di LU (modello display 3270 o stampante 3270).
- Nome pool (se si aggiunge la LU ad un pool).

Per configurare una LU del tipo 0–3 per una stazione di collegamento precedentemente definita, eseguire quanto segue dalla finestra Node:

1. Selezionare la stazione di collegamento all'host nel riquadro Connectivity della finestra.
2. Fare clic sul pulsante **New**.
3. Nella successiva finestra di dialogo, selezionare il tipo di LU (**New 3270 display LU** o **New 3270 printer LU**).

   Una volta selezionata questa voce e fatto clic su **OK**, CS/AIX visualizza la finestra di dialogo LU Type 0–3.
4. Immettere i valori appropriati nei campi della finestra di dialogo.
5. Fare clic su **OK** per definire la LU.

   La LU viene visualizzata nel riquadro Connectivity della finestra Node, sotto la stazione di collegamento all'host.

Definizione di un pool di LU

Per la LU di tipo 0–3, è possibile definire dei pool di LU al fine di semplificare la configurazione utente e offrire una maggiore flessibilità per la creazione di sessioni host. Ad esempio, è possibile definire più LU in un unico pool di LU e poi configurare più utenti tramite tale pool. Ciò agevola la configurazione delle sessioni degli utenti e consente a ciascuna sessione di utilizzare qualunque LU del pool.

Nota: La sessione utente può essere assegnata a una determinata LU o a un pool di LU.

- Se si assegna la sessione utente a una determinata LU di un pool, se questa è disponibile la sessione la utilizza. In caso contrario, utilizza qualsiasi LU del pool disponibile, come se la sessione fosse stata assegnata al pool di LU invece che a quella determinata LU.
- Se si desidera che l'utente utilizzi solo una determinata LU affinché la sessione dell'utente non possa essere stabilita se la LU è già in uso, assicurarsi che la LU non appartenga a un pool.

È possibile visualizzare i pool di LU del nodo CS/AIX locale tramite la finestra LU Pools. Questa finestra elenca i pool di LU configurati nel sistema locale e consente di selezionare le LU da aggiungere a un pool di LU.

È possibile aggiungere i seguenti tipi di LU a un pool (non mischiare LU di differenti tipi nello stesso pool):

- LU display 3270
- LU illimitata

Per poter aggiungere delle LU a un pool, queste devono essere definite sul nodo locale.

Per configurare un pool di LU, eseguire quanto segue dalla finestra Node:

1. Selezionare **LU Pools** dal menu **Windows**.

   CS/AIX visualizza la finestra LU Pools.
2. Fare clic sul pulsante **New**.

   CS/AIX visualizza la finestra di dialogo LU Pool Configuration.

   La casella a destra elenca le LU non ancora allocate ad alcun pool. Qualunque LU di questo elenco può essere inclusa nel nuovo pool.
3. Selezionare la LU o le LU da aggiungere al pool, quindi fare clic sul pulsante **New** per spostare le LU selezionate nella casella a sinistra.

   Per eliminare una LU dalla casella di sinistra, selezionarla e fare clic sul pulsante **Remove**.
4. Fare clic su **OK** per definire il pool di LU.

   Tutte le LU della casella a sinistra vengono aggiunge al pool di LU.

   Il pool viene visualizzato nella finestra LU Pools.

Configurazione della comunicazione APPC

Le applicazioni APPC e le applicazioni CPI-C necessitano, innanzitutto, della configurazione di APPC. Un'applicazione APPC utilizza le risorse della LU di tipo 6.2 del nodo per comunicare con un'altra applicazione APPC o CPI-C su un host o su un computer peer tramite la modalità specificata.

Prima di poter configurare la comunicazione APPC, è necessario effettuare la seguente configurazione:

1. Configurare il nodo come descritto in "Configurazione del nodo" a pagina 80.
2. Configurare la connettività come descritto in "Configurazione della connettività" a pagina 81.

Le restanti fasi della configurazione dipendono dal tipo di traffico supportato dalla configurazione (dipendente, indipendente o entrambi):

APPC indipendente

L'APPC indipendente utilizza LU indipendenti. Ciascuna sessione LU-LU coinvolge una LU locale e una LU partner.

Per la LU locale, è possibile utilizzare la LU predefinita associata al punto di controllo del nodo o configurare nuove LU locali.

Se il nodo CS/AIX è un nodo finale o un nodo di una rete APPN non è affatto necessario configurare la LU partner, poiché APPN è in grado di localizzare le LU partner dinamicamente. Tuttavia, se la rete in uso non è una rete APPN o se il nodo è un nodo LEN, la LU partner deve essere invece configurata. In tal caso, occorre configurare il nodo remoto in cui risiede la LU partner e definirla sul nodo remoto.

APPC dipendente
Se il nodo remoto è un host che non supporta la LU 6.2 indipendente, effettuare la configurazione per il traffico dipendente. Per l'APPC dipendente, è necessario configurare una LU locale.

Se le applicazioni utilizzano CPI-C, dopo aver configurato l'APPC potrebbe essere necessaria un'ulteriore configurazione di CPI-C (consultare "Configurazione delle comunicazioni CPI" a pagina 93). Per comunicare con un'altra applicazione CPI-C o APPC su un host o su un computer peer, un'applicazione CPI-C utilizza le risorse di modalità e della LU 6.2 del nodo. Le risorse definite per un'applicazione CPI-C sono le stesse definite per un'applicazione APPC. Inoltre, se il TP sul computer CS/AIX è il TP di richiamo, noto anche come TP di origine (il TP che avvia la conversazione), potrebbe essere necessario definire al riguardo una o più voci di informazioni aggiuntive, come descritto in "Configurazione delle comunicazioni CPI" a pagina 93. Ciascuna di queste voci fornisce informazioni su un TP partner, sulla LU e sulle risorse di modalità utilizzate per accedervi, nonché qualsiasi informazione necessaria relativa alla sicurezza.

Questa sezione illustra come configurare una rete APPN semplice (tramite una LU 6.2 indipendente) composta da un nodo di rete, un nodo finale e un nodo LEN, come descritto in "Configurazione di una rete APPN semplice" (questo scenario mostra anche come ottenere informazioni sullo stato delle sessioni CP-CP tra due nodi).

Questa sezione spiega, inoltre, come configurare la comunicazione APPC dipendente, come descritto in "Configurazione dell'APPC dipendente" a pagina 92.

Entrambi questi scenari presumono che le sessioni APPC utilizzino una modalità e una classe di servizio (COS, Class-Of-Service) standard.

Per informazioni sulla configurazione delle informazioni aggiuntive relative all'APPC, quali modalità, sicurezza e TP richiamabili (o di destinazione), consultare *IBM Communications Server for AIX Administration Guide*.

Configurazione di una rete APPN semplice

La rete APPN più semplice che si possa configurare include due nodi: un nodo di rete APPN e un nodo finale APPN. Il nodo di rete gestisce l'instradamento della sessione per il nodo finale.

Configurazione di un nodo di rete

Questo scenario presume che si utilizzino la LU del punto di controllo, una modalità standard e un tipo di collegamento LAN (Token Ring o Ethernet). In questo caso, è possibile configurare il nodo di rete eseguendo semplicemente le seguenti attività di configurazione:

1. Configurare il nodo come descritto in "Configurazione del nodo" a pagina 80. Nel campo *APPN support*, selezionare il valore `Network node`. Annotarsi il nome del punto di controllo.
2. Configurare la connettività come descritto in "Configurazione della connettività" a pagina 81. Configurare il collegamento affinché supporti il traffico indipendente.

Per contattare questo nodo di rete da un nodo finale adiacente, sarà necessario conoscere l'indirizzo MAC e il numero SAP della porta sul nodo di rete. Utilizzare la seguente procedura per ottenere l'indirizzo MAC sul nodo di CS/AIX:

1. Selezionare la porta nella finestra Node.

2. Fare clic sul pulsante **Start** per avviare la porta.
3. Fare clic sul pulsante **Status** per ottenere informazioni sullo stato della porta. La finestra di dialogo Port Status mostra l'indirizzo MAC e il numero SAP.
4. Annotarsi l'indirizzo MAC e il numero SAP per poter immettere questi valori nella finestra di dialogo della configurazione della stazione di collegamento del nodo finale.

Configurazione di un nodo finale

Questo scenario presume che si utilizzino la LU del punto di controllo, una modalità standard e un tipo di collegamento LAN (Token Ring o Ethernet). In questo caso, è possibile configurare il nodo di rete eseguendo semplicemente le seguenti attività di configurazione:

1. Configurare il nodo come descritto in "Configurazione del nodo" a pagina 80. Nel campo *APPN support*, selezionare il valore `End node`.
2. Configurare la connettività come descritto in "Configurazione della connettività" a pagina 81. Configurare il collegamento affinché supporti il traffico indipendente e fornire le seguenti informazioni sulla stazione di collegamento:
   - Immettere il nome del nodo di rete (consultare "Configurazione di un nodo di rete" a pagina 88) come valore del campo *Remote node*.
   - Nel riquadro Contact Information della finestra di dialogo per la configurazione della stazione di collegamento, immettere l'indirizzo MAC e il numero SAP della porta sul nodo di rete.

   In una rete APPN è possibile utilizzare una sola stazione di collegamento con un nodo di rete adiacente per comunicare con qualsiasi nodo remoto della rete, non è dunque necessario configurare una stazione di collegamento distinta per ciascun nodo remoto.

Verifica della connettività tra due nodi

Questo scenario presume che l'utente abbia configurato un nodo di rete come descritto in "Configurazione di un nodo di rete" a pagina 88 e un nodo finale come descritto in "Configurazione di un nodo finale". È possibile effettuare la seguente procedura dal nodo finale:

1. Nella finestra Node, selezionare la stazione di collegamento che si collega con il nodo di rete adiacente.
2. Fare clic sul pulsante **Start** per avviare la stazione di collegamento.

   Se la stazione di collegamento è avviata, le sessioni CP-CP tra i due nodi vengono stabilite automaticamente. Tali sessioni vengono visualizzate nel riquadro Independent Local LU della finestra Node.
3. Per ottenere informazioni sullo stato di una sessione, selezionare la sessione nella finestra Node e fare clic sul pulsante **Status**.

Configurazione di una LU indipendente APPC

Spesso le applicazioni possono utilizzare la LU del punto di controllo del nodo locale definita automaticamente durante la configurazione del nodo. Si tratta della LU predefinita: se l'applicazione non specifica una LU particolare, può utilizzare questa. Se l'applicazione utilizza la LU predefinita, non è necessario definire una LU locale. Consultare la documentazione sulla propria applicazione APPC o contattare il programmatore dell'applicazione.

Per configurare una LU 6.2 indipendente sono necessarie le seguenti informazioni:

- Nome LU locale.
- Alias LU locale (se in un TP supportato da questa LU viene utilizzato un alias).

Per configurare una LU locale indipendente, eseguire quanto segue dalla finestra Node:

1. Selezionare il riquadro Independent Local LU della finestra.
2. Selezionare **New independent local LU** dal sottomenu **APPC** del menu **Services** (o fare clic sul pulsante **New**).

   CS/AIX visualizza la finestra di dialogo Local LU.
3. Immettere i valori appropriati nei campi della finestra di dialogo.
4. Fare clic sul pulsante **OK** per definire la LU locale. La LU indipendente viene visualizzata nel riquadro Independent Local LU della finestra Node.

Configurazione delle LU partner di un nodo LEN

Nelle seguenti situazioni è necessario definire un nodo remoto (e le LU partner sul nodo):

- Se il nodo locale è un nodo LEN, è necessario definire tutti i nodi remoti e qualsiasi LU partner sul nodo remoto con cui comunica tramite APPC. Un nodo LEN non è in grado di localizzare dinamicamente le LU partner: la definizione del nodo remoto glielo consente.
- Se il nodo locale non appartiene a una rete APPN (ad esempio, se sono presenti due nodi finali direttamente connessi senza un server nodo di rete), le LU non possono essere localizzate dinamicamente. In questo caso, occorre configurare ciascuna LU partner.
- Se il nodo remoto è un nodo LEN e il nodo locale è un nodo di rete che funge da server nodo di rete (NNS) del nodo LEN, è necessario definire il nodo LEN (e le rispettive LU partner) come nodo remoto sul server nodo di rete. Questa definizione consente ai nodi del resto della rete APPN di localizzare le LU sul nodo LEN.
- Se il nodo remoto si trova in un'altra rete APPN, è necessario definirlo in quanto non può essere localizzato dinamicamente.

Non definire le LU partner se sia il nodo locale che il nodo remoto appartengono alla stessa rete APPN.

