IBM Communications Server pour AIX

Guide d'initiation

V6.3

GC11-1439-02

IBM Communications Server pour AIX

Guide d'initiation

V6.3

GC11-1439-02

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 127.

Remarque

Les captures d'écrans de ce manuel ne sont pas disponibles en français à la date d'impression.

Troisième édition - novembre 2005

Réf. US : GC31-8583-02

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- http://www.fr.ibm.com (serveur IBM en France)
- http://www.can.ibm.com (serveur IBM au Canada)
- http://www.ibm.com (serveur IBM aux Etats-Unis)

Compagnie IBM France
Direction Qualité
Tour Descartes
92066 Paris-La Défense Cedex 50

Table des matières

Avis aux lecteurs canadiens

Le présent document a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

Terminologie

La terminologie des titres IBM peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

IBM France	IBM Canada
ingénieur commercial	représentant
agence commerciale	succursale
ingénieur technico-commercial	informaticien
inspecteur	technicien du matériel

Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien de type QWERTY.

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

- les pages de codes 850 (multilingue) et 863 (français-canadien),
- le code pays 002,
- le code clavier CF.

Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

France	Canada	Etats-Unis
(Pos1)		Home
Fin	Fin	End
(PgAr)		PgUp
(PgAv)		PgDn
Inser	Inser	Ins
Suppr	Suppr	Del
Echap	Echap	Esc
Attn	Intrp	Break
Impr écran	ImpEc	PrtSc
Verr num	Num	Num Lock
Arrêt défil	Défil	Scroll Lock
(Verr maj)	FixMaj	Caps Lock
AltGr	AltCar	Alt (à droite)

Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.

Tableaux

Figures

Bienvenue dans Communications Server pour AIX

Ce manuel présente IBMCommunications Server pour AIX (CS/AIX), un logiciel IBM qui permet l'échange de données entre un serveur fonctionnant avec le système d'exploitation AIX d'IBM et les autres noeuds sur un système SNA (Systems Network Architecture). Il s'agit du produit de réseau SNA le plus complet actuellement disponible pour les postes de travail POWER fonctionnant avec le système d'exploitation de base AIX Version 5.

Communications Server pour AIX est conçu pour fonctionner sur un poste de travail AIX relié à un ou plusieurs réseaux. CS/AIX V6.3 peut fonctionner sur tout système IBM RISC System/6000 ou eServer pSeries pris en charge par AIX v5.2 ou v5.3. Dans le présent manuel, le terme station de travail AIX désigne tout système parmi ceux mentionnés ci-dessus.

CS/AIX fournit des éléments offrant une large gamme de solutions de réseau pour répondre à des besoins très variés. Il permet de communiquer avec des nœuds de réseau SNA, TCP/IP et SNA-TCP/IP intégrés.

Pour nous faire part de vos commentaires et suggestions sur le *Guide d'initiation d'IBM Communications Server pour AIX*, utilisez le formulaire "Remarques du lecteur", à la fin de ce manuel. Ce formulaire indique comment nous adresser vos commentaires par voie postale, par télécopie ou par courrier électronique.

Dans ce manuel, les dénominations suivantes sont utilisées pour désigner Communications Server pour AIX et ses fonctions :

Nom complet	Dénomination abrégée
Communications Server pour AIX version 6	CS/AIX V6.3
AnyNetAIX APPC sur TCP/IP	APPC sur TCP/IP

Comment utiliser ce manuel ?

Cette section décrit l'organisation et la présentation des informations dans le manuel.

Où trouver l'information ?

Ce manuel s'adresse au personnel de gestion et au service technique chargé de la planification du réseau, et à toute personne intéressée par Communications Server pour le système d'exploitation AIX.

Pour obtenir les informations nécessaires à l'apprentissage de CS/AIX, reportez-vous au tableau 1.

Tableau 1. Où trouver l'information ?

Pour...	Consultez...
En savoir plus sur CS/AIX	Chapitre 1, «A propos de Communications Server pour AIX», à la page 1

Tableau 1. Où trouver l'information ? (suite)

Pour...	Consultez...
Planifier l'utilisation de CS/AIX dans votre réseau	Chapitre 2, «Organisation du réseau et de Communications Server pour AIX», à la page 19
Installer CS/AIX sur des serveurs AIX	Chapitre 3, «Installation de CS/AIX sur des serveurs AIX», à la page 29
Installer les clients Remote API Client sous Linux	Chapitre 4, «Installation des clients IBM Remote API Client sous Linux», à la page 47
Installer les clients Remote API Client sous Linux pour zSeries	Chapitre 5, «Installation d'IBM Remote API Clients sous Linux pour zSeries», à la page 53
Installer les clients Remote API Client sous Linux pour pSeries	Chapitre 6, «Installation d'IBM Remote API Clients sous Linux pour pSeries», à la page 59
Installer les clients Remote API Client sous AIX	Chapitre 7, «Installation d'IBM Remote API Client sur des systèmes AIX», à la page 65
Installer les clients Remote API Client sous Windows	Chapitre 8, «Préparation et installation de Remote API Client sous Windows», à la page 71
Configurer CS/AIX	Chapitre 9, «Configuration et utilisation de CS/AIX», à la page 83
Trouver des informations sur la documentation CS/AIX et d'autres publications, notamment l'aide en ligne	Chapitre 10, «Sources d'informations pour CS/AIX et SNA», à la page 125
Lire les remarques et les informations relatives aux marques	«Remarques», à la page 127

Conventions typographiques

Le tableau 2 indique les styles typographiques utilisés dans le présent document.