Se si aggiunge una definizione del nodo remoto, viene aggiunta automaticamente anche una LU partner con lo stesso nome del nodo remoto; si tratta della LU del punto di controllo del nodo remoto. Se la propria applicazione utilizza questa LU partner non è necessario aggiungerne un'altra, mentre si potrebbe voler aggiungere un alias per tale LU. Per aggiungere un alias, fare doppio clic sulla LU partner e immettere l'alias nella finestra di dialogo Partner LU Configuration.

Se per fare riferimento alla propria LU partner l'applicazione in uso utilizza un alias LU, si deve aggiungere una definizione dell'alias della LU partner.

Se il nodo locale o il nodo remoto è un nodo LEN, occorre definire la LU partner come voce secondaria del nodo remoto, in quanto un nodo LEN non può partecipare alla localizzazione dinamica delle LU. Se la propria applicazione utilizza la LU del punto di controllo del nodo remoto come LU partner, la LU del punto di controllo è stata definita automaticamente quando è stato definito il nodo remoto.

Il programma di gestione Motif può essere utilizzato per aggiungere un alias della LU partner (consultare "Definizione di un alias della LU partner" a pagina 91), aggiungere una definizione di una LU partner su un determinato nodo remoto (consultare "Definizione di una LU partner su un nodo remoto" a pagina 91) o

definire più LU partner mediante caratteri jolly (consultare "Definizione di più LU partner tramite caratteri jolly" a pagina 92).

Definizione di un nodo remoto: Per poter configurare un nodo remoto, sono necessarie le seguenti informazioni:

- Nome completo della rete SNA del nodo.

Per configurare un nodo remoto, eseguire quanto segue dalla finestra Node:

1. Selezionare il riquadro Remote Systems della finestra.
2. Selezionare **New remote node** dal sottomenu **APPC** del menu **Services** (o fare clic sul pulsante **New** nella barra dei pulsanti, quindi selezionare **Define remote node**).

   CS/AIX visualizza la finestra di dialogo Remote Node Configuration.
3. Immettere i valori appropriati nei campi della finestra di dialogo.
4. Fare clic sul pulsante **OK** per definire il nodo remoto. Nel riquadro Remote Systems della finestra Node viene visualizzato il nodo remoto.

   Se si definisce un sistema remoto, CS/AIX definisce automaticamente la LU del punto di controllo sul nodo remoto come LU partner sul nodo locale.

Definizione di un alias della LU partner: Per definire un alias della LU partner, sono necessarie le seguenti informazioni:

- Nome completo della LU partner (nome della rete SNA e nome LU)
- Alias della LU partner utilizzato da un TP locale

Per aggiungere un alias della LU partner, eseguire quanto segue dalla finestra Node:

1. Selezionare il riquadro Remote Systems della finestra.
2. Selezionare **APPC**, **New partner LUs** e **Partner LU alias** dal menu **Services** (o fare clic sul pulsante **New** nella barra dei pulsanti, quindi selezionare **Define partner LU alias**).

   CS/AIX visualizza la finestra di dialogo Partner LU Alias Configuration.
3. Immettere il nome e l'alias della LU partner nella finestra di dialogo.
4. Fare clic sul pulsante **OK** per definire l'alias della LU partner. Nel riquadro Remote Systems della finestra Node viene visualizzato l'alias della LU partner (come parte della definizione della rete).

Definizione di una LU partner su un nodo remoto: Per definire una LU partner su un determinato nodo remoto, sono necessarie le seguenti informazioni:

- Nome LU partner completo.
- Alias LU partner (se un TP locale utilizza un alias).
- Nome completo del nodo che contiene informazioni sulla directory della LU partner.
- Se la LU partner si trova su una rete TCP/IP, metodo di instradamento preferito (APPN o AnyNet).

Per aggiungere una definizione LU partner per un determinato nodo remoto, eseguire quanto segue dalla finestra Node:

1. Selezionare il nodo remoto.
2. Selezionare **APPC**, **New partner LUs** e **Partner LU on remote node** dal menu **Services** (o fare clic sul pulsante **New** nella barra dei pulsanti, quindi selezionare **Define partner LU on remote node**).

CS/AIX visualizza la finestra di dialogo Partner LU Configuration.

3. Immettere i valori appropriati nei campi della finestra di dialogo.
4. Fare clic sul pulsante **OK** per definire la LU partner. L'alias della LU partner viene visualizzato nel riquadro Remote Systems della finestra Node, sotto il sistema remoto di appartenenza.

Definizione di più LU partner tramite caratteri jolly: È possibile utilizzare i caratteri jolly per configurare l'ubicazione di una serie di LU partner poste sullo stesso nodo remoto e il cui nome inizi con gli stessi caratteri. Se si utilizzano caratteri jolly non occorre configurare ciascuna LU partner individualmente.

Se si definiscono le LU partner tramite caratteri jolly, è necessario fornire le seguenti informazioni:

- Nome LU partner con caratteri jolly. Il nome della LU partner con caratteri jolly è formato da due tipi di stringhe A EBCDIC, ciascuna delle quali è composta da 1 a 8 caratteri, corrispondenti ai nomi LU completi di più LU partner.

  La prima stringa può essere un nome rete SNA completo che corrisponde esattamente al nome della rete delle LU partner o un prefisso composto da caratteri jolly corrispondente all'inizio del nome della rete. Se per il nome della rete si immette un prefisso composto da caratteri jolly, lasciare vuota la seconda stringa.

  Se si fornisce un nome rete SNA completo per la prima stringa, è possibile immettere un valore anche per la seconda (non è possibile immettere la seconda stringa se non si è fornito un nome rete SNA valido per la prima). La seconda stringa è trattata come un prefisso formato da caratteri jolly che deve corrispondere all'inizio della seconda parte dei nomi completi delle LU partner.
- Nome del nodo in cui sono ubicate le LU partner.

Per aggiungere più LU partner, eseguire quanto segue dalla finestra Node:

1. Selezionare il nodo remoto per cui si definiscono le LU partner.
2. Selezionare **APPC**, **New partner LUs** e **Wildcard partner LUs on remote node** dal menu **Services** (o fare clic sul pulsante **New** nella barra dei pulsanti, quindi selezionare **Define wildcard partner LUs on remote node**).

   CS/AIX visualizza la finestra di dialogo Wildcard Partner LU Configuration.
3. Immettere le informazioni appropriate nei campi della finestra di dialogo.
4. Fare clic sul pulsante **OK** per definire le LU partner. Le LU partner vengono visualizzate nel riquadro Remote Systems della finestra Node, sotto il nodo remoto di appartenenza.

Configurazione dell'APPC dipendente

Per configurare una LU 6.2 dipendente sono necessarie le seguenti informazioni:

- Nome LU locale.
- Alias LU locale (se in un TP supportato da questa LU viene utilizzato un alias).
- Nome della stazione di collegamento che fornisce la connessione all'host.
- Numero LU.
- Indicazione sull'eventuale assegnazione della LU al pool predefinito per la LU 6.2 dipendente.

Se si configurano LU 6.2 dipendenti in modo tale che possano essere utilizzate con applicazioni APPC o CPI-C, si potrebbe voler definire che tali LU appartengono al

pool predefinito. Ad un'applicazione che non specifica una determinata LU locale viene attribuita un LU inutilizzata appartenente al pool di LU definite come predefinite.

Per configurare una LU locale dipendente, eseguire quanto segue dalla finestra Node:

1. Selezionare una stazione di collegamento nel riquadro Connectivity della finestra.
2. Selezionare **New dependent local LU** dal sottomenu **APPC** del menu **Services** (o fare clic sul pulsante **New** nella barra dei pulsanti, quindi selezionare **New dependent local LU**).

   CS/AIX visualizza la finestra di dialogo Local LU.
3. Immettere i valori appropriati nei campi della finestra di dialogo.
4. Fare clic sul pulsante **OK** per definire la LU locale. La LU dipendente viene visualizzata nel riquadro Connectivity, sotto la stazione di collegamento di appartenenza.

Configurazione delle comunicazioni CPI

Se si supporta un'applicazione CPI-C che utilizza nomi di destinazione CPI-C simbolici, è necessario definire le informazioni ubicazione CPI-C. Le informazioni ubicazione associano il nome destinazione simbolico a informazioni sul TP partner, sulla LU partner, sulla modalità e sulla sicurezza della conversazione.

Per determinare il nome destinazione simbolico di CPI-C, consultare lo sviluppatore dell'applicazione (o per un'applicazione di terzi, consultare la documentazione del prodotto).

Prima di configurare le informazioni ubicazione CPI-C, sono necessarie le seguenti informazioni:

- Nome destinazione simbolico utilizzato dal TP
- Nome TP partner
- Nome o alias della LU partner
- Nome modalità

Per configurare le informazioni ubicazione CPI-C, eseguire quanto segue dalla finestra Node:

1. Selezionare **CPI-C** dal sottomenu **APPC** del menu **Services**.

   CS/AIX visualizza la finestra CPI-C Destination Names.
2. Fare clic sul pulsante **New**.

   CS/AIX visualizza la finestra di dialogo CPI-C Destination Configuration.
3. Immettere i valori appropriati nei campi della finestra di dialogo.
4. Fare clic sul pulsante **OK** per definire le informazioni ubicazione CPI-C.

Configurazione della LUA

L'API LUA può essere utilizzata per applicazioni che utilizzano la LU di tipo 0–3 per comunicare con un computer host (per informazioni dettagliate sull'API LUA, consultare *IBM Communications Server for AIX o Linux LUA Programmer's Guide*.)

Prima di configurare la LUA, eseguire la seguente configurazione:

1. Configurare il nodo come descritto in "Configurazione del nodo" a pagina 80.

2. Configurare la connettività per il traffico dipendente come descritto in "Configurazione della connettività" a pagina 81 (se si utilizza un gateway SNA in upstream o DLUR, configurare il collegamento al nodo in upstream invece che un collegamento diretto all'host).

Per configurare la LUA, sono necessarie le seguenti informazioni:

- Nome LU o nome del pool di LU.
- Numero LU di ciascuna LU. Il numero LU deve corrispondere al numero LU configurato sull'host.

Per configurare la LUA, definire la LU utilizzando la seguente procedura:

1. Selezionare la stazione di collegamento all'host nel riquadro Connectivity della finestra Node.
2. Fare clic sul pulsante **New**.
3. Nella successiva finestra di dialogo, selezionare **New LU for LUA**.
4. Immettere i valori appropriati nei campi della finestra di dialogo. Specificare il tipo di LU `Unrestricted`.
5. Fare clic sul pulsante **OK**. La LU viene visualizzata nel riquadro Connectivity della finestra Node, sotto la stazione di collegamento all'host.
6. Se si intendono utilizzare tutti i pool di LU, definirli come descritto in "Definizione di un pool di LU" a pagina 86.

Configurazione del gateway SNA

Oltre a fornire l'accesso diretto a un computer host, CS/AIX può fornire le funzionalità gateway SNA. Questa funzione consente ad altri computer di accedere a un computer host tramite un nodo di CS/AIX, invece di richiedere una connessione distinta all'host da ciascun computer.

La funzione del gateway SNA viene mostrata in Figura 8.

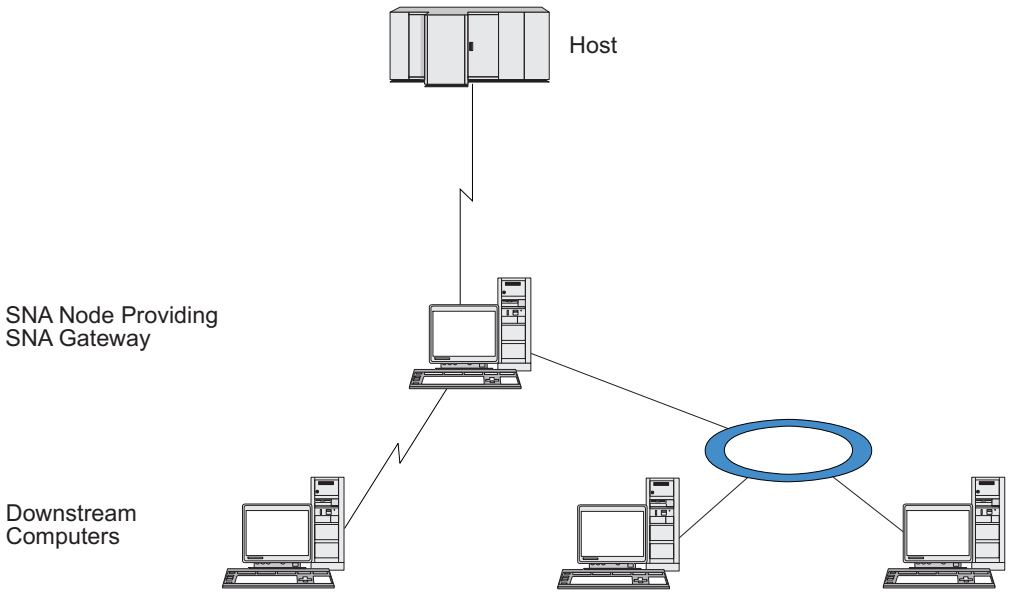

Figura 8. Gateway SNA

Per supportare le LU dipendenti, il computer in downstream deve contenere una PU SNA di tipo 2.0 o 2.1. Ad esempio, il computer in downstream potrebbe essere un altro computer CS/AIX o un PC che esegue Communications Server for Windows.

Quando un nodo CS/AIX locale utilizza la funzione gateway SNA, tutti i dati trasferiti tra l'host e il computer in downstream vengono instradati tramite il nodo locale. Ciò consente al computer in downstream di condividere una connessione host con CS/AIX o con altri computer in downstream, invece di richiedere un collegamento diretto. Ad esempio, è possibile impostare più computer in downstream connessi a CS/AIX su una rete Token Ring locale, affinché possano tutti accedere alla stessa linea dedicata a lunga distanza da CS/AIX all'host.

L'utilizzo del gateway SNA semplifica anche la configurazione dell'host, poiché non è necessario definire i computer in downstream e i collegamenti di comunicazione a tali computer. La configurazione dell'host deve includere solo il computer CS/AIX e il suo collegamento di comunicazione all'host; le LU nei computer in downstream vengono configurate come parte delle risorse del computer CS/AIX. Il computer host non rileva che il gateway SNA è in uso.

Prima di configurare il gateway SNA, è necessario eseguire le seguenti attività di configurazione:

- Definire il nodo locale come descritto in "Configurazione del nodo" a pagina 80.
- Configurare una porta e una stazione di collegamento per il traffico dipendente tra il nodo locale e l'host, come descritto in "Configurazione della connettività" a pagina 81. Configurare anche le porte e le stazioni di collegamento per il traffico dipendente tra il nodo locale e i nodi in downstream. Se occorre supportare le LU in downstream non definite in precedenza, è possibile definire una maschera sulla porta per supportare le PU implicite e le LU in downstream (consultare "Supporto di LU in downstream implicite").
- Definire le LU sul nodo locale utilizzate per la comunicazione con l'host (LU in upstream). Definire le LU in upstream come LU di tipo 0–3 con un tipo LU `Unrestricted` (`unknown`) (le LU sui nodi in downstream possono appartenere a qualsiasi tipo di LU).
- Se si intendono utilizzare tutti i pool di LU, definirli come descritto in "Definizione di un pool di LU" a pagina 86.

Supporto di LU in downstream implicite

Per supportare le LU in downstream non predefinite per CS/AIX, è possibile definire una maschera sulla porta per le PU e le LU in downstream implicite (per informazioni sulla configurazione di base della porta, consultare "Configurazione della connettività" a pagina 81). Queste maschere forniscono supporto per le LU in downstream senza che sia necessario configurare la LU del nodo locale affinché supporti qualsiasi LU su un nodo in downstream.

Per poter configurare una LU in downstream per il gateway SNA, sono necessarie le seguenti informazioni:

- Intervallo di numeri LU a supporto delle LU in downstream.
- Nome LU dell'host.

Per definire una maschera per le LU in downstream implicite, attenersi alla seguente procedura:

1. Se la porta è già stata configurata, fare doppio clic sulla definizione della porta nel riquadro Connectivity della finestra Node. CS/AIX visualizza la finestra di dialogo Port Configuration.

   Se la porta non è ancora stata configurata, farlo ora eseguendo la seguente procedura:

   a. Selezionare il riquadro Connectivity della finestra Node.
   b. Fare clic sul pulsante **New**.
   c. Nella successiva finestra di dialogo, scegliere di definire una porta e selezionare il tipo di protocollo di collegamento.

      CS/AIX visualizza la finestra di dialogo Port Configuration.
   d. Immettere i parametri di base della porta, come descritto in "Configurazione della connettività" a pagina 81.
2. Fare clic sul pulsante **Advanced** in fondo alla finestra di dialogo.

   CS/AIX visualizza la finestra di dialogo Port Parameters. Il riquadro inferiore mostra le impostazioni che influiscono sulle maschere della LU in downstream.
3. Selezionare l'opzione *Configure downstream LUs for implicit PU access*.
4. Fare clic su **OK**.

   CS/AIX visualizza la finestra di dialogo Downstream LU Template Configuration.
5. Immettere i valori appropriati nei campi della finestra di dialogo.
6. Fare clic su **OK** per definire la maschera della LU in downstream implicita.

Definizione delle LU in downstream

Per poter configurare una LU in downstream per il gateway SNA, sono necessarie le seguenti informazioni:

- Nome LU di ciascuna LU in downstream (si tratta di un identificativo locale e non deve necessariamente corrispondere alla configurazione del sistema in downstream).
- Numero LU di ciascuna LU in downstream.
- Stazione di collegamento al nodo in downstream.
- Nome della LU in upstream (per la LU dell'host).

Per poter configurare una LU in downstream per il gateway SNA, attenersi alla seguente procedura:

1. Selezionare la stazione di collegamento al nodo in downstream nel riquadro Connectivity della finestra Node.
2. Fare clic sul pulsante **New**.
3. Selezionare **New downstream LU** e fare clic su **OK**.

   CS/AIX visualizza la finestra di dialogo Downstream LU.
4. Immettere i valori appropriati nei campi della finestra di dialogo.
5. Fare clic su **OK** per definire la LU in downstream.

   La definizione della LU viene visualizzata nel riquadro Connectivity della finestra Node, sotto la stazione di collegamento al nodo in downstream.

Configurazione DLUR

Oltre a fornire l'accesso diretto a un computer host, CS/AIX può fornire le funzionalità DLUR (Dependent LU Requester). Questa funzione consente alle sessioni delle LU dipendenti di estendersi su più nodi in una rete APPN, invece di richiedere una connessione diretta all'host.

Solitamente, una sessione di una LU dipendente necessita di un collegamento di comunicazione diretto con il computer host. Se i nodi interconnessi in una rete APPN (incluso un nodo host) sono numerosi, alcuni di essi potrebbero non avere una connessione diretta all'host, ma solo una connessione indiretta tramite un altro nodo. Non è possibile stabilire sessioni LU dipendenti dalle LU all'host in questi nodi indirettamente connessi.

Il DLUR (Dependent LU Requester) è una funzione APPN progettata per superare questa limitazione.

Il DLUR su un nodo APPN (ad esempio il nodo CS/AIX) opera congiuntamente al server LU dipendente (DLUS, Dependent LU Server) nell'host, per instradare le sessioni dalle LU dipendenti sui nodi DLUR all'host DLUS tramite la rete APPN. Il percorso verso l'host può estendersi su più nodi e sfruttare la gestione della rete, la localizzazione dinamica delle risorse e le funzionalità di calcolo del percorso di APPN. Il DLUR deve essere disponibile sul nodo in cui sono ubicate le LU e il DLUS deve essere disponibile sul nodo dell'host, ma il DLUR non è necessario su nessun nodo intermedio del percorso della sessione.

Se il nodo DLUR di CS/AIX è un nodo di rete o un BrNN (Branch Network Node), può fornire anche funzionalità DLUR pass-through per le LU dipendenti sui computer in downstream connessi al nodo CS/AIX. Queste LU possono usare il DLUR sul nodo CS/AIX per accedere all'host tramite la rete, così come accade alle LU interne al nodo. I computer in downstream non eseguono il DLUR e non hanno nemmeno bisogno di rilevare che il DLUR è in uso.

Figura 9 a pagina 98 mostra un server CS/AIX configurato come nodo della rete APPN che implementa il DLUR pass-through per supportare le sessioni tra le LU dell'host (il nodo in upstream) e le LU dei nodi della rete APPN (nodi in downstream).

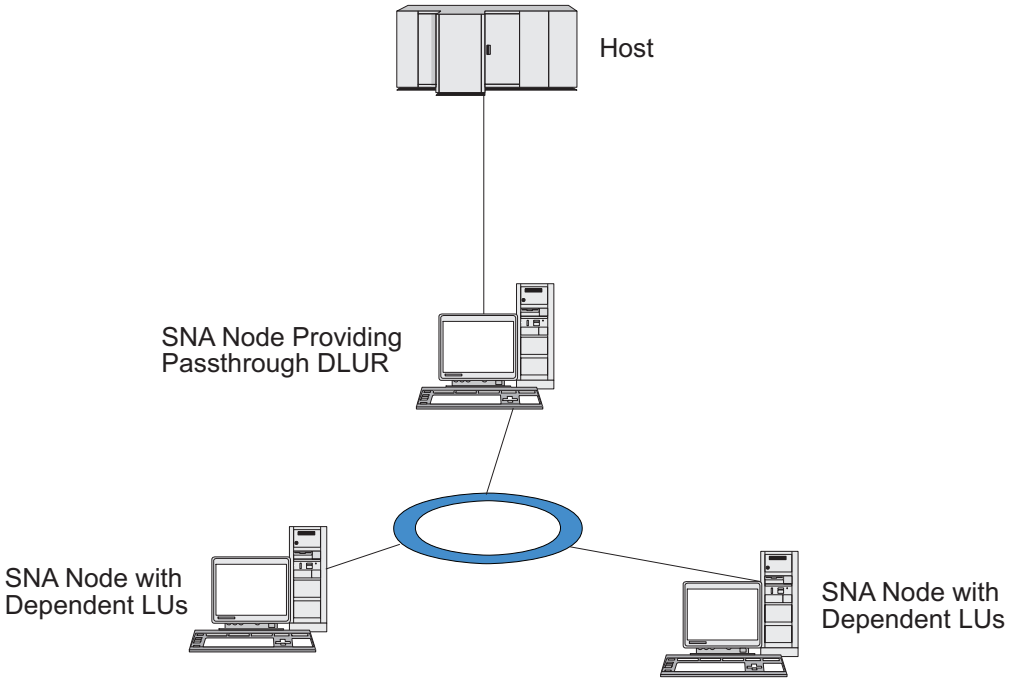

Figura 9. Nodo CS/AIX che fornisce il DLUR

Nota:

1. Il DLUR non può essere configurato su un nodo LEN.
2. Il DLUR pass-through può essere configurato solo su un nodo di rete o un nodo BrNN.
3. Se si utilizza Branch Extender, non è possibile configurare il DLUR su un nodo finale della filiale (con un nodo Branch Network come rispettivo server nodo di rete). Tuttavia, è possibile supportare le applicazioni della LU dipendente da questo nodo configurando il DLUR pass-through nel nodo Branch Network (affinché il nodo finale nella filiale non esegua il DLUR, ma utilizzi il DLUR pass-through sul nodo Branch Network).

Le attività da eseguire per configurare il DLUR variano a seconda che le LU dipendenti si trovino sul nodo locale o sui nodi in downstream.

Configurazione del supporto DLUR nel nodo locale

Per questa attività sono necessarie le seguenti informazioni:

- ID PU per la PU sul nodo locale.
- Nome PU (si tratta di un identificativo locale e non deve necessariamente corrispondere alla configurazione dell'host).
- Nome del DLUS sull'host (e il nome del DLUS di backup, se esistente).
- Nome LU, numero LU e tipo LU per ciascuna LU in downstream. Il numero LU deve corrispondere al numero configurato nell'host.

Per configurare il supporto DLUR sul nodo locale, è necessario eseguire le seguenti attività di configurazione:

1. Definire il nodo locale come descritto in "Configurazione del nodo" a pagina 80. Se si fornisce un supporto DLUR pass-through per i nodi in downstream, definire il nodo come nodo della rete APPN o nodo Branch Network.

2. Configurare la connettività alla rete APPN. La connettività APPN richiede almeno una porta e una stazione di collegamento per il traffico indipendente tra il nodo locale e il nodo di rete APPN adiacente, come descritto in "Configurazione della connettività" a pagina 81.
3. Definire una PU DLUR sul nodo locale (la PU DLUR supporta la connettività all'host).

   Per configurare la PU DLUR, eseguire quanto segue dalla finestra Node:

   a. Selezionare il menu **Services**, quindi il sottomenu **Connectivity** e **New DLUR PU** (o fare clic sul pulsante **New** nella barra dei pulsanti, quindi selezionare **DLUR PU**).

      Se si fa clic sul pulsante **OK**, CS/AIX visualizza la finestra di dialogo DLUR PU Configuration.

   b. Immettere i valori appropriati nei campi della finestra di dialogo.
   c. Fare clic sul pulsante **OK** per definire la PU DLUR.

      La PU DLUR viene visualizzata nel riquadro Connectivity sotto la voce DLUR.
4. Per configurare il DLUR affinché supporti le LU sul nodo locale, è necessario aggiungere le LU al nodo locale. Le LU devono essere configurate per supportare la LUA, come descritto in "Configurazione della LUA" a pagina 93. A seconda dei requisiti delle applicazioni utente supportate da queste LU, potrebbe essere necessaria anche un'ulteriore configurazione.

Configurazione del supporto DLUR pass-through per i nodi in downstream

Per questa attività sono necessarie le seguenti informazioni:

- Nome PU in downstream per ciascun nodo in downstream o per ciascun PU sul nodo in downstream (si tratta di un identificativo locale e non deve necessariamente corrispondere alla configurazione dell'host).
- Nome del DLUS sull'host.

Per configurare il supporto DLUR pass-through per i nodi in downstream, è necessario eseguire le seguenti attività di configurazione:

1. Definire il nodo locale come nodo della rete APPN (consultare "Configurazione del nodo" a pagina 80).
2. Configurare la connettività ai nodi in downstream. Configurare le porte e le stazioni di collegamento per il traffico dipendente tra il nodo locale e ciascun nodo in downstream, come descritto in "Configurazione della connettività" a pagina 81 (non è necessario definire una PU DLUR per supportare il DLUR pass-through per i nodi in downstream).
3. Un nodo in downstream può supportare più PU. In tal caso, ciascuna PU in downstream viene associata a un differente collegamento ed è quindi necessario configurare più collegamenti tra il nodo DLUR di CS/AIX e il nodo in downstream, nonché conoscere il nome della PU in downstream per ciascun collegamento.

Configurazione del server TN

I programmi di emulazione 3270 che comunicano tramite TCP/IP (piuttosto che su una rete SNA) vengono denominati programmi TN3270 (programmi di emulazione Telnet 3270).

I programmi TN3270 possono includere anche il supporto per TN3270E (le estensioni standard di Telnet 3270). TN3270E è un protocollo aperto che supporta la simulazione di dispositivi 3270 (inclusi sia i terminali che le stampanti) che utilizzano Telnet. Consente a un client Telnet di selezionare un determinato dispositivo (specificando il nome LU) e fornisce maggiore supporto per differenti funzioni, incluse le chiavi ATTN e SYSREQ e la gestione delle risposte SNA.

Nota: Questa guida utilizza il termine TN3270 per informazioni ugualmente applicabili ai protocolli TN3270, TN3287 e TN3270E.

Il server TN di CS/AIX fornisce l'accesso ai computer host 3270 agli utenti TN3270 che operano su altri computer. Il server TN consente agli utenti TN3270 di condividere una connessione host con CS/AIX o con altri utenti TN3270, invece di richiedere un collegamento diretto. Il server TN consente inoltre agli utenti TN3270 di accedere agli host che non eseguono TCP/IP.

Nella Figura 10 viene mostrato un nodo CS/AIX che fornisce supporto al server TN per i client TN3270. I client e il nodo del server TN comunicano tramite la rete TCP/IP.

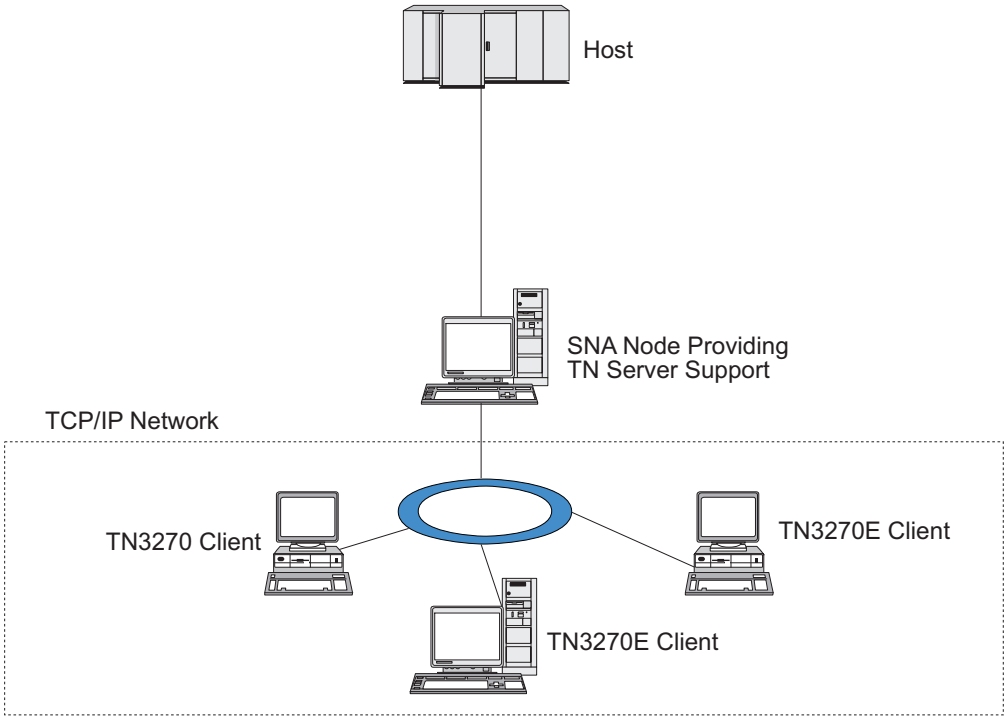

Figura 10. Nodo CS/AIX configurato per il server TN

La funzione del server TN di CS/AIX fornisce un collegamento tra un utente TN3270 e la LU 3270 di CS/AIX. Tutti i dati provenienti dall'utente TN3270 vengono instradati alla LU. Ciò significa che la configurazione dell'host e dell'utente TN3270 è la stessa che si presenterebbe se fossero direttamente connessi e non necessita del rilevamento dell'instradamento dei dati tramite il server TN.

Il server TN di CS/AIX supporta tutti i programmi di emulazione dei client TN3270 che implementano correttamente i protocolli definiti dalla IETF nelle RFC 1123, 1576, 1646, 1647 e 2355.

Quando un programma TN3270 comunica con un server TN, CS/AIX identifica il programma tramite l'indirizzo TCP/IP del computer in cui è in esecuzione il programma TN3270. CS/AIX non è in grado di distinguere tra due differenti programmi TN3270 utilizzati da differenti utenti sullo stesso computer. Nei manuali di CS/AIX il termine utente del server TN fa riferimento al computer in cui è in esecuzione il programma TN3270 e non a un singolo utente di quel programma.

Come mostrato nella Figura 11, l'host e l'utente del server TN visualizzano la configurazione di tale server in maniera differente.

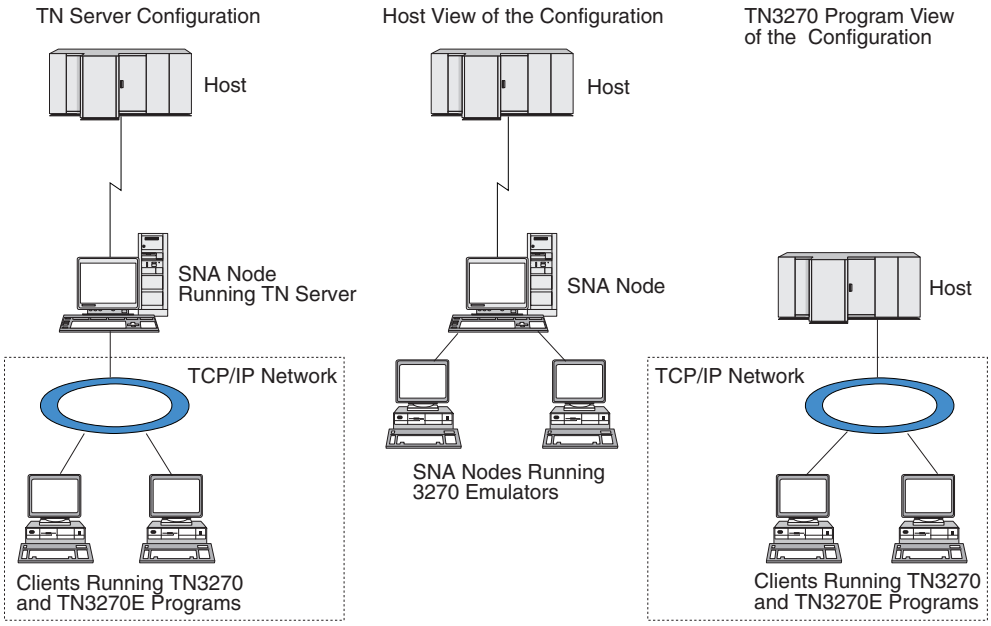

Figura 11. server TN

Ciascun utente del server TN connesso a CS/AIX tramite la funzione Server TN3270 viene solitamente configurato per accedere a un'unica LU 3270 ed è dunque limitato a una sola sessione host alla volta. Tuttavia, è possibile anche configurare un utente del server TN in modo tale che possa accedere a un pool di LU 3270, invece di avere un'unica LU 3270 dedicata per ciascun utente. Ciò consente agli utenti di accedere a tante sessioni quante sono le LU disponibili nel pool.

Prima di poter configurare l'accesso al server TN, è necessario effettuare le seguenti attività di configurazione:

- Definire il nodo locale come descritto in "Configurazione del nodo" a pagina 80.
- Configurare una porta e una stazione di collegamento per il traffico dipendente tra il nodo locale e l'host, come descritto in "Configurazione della connettività" a pagina 81.

Per configurare l'accesso al server TN, è necessario eseguire le seguenti attività di configurazione:

- Definire le LU 3270 sul nodo locale utilizzate per la comunicazione con l'host. Per aggiungere le LU, consultare "Definizione delle LU 3270" a pagina 102.
- Se si intendono utilizzare tutti i pool di LU, definirli come descritto in "Definizione di un pool di LU" a pagina 102.

Definizione delle LU 3270

Prima di configurare le LU 3270, raccogliere le seguenti informazioni:

- Nome LU (si tratta di un identificativo locale e non deve necessariamente corrispondere alla configurazione dell'host).
- Numero LU (o numeri LU, nel caso di un intervallo di LU).
- Tipo di LU (modello display 3270 o stampante 3270).
- Nome pool (se si aggiunge la LU ad un pool).

Per configurare una LU del tipo 0–3 per una stazione di collegamento precedentemente definita, eseguire quanto segue dalla finestra Node:

1. Selezionare la stazione di collegamento all'host nel riquadro Connectivity della finestra.
2. Fare clic sul pulsante **New**.
3. Nella successiva finestra di dialogo, selezionare il tipo di LU (**New 3270 display LU** o **New 3270 printer LU**).

   Una volta selezionata questa voce e fatto clic su **OK**, CS/AIX visualizza la finestra di dialogo LU Type 0–3.
4. Immettere i valori appropriati nei campi della finestra di dialogo.
5. Fare clic su **OK** per definire la LU.

   La LU viene visualizzata nel riquadro Connectivity della finestra Node, sotto la stazione di collegamento all'host.

Definizione di un pool di LU

Per le LU 3270, è possibile definire dei pool di LU al fine di semplificare la configurazione utente e offrire una maggiore flessibilità per la creazione di sessioni host. Ad esempio, è possibile definire più LU 3270 in un unico pool di LU e poi configurare più client TN3270 tramite tale pool. Ciò agevola la configurazione delle sessioni 3270 e consente a ciascun client di utilizzare qualunque LU del pool.

Nota: Il client TN3270 può essere assegnato a una determinata LU o a un pool di LU.

- Se si assegna il client a una determinata LU di un pool, se questa è disponibile il client la utilizza. In caso contrario, utilizza qualsiasi LU del pool disponibile, come se il client fosse stato assegnato al pool di LU invece che a quella determinata LU.
- Se si desidera che il client utilizzi solo una determinata LU affinché la sessione del client non possa essere stabilita se la LU è già in uso, assicurarsi che la LU non appartenga a un pool.

È possibile visualizzare i pool di LU del nodo CS/AIX locale tramite la finestra LU Pools. Questa finestra elenca i pool di LU configurati nel sistema locale e consente di selezionare le LU da aggiungere a un pool di LU.

È possibile aggiungere i seguenti tipi di LU a un pool affinché possano essere utilizzati da 3270 (non mischiare LU di differenti tipi nello stesso pool):

- LU display 3270
- LU illimitata

Per poter aggiungere delle LU a un pool, queste devono essere definite sul nodo locale.

Per configurare un pool di LU, eseguire quanto segue dalla finestra Node:

1. Selezionare **LU Pools** dal menu **Windows**.

   CS/AIX visualizza la finestra LU Pools.
2. Fare clic sul pulsante **New**.

   CS/AIX visualizza la finestra di dialogo LU Pool Configuration.

   La casella a destra elenca le LU non ancora allocate ad alcun pool. Qualunque LU di questo elenco può essere inclusa nel nuovo pool.
3. Selezionare la LU o le LU da aggiungere al pool, quindi fare clic sul pulsante **New** per spostare le LU selezionate nella casella a sinistra.

   Per eliminare una LU dalla casella di sinistra, selezionarla e fare clic sul pulsante **Remove**.
4. Fare clic su **OK** per definire il pool di LU.

   Tutte le LU della casella a sinistra vengono aggiunge al pool di LU.

   Il pool viene visualizzato nella finestra LU Pools.

Configurazione del server TN3270

Per poter configurare il server TN3270, sono necessarie le seguenti informazioni:

- Se il server supporta solo TN3270 o anche TN3270E (che include il supporto TN3270).
- Se un client TN3270E può richiedere una LU specifica.
- Nomi LU (o nomi dei pool di LU) di display e stampante per ciascun client (i nomi delle LU stampanti sono necessari solo se si supporta TN3270E).
- Se sono permessi solo alcuni client o se si vogliono restringere alcuni client a determinate LU, sono necessari l'indirizzo o il nome TCP/IP del client.
- Numero della porta TCP/IP sul nodo del server TN.
- Se sono richieste la crittografia di dati SSL, l'autenticazione del client e l'autenticazione del server (questa opzione è disponibile solo se è stato installato il software aggiuntivo richiesto per supportarla).
- Se il server TN3270 è in funzione in una rete SLP.

Per associare una LU display a una LU stampante, occorrono anche i nomi di tali LU. Un record di associazione al server TN definisce un'associazione tra una LU stampante e una LU display, affinché il protocollo TN3270E possa connetterle. Se non si supporta TN3270E o delle LU stampanti non è necessario definire alcun record di associazione.

Il record di valori predefiniti del server TN definisce i parametri utilizzati in tutte le sessioni client TN3270. È possibile definire un unico record di valori predefiniti per ciascun server.

Per configurare il server TN3270, eseguire quanto segue dalla finestra Node:

1. Definire un record degli accessi al server TN:
   a. Selezionare **TN Server** dal menu **Services**.

      CS/AIX visualizza la finestra TN Server che elenca tutti i record degli accessi al server TN configurati nel riquadro superiore e i record di associazione al server TN in quello inferiore.
   b. Selezionare il riquadro contenente i record degli accessi al server TN3270 e fare clic sul pulsante **New**.

      CS/AIX visualizza la finestra di dialogo TN Server Access.
   c. Immettere i valori appropriati nei campi della finestra di dialogo.

d. Fare clic su **OK** per definire il record degli accessi al server TN. Il record viene visualizzato nella finestra TN Server.

2. Definire un record di associazione al server TN:
   a. Selezionare il riquadro contenente i record di associazione nella finestra TN Server e fare clic sul pulsante **New**.

      CS/AIX visualizza la finestra di dialogo TN Server Association Record.
   b. Immettere i valori appropriati nei campi della finestra di dialogo.
   c. Fare clic su **OK** per definire il record di associazione al server TN. Il record viene visualizzato nella finestra TN Server.
3. Per forzare le risposte delle stampanti, specificare un metodo keep-alive per tutte le sessioni TN3270, specificare come accedere al server LDAP esterno in cui risiede l'elenco di revoche utilizzato per verificare l'autorizzazione dei client TN3270 o utilizzare SLP (Service Location Protocol) TN3270, utilizzare la finestra di dialogo TN Server Advanced Parameters.

Per ulteriori informazioni sulla configurazione del supporto SSL per il server TN, consultare le pagine Web di IBM Communications Server Support all'indirizzo http://www.ibm.com/software/network/commserver/support/.

Configurazione del programma di reindirizzamento TN

Il programma di reindirizzamento TN di CS/AIX offre un accesso host TCP/IP pass-through ai client TN3270, TN3270E, TN5250 e VT collettivamente denominati client Telnet. L'utente Telnet comunica con CS/AIX su una connessione TCP/IP; CS/AIX quindi comunica con l'host su un'altra connessione TCP/IP. Ciò consente l'utilizzo del controllo di sicurezza SSL (Secure Sockets Layer) laddove necessario e non su tutta la connessione utente-host. Ad esempio:

- Se i client si connettono a CS/AIX tramite una LAN TCP/IP in cui il controllo non è richiesto e a un host remoto che invece richiede SSL, è possibile utilizzare SSL sulla connessione TCP/IP tra CS/AIX e l'host. Ciò significa che viene effettuato un controllo di sicurezza unico per tutti i client e che i singoli client non devono fornire informazioni sulla sicurezza.
- Se CS/AIX e l'host sono installati nella stessa ubicazione, mentre i client accedono da siti esterni, è possibile utilizzare SSL sulle connessioni tra client e CS/AIX senza dover installare il software SSL sull'host.

Configurazione del programma di reindirizzamento TN

Prima di poter configurare l'accesso al programma di reindirizzamento TN, è necessario definire il nodo locale come descritto in "Configurazione del nodo" a pagina 80. Sono necessarie anche le seguenti informazioni:

- Se sono permessi solo alcuni client, sono necessari l'indirizzo e il nome TCP/IP del client.
- Il numero della porta TCP/IP utilizzata dal client per connettersi al nodo del programma di reindirizzamento TN.
- L'indirizzo e il nome TCP/IP dell'host.
- Il numero di porta TCP/IP utilizzata dal programma di reindirizzamento TN per connettersi all'host.
- Se sono richieste la crittografia di dati SSL, l'autenticazione del client e l'autenticazione del server tra il client e il nodo del programma di reindirizzamento TN (questa opzione è disponibile solo se è stato installato il software aggiuntivo richiesto per supportarla).

- Se è richiesta la crittografia di dati SSL tra il nodo del programma di reindirizzamento TN e l'host.

Il record di valori predefiniti del programma di reindirizzamento TN definisce i parametri utilizzati in tutte le sessioni client del programma di reindirizzamento TN. È possibile definire un unico record di valori predefiniti per ciascun numero di porta TCP/IP del client.

Per configurare il programma di reindirizzamento TN, eseguire quanto segue dalla finestra Node per definire un record degli accessi al programma di reindirizzamento TN:

1. Selezionare **TN Server** dal menu **Services**.

   CS/AIX visualizza la finestra TN Server che elenca tutti i record degli accessi al server TN3270 configurati, i record di associazione al server TN3270 e i record degli accessi al programma di reindirizzamento TN.
2. Selezionare il riquadro contenente i record degli accessi al programma di reindirizzamento TN e fare clic sul pulsante **New**.

   CS/AIX visualizza la finestra di dialogo TN Redirector Access.
3. Immettere i valori appropriati nei campi della finestra di dialogo.
4. Fare clic su **OK** per definire il record degli accessi al programma di reindirizzamento TN. Il record viene visualizzato nel riquadro TN Redirector della finestra TN Server.

Nota: Per poter utilizzare il programma di reindirizzamento TN, il nodo SNA deve essere attivo anche se il programma non utilizza nessuna delle risorse SNA del nodo.

Configurazione di AnyNet

CS/AIX include la funzione AnyNet APPC over TCP/IP che supporta la conversione dei protocolli e la comunicazione tra applicazioni tramite una rete non nativa. La funzione del nodo di accesso AnyNet APPC over TCP/IP consente alle applicazioni (APPC) LU 6.2 di comunicare tramite una rete TCP/IP e la funzione gateway APPC over TCP/IP consente alle applicazioni APPC di comunicare tramite una rete che è in parte TCP/IP e in parte SNA. AnyNet APPC over TCP/IP funziona solo sulle reti TCP/IP che supportano IPv4. Per ulteriori informazioni su APPC over TCP/IP, consultare *IBM Communications Server for AIX AnyNet Guide to APPC over TCP/IP*.

Nota: La funzione AnyNet APPC over TCP/IP non supporta l'indirizzamento IPv6 ed è disponibile solo su sistemi a 32 bit (e non su sistemi a 64 bit). Nei rilasci futuri non sarà più supportata.

La Figura 12 a pagina 106 mostra un nodo di accesso APPC over TCP/IP.

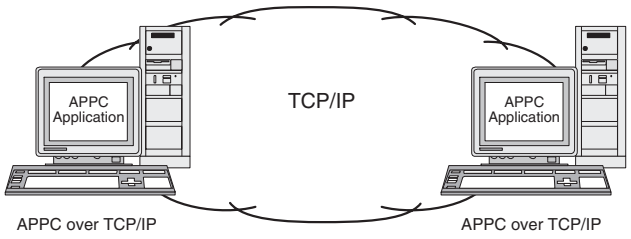

Figura 12. Nodo di accesso AnyNet APPC over TCP/IP

La Figura 13 mostra un gateway APPC over TCP/IP.

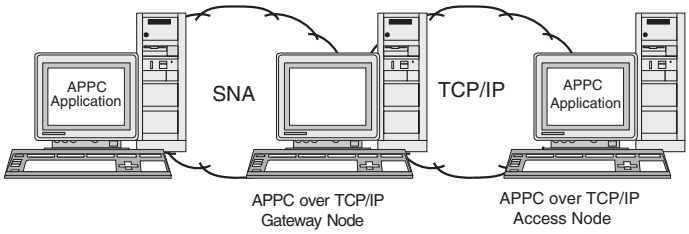

Figura 13. Gateway AnyNet APPC over TCP/IP

Configurazione di APPC over TCP/IP

Prima di poter configurare APPC over TCP/IP, è necessario effettuare la seguente configurazione:

1. Configurare il nodo come descritto in "Configurazione del nodo" a pagina 80.

   Se si configura un nodo di accesso APPC over TCP/IP, il nodo può essere un nodo di rete APPN, un nodo finale o un nodo LEN. Se si configura un gateway APPC over TCP/IP, il nodo locale deve essere un nodo di rete.
2. Se si configura un gateway APPC over TCP/IP, configurare la connettività alla rete SNA come descritto in "Configurazione della connettività" a pagina 81 (fase non necessaria per i nodi di accesso APPC over TCP/IP).

Prima di configurare APPC over TCP/IP, raccogliere le seguenti informazioni:

- Se il sistema locale funge da gateway o da nodo di accesso APPC over TCP/IP. Se il sistema locale è connesso sia a una rete SNA che a una rete TCP/IP, può essere configurato come gateway per consentire la comunicazione tra i nodi delle due reti.
- Nome dominio della rete TCP/IP. Un nome LU con formato *NOMERETE.NOMELU* viene convertito in un indirizzo TCP/IP con formato *NOMELU.RETE.DOMINIO*. Il nome dominio viene configurato nel file **/etc/hosts** o in una voce DNS sul sistema locale.
- La preferenza di instradamento predefinita utilizzata per cercare le LU (solo rete SNA, solo rete TCP/IP o entrambe).
- Se la preferenza di instradamento predefinita non include una ricerca sulla rete TCP/IP, è necessario un elenco delle LU partner da localizzare tramite la rete TCP/IP. Le LU partner ubicate nella rete TCP/IP possono essere nodi di accesso in una rete TCP/IP o LU in una rete SNA connessa alla rete TCP/IP tramite un gateway APPC over TCP/IP.
- Gli indirizzi IP di ciascuna LU da localizzare tramite la rete TCP/IP. Queste informazioni vengono configurate nel file **/etc/hosts** o nel server DNS.

Per configurare APPC over TCP/IP, attenersi alla seguente procedura:

1. Configurare i valori predefiniti di APPC over TCP/IP:
   a. Selezionare l'opzione **AnyNet** dal menu **Services** della finestra Node e l'opzione **AnyNet** nel sottomenu **AnyNet**.

      CS/AIX visualizza la finestra AnyNet.
   b. Selezionare l'opzione **APPC over TCP/IP parameters** dal menu **Selection**

      CS/AIX visualizza la finestra di dialogo AnyNet APPC over TCP/IP Parameters.
   c. Immettere i valori appropriati nei campi della finestra di dialogo.
   d. Fare clic sul pulsante **OK**. La definizione dei valori predefiniti di APPC over TCP/IP viene visualizzata nel riquadro APPC over TCP/IP Sessions della finestra AnyNet.
2. Se non è stata definita una preferenza di instradamento predefinita che include la rete TCP/IP, occorre configurare ciascuna LU partner localizzata tramite la rete TCP/IP:
   a. Selezionare il riquadro Remote Systems della finestra Node e fare clic sul pulsante **New**.
   b. Nella successiva finestra di dialogo, selezionare **Partner LU on remote node** e fare clic sul pulsante **OK**.
   c. Immettere il nome completo della LU partner e selezionare un'opzione di instradamento AnyNet che comprenda la rete TCP/IP.
   d. Fare clic sul pulsante **OK**. La definizione della LU partner viene visualizzata nel riquadro Remote Systems della finestra Node.
3. Configurare gli indirizzi TCP/IP delle LU partner. È possibile aggiungere al file **/etc/hosts** sul sistema locale o al server DNS della rete TCP/IP un'immissione avente il seguente formato:

   dotted_decimal_address NOMELU.NOMERETE.NOMEDOMINIO

   Per una LU partner ubicata in un nodo d'accesso APPC over TCP/IP della rete TCP/IP, utilizzare l'indirizzo IP del nodo di accesso. Per una LU partner ubicata in una rete SNA e connessa alla rete TCP/IP tramite un gateway APPC over TCP/IP, utilizzare l'indirizzo IP del gateway APPC over TCP/IP.

Disabilitazione di CS/AIX

La disabilitazione del software di CS/AIX comporta automaticamente l'arresto del nodo CS/AIX e dei componenti di connettività ad esso associati. Inoltre, se si disabilita CS/AIX qualsiasi altro processo (quale il programma di emulazione 3270) smette di utilizzare le risorse di CS/AIX sul server.

In generale, si devono arrestare i singoli servizi non appena gli utenti hanno finito di utilizzarli e si deve disabilitare il sistema solo quando non sono presenti attività di CS/AIX.

Se è necessario disabilitare CS/AIX mentre gli utenti sono attivi, avvisarli del prossimo arresto di CS/AIX e dar loro il tempo di terminare le proprie attività prima di disabilitare il software.

Se un programma di emulazione 3270 utilizza le LU sul nodo nel momento in cui si disabilita il software di CS/AIX, tutte le sessioni di emulazione 3270 che utilizzano queste LU vengono arrestate. Il programma continua ad essere eseguito, ma l'utente non può utilizzare le sessioni finché il software non viene riabilitato. Le

applicazioni che utilizzano le API APPC, CSV, LUA, NOF o MS vengono avvisate tramite un codice di ritorno `COMM_SUBSYSTEM_ABENDED` e le applicazioni CPI-C tramite un codice di ritorno `CM_PRODUCT_SPECIFIC_ERROR`.

Per disabilitare il software di CS/AIX, immettere il seguente comando nel prompt dei comandi di AIX:

sna stop

Se CS/AIX viene disabilitato correttamente, **sna stop** restituisce il codice di uscita `0`. Qualsiasi altro codice di uscita indica che si è verificato un errore e che il software di CS/AIX non è stato disabilitato. Per ulteriori informazioni sui valori dei codici di uscita, consultare *IBM Communications Server for AIX Diagnostics Guide* .

Capitolo 9. Risorse informative su CS/AIX e SNA

Questo capitolo descrive le risorse della libreria SNA che offrono informazioni sulla tecnologia SNA e sui numerosi servizi e prodotti di rete offerti da IBM. Descrive, inoltre, le informazioni disponibili nei forum in rete.

Libreria SNA

La libreria SNA include opuscoli pubblicitari, libri, manuali utente e supporti didattici che offrono informazioni generali o approfondite sui seguenti argomenti:

- Teoria SNA
- Prodotti SNA
- Implementazione dei prodotti
- Configurazione di sistemi e reti
- Applicazioni SNA e API
- Pianificazione generale, prestazioni e ottimizzazione
- Diagnosi dei problemi
- Gestione delle reti
- Sicurezza delle reti

Tutte le pubblicazioni IBM possono essere ordinate tramite un rappresentante IBM, la filiale locale IBM oppure chiamando direttamente IBM al numero 1-800-879-2755.

Per un elenco delle pubblicazioni più rilevanti per CS/AIX, consultare la Bibliografia alla fine del libro.

Per informazioni su altre pubblicazioni, contattare il rappresentante IBM.

Informazioni accessibili dalla rete

Al fine di promuovere lo scambio di informazioni, IBM sponsorizza forum e bacheche elettronici. Inserisce home page su Internet e fornisce documentazione in linea accessibile anche su CompuServe e sul World Wide Web.

Supporto per i prodotti su IBMLink

Il forum IBMLink è ospitato su reti IBM. È progettato per aiutare i clienti che hanno acquistato prodotti concessi in licenza da IBM a risolvere problemi tecnici e altre questioni relative al proprio sistema o alla propria rete. Il personale IBM risponde alle domande e media le discussioni che si svolgono in linea tra i clienti IBM.

Per ulteriori informazioni su IBMLink, visitare l'indirizzo http://www.ibmlink.ibm.com.

Informazioni nelle home page IBM

Su Internet, varie home page IBM danno accesso a dei forum. Per una guida completa è possibile navigare dalla home page principale di IBM nei centri informazioni su Internet e sul World Wide Web. È possibile accedere all'home page principale dall'indirizzo http://www.ibm.com.

Per accedere alle informazioni relative al software di rete IBM, incluso CS/AIX, visitare il sito all'indirizzo http://www.ibm.com/software/

network. Per informazioni su CS/AIX, consultare l'indirizzo http://www.ibm.com/software/network/commserver.

Per informazioni più dettagliate sul supporto dedicato a CS/AIX, visitare l'indirizzo http://www.ibm.com/software/network/commserver/support.

Informazioni per il download

Gli utenti possono scaricare le pubblicazioni Redbook dal World Wide Web all'indirizzo http://www.redbooks.ibm.com.

Gli utenti hanno anche ampio accesso ad altre informazioni utili (ad esempio i codici dei programmi) tramite APPC Online sulla rete CompuServe (utilizzare `GO APPC`).

Per informazioni sul software IBM, visitare l'indirizzo http://www.ibm.com/software, da cui si accede alle pagine dedicate a CS/AIX e a tutti gli altri server software IBM.

Software di prova

In alcuni paesi, IBM offre software SNA gratuito in prova per 90 giorni, inclusa l'ultima versione di CS/AIX. Per informazioni dettagliate su come ottenere le copie di prova, contattare il rappresentante IBM locale o visitare la pagina di CS/AIX sul World Wide Web, all'indirizzo http://www.ibm.com/software/network/commserver/downloads.

Letture consigliate

Per coloro che desiderano approfondire le proprie conoscenze sulle reti SNA, i seguenti libri trattano la teoria SNA e l'utilizzo pratico di CS/AIX. I libri sono utili sia per i principianti che per gli esperti che potrebbero desiderare un punto di inizio per conoscere SNA o una trattazione approfondita dell'argomento.

- *Systems Network Architecture: Technical Overview* (GC30–3073)
- *IBM Communications Server for AIX Administration Guide* (SC31–8586)
- *IBM Communications Server for AIX Version 6* (SG24-5947)
- *IBM CS/AIX Understanding and Migrating to Version 5: Part 1 - Configuration and New Features* (SG24-5215)
- *IBM CS/AIX Understanding and Migrating to Version 5: Part 2 - Performance* (SG24-2136)
- *Multiprotocol Transport Networking Architecture: Technical Overview* (GC31–7073)

Per informazioni più specifiche, consultare la Bibliografia per altri riferimenti o contattare il rappresentante IBM locale.

Appendice. Note legali

Queste informazioni sono state sviluppate per prodotti e servizi offerti negli Stati Uniti. IBM può non offrire i prodotti, i servizi o le funzioni presentati in questo documento in altri paesi. Consultare il proprio rappresentante locale IBM per informazioni sui prodotti ed i servizi attualmente disponibili nella propria zona. Qualsiasi riferimento ad un prodotto, programma, o servizio IBM non implica o intende dichiarare che solo quel prodotto, programma o servizio IBM può essere utilizzato. Qualsiasi prodotto funzionalmente equivalente al prodotto, programma o servizio che non violi alcun diritto di proprietà intellettuale IBM può essere utilizzato. Tuttavia, è responsabilità dell'utente valutare e verificare il funzionamento di qualsiasi prodotto, programma o servizio non IBM.

IBM può avere applicazioni di brevetti o brevetti in corso relativi all'argomento descritto in questo documento. La fornitura del presente documento non concede alcuna licenza a tali brevetti. È possibile inviare per iscritto richieste di licenze a:

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

Per richieste di licenze relative ad informazioni double-byte (DBCS), contattare il Dipartimento di Proprietà Intellettuale IBM nel proprio paese o inviare richieste per iscritto a:

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

Il seguente paragrafo non si applica al Regno Unito o a qualunque altro paese in cui tali dichiarazioni sono incompatibili con le norme locali: IBM INTERNATIONAL BUSINESS MACHINES CORPORATION FORNISCE LA PRESENTE PUBBLICAZIONE "NELLO STATO IN CUI SI TROVA" SENZA GARANZIE DI ALCUN TIPO, ESPRESSE O IMPLICITE, IVI INCLUSE, A TITOLO DI ESEMPIO,GARANZIE IMPLICITE DI NON VIOLAZIONE, DI COMMERCIABILITÀ E DI IDONEITÀ PER UNO SCOPO PARTICOLARE. Alcuni stati non consentono la rinuncia ad alcune garanzie espresse o implicite in determinate transazioni, pertanto, la presente dichiarazione può non essere applicabile.

Queste informazioni potrebbero includere inesattezze tecniche o errori tipografici. Le modifiche alle presenti informazioni vengono effettuate periodicamente; tali modifiche saranno incorporate nelle nuove edizioni della pubblicazione. IBM può effettuare miglioramenti e/o modifiche ai prodotti e/o ai programmi descritti nella presente pubblicazione in qualsiasi momento senza preavviso.

Qualsiasi riferimento in queste informazioni a siti Web non IBM sono fornite solo per convenienza e non servono in alcun modo da approvazione di tali siti Web. I materiali presenti in tali siti Web non sono parte dei materiali per questo prodotto IBM e l'utilizzo di tali siti Web è a proprio rischio.

IBM può utilizzare o distribuire qualsiasi informazione fornita in qualsiasi modo ritenga appropriato senza incorrere in alcun obbligo verso l'utente.

I licenziatari di questo Programma che desiderano ricevere informazioni allo scopo di abilitare: (i) lo scambio di informazioni tra i programmi creati indipendentemente e gli altri programmi (incluso il presente) e (ii) il reciproco utilizzo di informazioni che sono state scambiate, devono contattare:

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

Tali informazioni possono essere disponibili, in base ad appropriate clausole e condizioni, includendo, in alcuni casi, il pagamento di una tassa.

Il programma concesso in licenza descritto nel presente documento e tutto il materiale concesso in licenza disponibile sono forniti da IBM in base alle clausole dell'Accordo per Clienti IBM (IBM Customer Agreement), dell'IBM IPLA (IBM International Program License Agreement) o qualsiasi altro accordo equivalente tra le parti.

Qualsiasi dato sulle prestazioni qui contenuto è stato determinato in un ambiente controllato. Pertanto, i risultati ottenuti in altri ambienti operativi possono notevolmente variare. Alcune misurazioni possono essere state effettuate su sistemi del livello di sviluppo e non vi è alcuna garanzia che tali misurazioni resteranno invariate sui sistemi generalmente disponibili. Inoltre, alcune misurazioni possono essere state stimate tramite estrapolazione. I risultati reali possono variare. Gli utenti del presente documento dovranno verificare i dati applicabili per i propri ambienti specifici.

Le informazioni relative a prodotti non IBM sono ottenute dai fornitori di quei prodotti, dagli annunci pubblicati e da altre fonti disponibili al pubblico. IBM non ha testato quei prodotti e non può confermarne l'accuratezza della prestazione, la compatibilità o qualsiasi altro reclamo relativo ai prodotti non IBM. Le domande sulle capacità dei prodotti non IBM dovranno essere indirizzate ai fornitori di tali prodotti.

Queste informazioni contengono esempi di dati e report utilizzati in quotidiane operazioni aziendali. Per illustrarle nel modo più completo possibile, gli esempi includono i nomi di individui, società, marchi e prodotti. Tutti tali nomi sono fittizi e qualsiasi somiglianza con nomi ed indirizzi utilizzati da gruppi aziendali realmente esistenti è puramente casuale.

LICENZA SUL DIRITTO D'AUTORE: Queste informazioni contengono applicazioni di esempio in linguaggio sorgente, che illustrano tecniche di programmazione su varie piattaforme operative. È possibile copiare, modificare e distribuire questi programmi di esempio sotto qualsiasi forma senza alcun pagamento alla IBM, allo scopo di sviluppare, utilizzare, commercializzare o distribuire le applicazioni in conformità alle API (Application Programming Interface) a seconda della piattaforma operativa per cui i programmi di esempio sono stati scritti. Questi esempi non sono stati testati approfonditamente tenendo conto di tutte le condizioni possibili. IBM, quindi, non può garantire o sottintendere l'affidabilità, l'utilità o il funzionamento di questi programmi di esempio. È possibile copiare, modificare e distribuire questi programmi di esempio sotto qualsiasi forma senza

alcun pagamento alla IBM, allo scopo di sviluppare, utilizzare, commercializzare o distribuire i programmi applicativi in conformità alle API (Application Programming Interfaces) di IBM.

Ogni copia o qualsiasi parte di questi programmi di esempio o qualsiasi lavoro derivato, deve contenere le seguenti informazioni relative alle leggi sul diritto d'autore: ® (nome della propria azienda)(anno). Parti di questo codice derivano dai Programmi di Esempio di IBM Corp. ® Copyright IBM Corp. 2000, 2005, 2006, 2007, 2008, 2009. Tutti i diritti riservati.

Marchi

IBM, il logo IBM e ibm.com sono marchi o marchi registrati di International Business Machines Corp. in numerose giurisdizioni di tutto il mondo. Altri nomi di prodotti o servizi possono essere marchi di IBM o altre società. Un elenco corrente di marchi IBM è disponibile su Web nella sezione "Informazioni su copyright" e trademark all'indirizzo www.ibm.com/legal/copytrade.shtml.

Adobe è un marchio registrato di Adobe Systems Incorporated negli Stati Uniti e/o in altri paesi.

Intel e Pentium sono marchi o marchi registrati di Intel Corporation o delle sue controllate negli Stati Uniti e in altri paesi.

Java e tutti i marchi e i logo basati su Java sono marchi di Sun Microsystems, Inc. negli Stati Uniti e/o in altri paesi.

Linux è un marchio registrato di Linus Torvalds negli Stati Uniti e/o in altri paesi.

Microsoft, Windows e Windows NT sono marchi di Microsoft Corporation negli Stati Uniti e/o in altri paesi.

UNIX è un marchio registrato di The Open Group negli Stati Uniti e in altri paesi.

Nomi di altre società, prodotti o servizi possono essere marchi di altre società.

Bibliografia

Le seguenti pubblicazioni IBM forniscono informazioni sugli argomenti trattati nella presente libreria. Le pubblicazioni sono divise nelle seguenti macroaree:

- CS/AIX, V6.4
- Redbook
- Sistema operativo AIX
- Systems Network Architecture (SNA)
- Configurazione host
- z/OS Communications Server
- Transmission Control Protocol/Internet Protocol (TCP/IP)
- X.25
- Advanced Program-to-Program Communication (APPC)
- Programmazione
- Altri argomenti relativi alle reti IBM

I libri contenuti nella libreria CS/AIX sono corredati da una breve descrizione. Per gli altri libri, sono riportati solo i titoli e i codici prodotto.

Pubblicazioni relative a CS/AIX, V6.4

La libreria CS/AIX comprende i seguenti libri. Nel CD-ROM viene fornita altresì la versione elettronica di questi documenti. Per informazioni sull'accesso alle copie elettroniche su CD-ROM, consultare *IBM Communications Server for AIX - Guida rapida*. L'installazione di queste copie elettroniche nel proprio sistema richiede 9–15 MB di spazio libero su disco (a seconda delle versioni in lingua nazionale installate).

- *IBM Communications Server for AIX Migration Guide* (SC31-8585)

  Questo libro spiega come migrare da Communications Server for AIX Versione 4, rilascio 2 o a CS/AIX Versione 6 da una versione precedente.
- *IBM Communications Server for AIX - Guida rapida* (GC31-8583)

  Questo libro funge da introduzione generale a CS/AIX e comprende informazioni sulle caratteristiche di rete supportate, sull'installazione, sulla configurazione e sul funzionamento.
- *IBM Communications Server for AIX Administration Guide* (SC31-8586)

  Questo libro fornisce una panoramica di SNA e CS/AIX, nonché informazioni sulla configurazione e il funzionamento di quest'ultimo.
- *IBM Communications Server for AIX Administration Command Reference* (SC31-8587)

  Questo libro fornisce informazioni sui comandi SNA e CS/AIX.
- *IBM Communications Server for AIX or Linux CPI-C Programmer's Guide* (SC23-8691)

  Questo libro fornisce informazioni destinate a programmatori "C" o Java esperti in merito alla scrittura di programmi di transazioni SNA tramite l'API CPI-C di CS/AIX.
- *IBM Communications Server for AIX or Linux APPC Programmer's Guide* (SC23-8692)

Questo libro contiene le informazioni necessarie per scrivere applicazioni mediante APPC (Advanced Program-to-Program Communication).

- *IBM Communications Server for AIX or Linux LUA Programmer's Guide* (SC23-8690)

  Questo libro contiene le informazioni necessarie per scrivere applicazioni tramite LUA (Conventional LU Application Programming Interface).
- *IBM Communications Server for AIX or Linux CSV Programmer's Guide* (SC23-8689)

  Questo libro contiene le informazioni necessarie per scrivere applicazioni mediante l'API (Application Program Interface) CSV (Common Service Verb).
- *IBM Communications Server for AIX or Linux MS Programmer's Guide* (SC23-8596)

  Questo libro contiene le informazioni necessarie per scrivere applicazioni mediante l'API MS (Management Services).
- *IBM Communications Server for AIX NOF Programmer's Guide* (SC31-8595)

  Questo libro contiene le informazioni necessarie per scrivere applicazioni mediante l'API NOF (Node Operator Facility).
- *IBM Communications Server for AIX Diagnostics Guide* (SC31-8588)

  Questo libro fornisce informazioni sulla risoluzione dei problemi della rete SNA.
- *IBM Communications Server for AIX or Linux APPC Application Suite User's Guide* (SC23-8595)

  Questo libro fornisce informazioni sulle applicazioni APPC utilizzate con CS/AIX.
- *IBM Communications Server for AIX Glossary* (GC31-8589)

  Questo libro fornisce un elenco esaustivo dei termini e delle definizioni utilizzati nella libreria CS/AIX.

Redbook IBM

IBM gestisce un centro di supporto tecnico internazionale che elabora pubblicazioni note con il termine "Redbook". Analogamente alla documentazione dei prodotti, i Redbook trattano aspetti teorici e pratici legati alla tecnologia SNA. Tuttavia, non includono le informazioni fornite con i prodotti di rete acquistati.

I seguenti libri contengono informazioni potenzialmente utili per CS/AIX:

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

Le pubblicazioni Redbook sono scaricabili dal Web all'indirizzo http://www.redbooks.ibm.com.

Pubblicazioni relative al sistema operativo AIX

I seguenti libri contengono informazioni relative al sistema operativo AIX:

- *AIX Versione 5.3 System Management Guide: Operating System and Devices* (SC23-4910)
- *AIX Versione 5.3 System Management Concepts: Operating System and Devices* (SC23-4908)
- *AIX Versione 5.3 System Management Guide: Communications and Networks* (SC23-4909)
- *AIX Versione 5.3 Performance Management Guide* (SC23-4905)

- *AIX Versione 5.3 Performance Tools Guide and Reference* (SC23-4906)
- *Performance Toolbox Version 2 and 3 Guide and Reference* (SC23-2625)
- *AIX Versione 5.3 Communications Programming Concepts* (SC23-4894)
- *AIX Versione 5.3 Installation Guide and Reference* (SC23-4887)
- *AIXlink/X.25 Version 2.1 for AIX: Guide and Reference* (SC23-2520)

Pubblicazioni relative alla SNA (Systems Network Architecture)

I seguenti libri contengono informazioni relative alle reti 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)

Pubblicazioni relative alla configurazione host

I seguenti libri contengono informazioni relative alla configurazione host:

- *ES/9000, ES/3090 IOCP User's Guide Volume A04* (GC38-0097)
- *3174 Establishment Controller Installation Guide* (GG24-3061)
- *3270 Information Display System 3174 Establishment Controller: Planning Guide* (GA27-3918)
- *OS/390 Hardware Configuration Definition (HCD) User's Guide* (SC28-1848)
- *ESCON Director Planning* (GA23-0364)

Pubblicazioni relative a z/OS Communications Server

I seguenti libri contengono informazioni relative a 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)

Pubblicazioni relative a TCP/IP

I seguenti libri contengono informazioni relative al protocollo di rete 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)

Pubblicazioni relative a X.25

I seguenti libri contengono informazioni relative al protocollo di rete X.25:

- *AIXLink/X.25 for AIX: Guide and Reference* (SC23-2520)
- *RS/6000 AIXLink/X.25 Cookbook* (SG24-4475)
- *Communications Server for OS/2 Version 4 X.25 Programming* (SC31-8150)

Pubblicazioni relative all'APPC

I seguenti libri contengono informazioni relative all'APPC (Advanced Program-to-Program Communication):

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

Pubblicazioni relative alla programmazione

I seguenti libri contengono informazioni relative alla programmazione:

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

Altre pubblicazioni relative alle reti IBM

I seguenti libri contengono informazioni su altri argomenti relativi a CS/AIX:

- *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)

Indice analitico

A

Abilitazione di CS/AIX
  nel sistema locale 74
Advanced Interactive Executive (AIX) 1
Advanced Program-to-Program Communication (APPC) 5
Agente SNMP 15
Aggiunta di una risorsa 77
AIX
  eseguire CS/AIX su 1
  pagine del manuale 30
  requisiti hardware per CS/AIX 19
Alias, definizione per la LU partner 91
AnyNet
  Configurazione di APPC over TCP/IP 105
API
  per la gestione di CS/AIX 13
  supporto 4
  tipi di CS/AIX 4
API NOF 13
APPC
  application suite 6, 8
  configurazione 87
  in linea 110
  Interactive Application Development Toolkit 30
  LU 6.2 dipendente 92
  LU 6.2 indipendente 89
  supporto applicazioni distribuite 5
APPC Application Suite 8
APPC over TCP/IP 105
  configurazione 106
Application Programming Interface (API) 4
Applicazione gestore 15
Applicazioni partner 5
APPN
  applicazioni per 6, 8
  configurazione 88, 89
  configurazione dinamica 13
  funzioni di sottoarea 2
  instradamento 14
  nodo di rete 1
  nodo finale 1
  rete di connessione 14
  segmentazione delle reti 26
  servizio di gestione distribuita 15
  supporto DLUR 2
  supporto host per 2
  supporto LU indipendente 3
  tipi di nodo 1
Arrestare una risorsa 77
Attività di preinstallazione 31
Avviare una risorsa 77
Avvio di CS/AIX
  automatico all'avvio del sistema 74
Avvisi 16

B

Backup
  file di configurazione 40
  ripristino 41
Base Operating System (BOS) 21
BOS (Base Operating System) 21
Branch Extender 7
Branch Network Node 7
Buffer di memoria (mbuf) 23

C

Caratteri jolly 92
CDE 34
Chiamate 4
CICS (Customer Information Control System) 5
Client 5
Client/server
  configurazione 79
Comandi di stato 15
Comandi query 15
Comando di arresto 108
Comando di avvio 74
Common Desktop Environment (CDE) 34
Common Programming Interface for Communications (CPI-C) 4
Compressione, dati di una sessione LU 3
Computer in downstream 95
Concentratore di PU 6
Concentrazione PU 94
Configurazione 18
  APPC over TCP/IP 106
  backup 40
  comunicazione APPC 87
  connettività 81
  DLUR 97
  esempi 80, 97, 100
  file 40, 42
  informazioni ubicazione CPI-C 93
  LU 6.2 89, 92
  LU di tipo 0–3 85
  LU in downstream implicite 95
  LU in downstream per il gateway SNA 94
  LU partner di un nodo LEN 90
  modifica 77
  nodo 80
  nodo remoto 91
  pianificazione 72
  porta 83
  record di associazione al server TN 103
  Valori predefiniti del programma di reindirizzamento TN 105
  Valori predefiniti del server TN 103
  visualizzazione 77
Configurazione della porta 83, 84, 85
Configurazione delle LU in downstream implicite 95
Configurazione di una LU 6.2 indipendente 89
Configurazione dinamica 13
Configurazioni avanzate, requisiti di memoria e memorizzazione 22
Connettività
  configurazione 81
  opzioni 2
Controllo collegamento dati (DLC, Data Link Control) 27
Convenzioni di denominazione 26
CPI-C
  API 4
  configurazione 93
  interoperabilità 16
CPI Communications (CPI-C) 4
Customer Information Control System (CICS) 5

D

DATABASE 2 (DB2) 5
DB2 (DATABASE 2) 5
DDDLU (Dynamic Definition of Dependent LU) 3
Dependent Logical Unit Server (DLUS) 97
Dependent LU Requester (DLUR) 2
Directory per i programmi eseguibili di CS/AIX 73
Disabilitazione di CS/AIX 107
Disinstallazione di Remote API Client su AIX 58
Disinstallazione di Remote API Client su Linux 47
Disinstallazione di Remote API Client su Linux for System z 53
DLC
  configurazione 84, 85
  installazione 31
  nella configurazione della porta 82
  scopo 27
DLUR
  configurazione 97
  configurazione PU 99
  descrizione 2
  nel nodo locale 98
  supporto per i nodi in downstream 99
DLUS 97
Documentazione, in linea 109
Dominio 5
Dynamic Definition of Dependent LU (DDDLU) 3

E

Elaborazione distribuita
  ambiente 1
  supporto applicazioni 5
Eliminazione di una risorsa 77
Enterprise Extender
  configurazione del collegamento 84
  finestra di dialogo della porta 85
  panoramica 9
Ethernet
  configurazione del collegamento 83
  finestra di dialogo SAP 84

F

File rc.sna 74
Finestra 75
Finestra Configuration, Remote API Client su Windows
  parametri 62
  parametri avanzati 64
Finestra di dialogo 75
Finestra di dialogo della porta IP 85
Finestra Node 75
Flusso di dati 4
Fogli di lavoro, pianificazione 72
Fogli di lavoro per la pianificazione 72
Fogli di lavoro per le attività 73
Formati dell'indirizzo IP 24
Forum, in linea 109
funzioni 30
Funzioni 4
Funzioni software 6

G

Gateway
  definizione 6
  Gateway SNA 6
Gateway SNA
  configurazione 94
  panoramica 6
Gestione dei componenti 75
Gruppi di discussione, in linea 109
GSKIT
  Remote API Client su AIX 55, 57
  Remote API Client su Linux 44, 46
  Remote API Client su Linux for System z 49, 52
  Remote API Client su Windows 67
Guida
  Programma di gestione Motif 12
  Programma di gestione Web 13

H

Hardware
  collegamento 20
  requisiti 19
Hardware di collegamento 20
Host
  in una rete APPN 2
  nella rete di sottoarea 1
  supporto LU 2
Host Access Class Library
  file 40
  panoramica 6
  serie di file 30
HPR
  rispetto all'ISR 14
HPR/IP 9
HTTPS
  configurazione 37
  Remote API Client su AIX 57
  Remote API Client su Linux 46
  Remote API Client su Linux for System z 52
  Remote API Client su Windows 67
  requisiti 22

I

In linea
  APPC 110
  documentazione 109
  forum 109
  gruppi di discussione 109
  guida 12, 13
Indirizzo IPv4 24
Indirizzo IPv6 24
Informazioni sul rilascio 39
Installazione
  attività di manutenzione successive 38
  informazioni dettagliate sui pacchetti esistenti 31
  manuale 34, 35, 36
  mediante Installazione rapida 33
  preparazione di 31
  Remote API Client su AIX 56, 57
  Remote API Client su Linux 45
  Remote API Client su Linux for System z 50
Installazione client/server 38
Installazione di Remote API Client su AIX 56, 57
Installazione di Remote API Client su Linux 45
Installazione di Remote API Client su Linux for System z 50
Installazione manuale 34
Installazione rapida
  mediante CDE 34
  tramite SMIT 34
Intermediate Session Routing (ISR) 14
International Organization for Standards (ISO) 26
ISO (International Organization for Standards) 26
ISR (Intermediate Session Routing) 14

J

Java
  Remote API Client su AIX 55
  Remote API Client su Linux 44
  Remote API Client su Linux for System z 49

L

LAN (Local Area Network) 2
Letture consigliate 110
Licensed Program Product (LPP) 29
Licenze nodelock 28
Local Area Network (LAN) 2
Logical Unit (LU) 2, 96
LPP (Licensed Program Product) 29
LU
  configurazione 89, 92, 102
  convenzioni di denominazione 26
  downstream 95, 96
  partner, definizione 90
  pool 101, 102
  supporto 2
LU 3270
  definizione 102
  per server TN 10, 100
LU 6.2 dipendente 92
LU di tipo 0–3 85, 86
LU in downstream
  configurazione 96
  esempi di hardware 95
  per il gateway SNA 94
LU locale, definizione 89
LU partner
  alias 91
  configurazione 90
  definizione tramite caratteri jolly 92
  su un nodo remoto 91

M

MAC (Medium Access Control) 84
mbuf (buffer di memoria) 23
MDS-NMVT (Multiple Domain Support-Network Management Vector Transport) 14
Meccanismi di gestione delle licenze 27
Medium Access Control (MAC) 84
Memoria di paginazione 23
Memoria principale 23
Memorizzazione principale 23
Mezzi di trasporto 20
Migrazione da livelli precedenti di CS/AIX 32
Modifica della configurazione 77
MPQP (Multiprotocol Quad Port) 20
Multiple Domain Support-Network Management Vector Transport (MDS-NMVT) 14
Multiprotocol Quad Port (MPQP) 20

N

Network Installation Management 36
NIM (Network Installation Management) 36
Nodo
  comunicazione con l'host 80
  configurazione 80
  downstream 99
  in una configurazione APPN 81
  locale 98
  remoto 90, 91
  upstream 97

Nodo in downstream 97
Nodo in upstream 97
Nodo LEN
  configurazione LU partner 90
  descrizione 1
  identificazione del nodo remoto 84
Nodo LEN (Low-Entry Networking) 84
Nodo remoto
  configurazione 90, 91
  configurazione LU partner 91
Nome server 62

O

Open Systems Interconnection (OSI) 26
Opzioni controllo collegamento dati (DLC) 2
Opzioni di sicurezza 14
Opzioni interfaccia 13
OSI (Open Systems Interconnection) 26

P

Pacing, livello sessione 14
Pacing adattivo a livello sessione 14
Pagine del manuale 30
Parametro dominio 62
Parametro numero massimo di tentativi di trasmissione 64
Parametro Timeout di accesso LAN 64
Parametro Timeout di riconnessione 64
Parametro trasmissioni UDP 63
PDF, visualizzazione dei libri 39
Peer
  rete 1
Percorso per i programmi eseguibili di CS/AIX 73
Physical Unit (PU) 6
Pianificazione della compatibilità 25
Pool di LU
  configurazione 87
  definizione 86
  visualizzazione 86
Problema
  dati 16
  strumenti diagnostici 15
Procedure
  installazione di Remote API Client su Windows 61, 65
Procedure successive all'installazione 38
Program Temporary Fixes (PTF) 31
Programma concesso in licenza 33
  Remote API Client su AIX 56
  Remote API Client su Linux 45
  Remote API Client su Linux for System z 50
Programma di gestione
  API NOF 13
  Motif 12, 15
  riga di comando 13
  SMIT 13
  Web 13
Programma di gestione da riga comando 13
Programma di gestione Motif
  descrizione 12
Programma di gestione Motif *(Continua)*
  funzionalità di gestione 15
  guida 12
  tramite 71
Programma di gestione Web
  descrizione 13
  guida 13
Programma di reindirizzamento TN
  configurazione 104
  configurazione dei valori predefiniti 105
  configurazione del record degli accessi 105
  panoramica 11
Programma snaadmin 13
Programma xsnaadmin 12, 71
Programmi TN3270 99
PTF (Program Temporary Fixes) 31
PU (Physical Unit) 6
Pulsanti della barra degli strumenti 78
Pulsanti delle finestre delle risorse 78
Punto centrale 14
Punto di accesso al servizio (SAP) 20, 83
Punto di ingresso 14

R

RAM (Random Access Memory) 23
Random Access Memory (RAM) 23
Remote API Client
  requisiti hardware di AIX 55
  requisiti hardware di Linux 43
  requisiti hardware di Linux for System z 49
  requisiti software di AIX 55
  requisiti software di Linux 44
  requisiti software di Linux for System z 49
Remote API Client su Linux
  informazioni dettagliate sui pacchetti esistenti 44
Remote API Client su Linux for System z
  informazioni dettagliate sui pacchetti esistenti 50
Remote API Client su Windows
  installazione 60
  installazione con il programma di installazione 61
  installazione dalla riga comando 65
Requisiti
  hardware 19
  HTTPS 22
  installazione 20
  memoria e memorizzazione 22
  personale e competenze 19
  software 21
  WebSphere Application Server 22
Requisiti del personale 19
Requisiti di installazione 20
Requisiti di memoria 22
  configurazioni avanzate 22
  tipi di memorizzazione 23
Requisiti di memorizzazione 22
Requisiti funzionali 17
Requisiti hardware
  Remote API Client su AIX 55
  Remote API Client su Linux 43
Requisiti hardware *(Continua)*
  Remote API Client su Linux for System z 49
  Remote API Client su Windows 59
Requisiti in termini di competenze 19
Requisiti software 21
  Remote API Client su AIX 55
  Remote API Client su Linux 44
  Remote API Client su Linux for System z 49
  Remote API Client su Windows 59
Rete
  avvisi 16
  convenzioni di denominazione 26
  gestione 14
  informazioni disponibili attraverso la 109
  peer-to-peer 1
  pianificazione 17, 18, 25, 26
  sottoarea 1
  supporto 1
Rete di connessione 14
Rete di connessione, configurazione 84
Risorsa
  arrestare 77
  avviare 77
  definizione 77
  eliminazione 77
  gestione 75
  informazioni 109
  requisiti 18
  voci 78
Risorse informative 109
RUI principale 3

S

SAA (Systems Application Architecture) 4
SAP (punto di accesso al servizio) 20, 83
Schede di comunicazione 20
SDLC
  configurazione 83
  per il traffico dipendente 82
Secure Sockets Layer (SSL)
  autenticazione del client 103, 104
  autenticazione del server 39, 103, 104
  crittografia dati 39, 103, 104
Server 5
  aggiunta 79
  eliminazione 79
Server, Telnet 9
Server di backup 5
Server di configurazione 79
  aggiunta 79
  eliminazione 79
Server master 5
Server master di backup 79
Server multipli in un dominio 5
Server peer 5
Server TN
  configurazione 99
  configurazione dei valori predefiniti 103
  configurazione del record degli accessi 103

Server TN *(Continua)*
configurazione del record di associazione 103, 104
panoramica 9
supporto sessioni multiple 101
utente 101
Sessione
a ″U″ 3
instradamento 14
pacing 14
supporto 3
Sessioni a ″U″ 3
Simple Network Management Protocol-Management Information Base (SNMP-MIB) 15
SMIT
configurazione DLC 27
installazione manuale 34
Installazione rapida 34
SMIT (System Management Interface Tool) 13, 19
SNA
libreria 109
SNA Channel Data Link 30
SNMP-MIB (Simple Network Management Protocol-Management Information Base) 15
Software del client
aggiornamento 68
disinstallazione 69
personalizzazione 68
reinstallazione 68
Software SDK
Remote API Client su Windows 60
Sottoroutine 4
Spazio su disco 23
Spazio su disco fisso 22
Stazione di collegamento
definizione nella porta 83
Stazione di lavoro
requisiti 19
Stazioni di lavoro RISC System/6000 19
Strumenti per la risoluzione dei problemi 15
Supporto client/server 5
Synchronous Data Link Control (SDLC) 82
System Management Interface Tool (SMIT) 13, 19, 27
Systems Application Architecture (SAA) 4

T

Tempo di risposta 24
TN3270
programmi 9
server 9
TP (Transaction Program) 4
Transaction Program (TP) 4
Trasparenza, locale/remota 3
Trasparenza locale/remota 3

U

Utente TN3270 10, 100

V

Variabile d'ambiente della lingua 32, 56
Remote API Client su Linux 44
Remote API Client su Linux for System z 50
Verbi 4
Versione, indirizzo IP 24
Visualizzazione della configurazione 77

W

WAN (Wide Area Network) 2
WebSphere Application Server
configurazione 37
requisiti 22
Wide Area Network (WAN) 2

Numero programma: 5765-E51

Stampato in Italia

GC13-4142-04