Tableau 2. Conventions typographiques

Élément	Exemple de typographie
Termes mis en évidence	**sauvegarder les fichiers avant suppression**
Titre de document	*Communications Server for AIX Administration Guide*
Nom de fichier ou de chemin	**/usr/spool/uucp/monfichier.bkp**
Programme ou application	**snaadmin**
Entrée utilisateur	**0p1**
Sortie d'ordinateur	**FERMETURE**

Abréviations utilisées dans ce manuel

Dans ce manuel, vous rencontrerez les abréviations suivantes :

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 (système d'exploitation de base)
BrNN	nœud de réseau de type branche
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 LUs
DES	Data Encryption Standard
DLC	Data link control (contrôle de liaison de données)
DLUR	Dependent LU Requester
DLUS	Dependent LU Server
FDDI	Fiber Distributed Data Interface
FTP	File Transfer Protocol
GSNA	Generic SNA API
HPR	High-Performance Routing
IEEE	Institute of Electrical and Electronics Engineers
IETF	groupe de travail IETF (Internet Engineering Task Force)
ISO	International Organization for Standards
ISR	Intermediate session routing
LAN	Local area network (réseau local)
LDAP	Lightweight Directory Access Protocol
LEN	Low-entry networking
LLC2	Logical Link Control 2
LU	Logical unit (unité logique)
LUA	interface API LU conventionnelle
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 (unité physique)
RFC	document RFC (Request For Comment)
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 (contrôle de liaison de données synchrone)
SLP	Service Location Protocol
SMIT	Systems Management Interface Tool
SMP	Symmetric multiprocessing
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 (programme de transaction)
VT	Virtual Terminal
VTAM	Virtual Telecommunications Access Method
WAN	Wide area network (réseau étendu)

Nouveautés

Communications Server pour AIX V6.3 remplace Communications Server pour AIX V6.1.

Les versions de ce produit encore prises en charge sont les suivantes :

- Communications Server pour AIX V6.1

En revanche, les versions ci-dessous ne sont plus prises en charge :

- Communications Server pour AIX version 6 (V6)
- Communications Server pour AIX version 5 (V5)
- Communications Server pour AIX version 4 édition 2 (V4R2)
- Communications Server pour AIX version 4 édition 1 (V4R1)
- SNA Server pour AIX version 3 édition 1.1 (3.1.1)
- SNA Server pour AIX version 3 édition 1 (3.1)
- SNA Server/6000 pour AIX version 2 édition 2 (2.2)
- SNA Server/6000 pour AIX version 2 édition 1 (2.1) sur AIX 3.2
- AIX SNA Services/6000 Version 1

Nouvelles fonctions

Dans cette version, CS/AIX s'est enrichi des fonctions suivantes :

- Prise en charge des clients IBM Remote API Client, fonctionnant sous AIX, Windows ou Linux. Ces clients peuvent communiquer avec le serveur CS/AIX (ou avec un serveur CS Linux) par TCP/IP, ou HTTPS via un serveur WebSphere.
- CS/AIX prend maintenant en charge la résolution dynamique de nom d'hôte IPv4 pour les noms d'hôtes IPv4 qualifiés et non qualifiés, tel que défini dans l'architecture APPN, mise à jour AMB 8538.
- L'interface SLI (Session Level Interface) est maintenant intégrée à l'interface LUA.
- CS/AIX prend maintenant en charge l'interface RUI principale au niveau de l'interface LUA. Cela permet d'écrire une application fonctionnant en tant que primaire SNA pour la communication avec les unités physiques en aval.
- Visibilité LU TN3270 : CS/AIX peut envoyer un vecteur de contrôle (CV64) à l'hôte lors de la connexion du client, pour identifier l'adresse IP du client TN3270.
- Les paramètres d'optimisation HPR sont maintenant fournis à l'aide des commandes d'administration **define_rtp_tuning** et **query_rtp_tuning**.
- Des informations d'état complémentaires sont fournies pour les redirections TN à l'aide de TN_REDIRECTION_INDICATION.

Fonctions retirées

La fonction AnyNet Sockets sur SNA a été retirée dans cette version.

La fonction AnyNet APPC sur TCP/IP est toujours prise en charge dans cette version, mais uniquement pour les systèmes 32 bits et non 64 bits. Elle ne sera plus prise en charge dans les prochaines versions.

Où trouver des informations supplémentaires ?

La bibliographie répertorie les autres manuels consacrés à CS/AIX, ainsi que des ouvrages contenant des informations complémentaires sur SNA, le système d'exploitation AIX et d'autres produits de ce type.

Dans les titres de la bibliothèque IBM Communications Server pour AIX, le nom du produit est abrégé sous la forme «Communications Server pour AIX». Dans les références aux manuels de Communications Server pour AIX V4R2 (pour les informations concernant la migration de V4R2 ou d'une édition antérieure vers l'édition actuelle), le titre du manuel contient l'abréviation «V4R2». Il n'est pas nécessaire de faire référence aux manuels précédents si la migration est effectuée de la version 5, 6 ou 6.1 vers la version en cours car aucune mesure n'est requise pour cette migration : votre configuration existante peut être utilisée sans que la version en cours soit modifiée.

Les informations contenues dans les manuels CS/AIX sont également disponibles au format HTML. Vous pouvez utiliser cette bibliothèque pour rechercher des informations spécifiques ou pour afficher les versions en ligne des manuels CS/AIX.

Chapitre 1. A propos de Communications Server pour AIX

Dans ce chapitre sont décrits les logiciels qui composent CS/AIX, leurs fonctions et leurs avantages.

Logiciels et fonctions de Communications Server pour AIX

CS/AIX V6.3 est un logiciel de communication qui fonctionne sur le système d'exploitation AIX . Il comprend les fonctions décrites dans les sections «Communications Server pour AIX V6.3» et «Fonctions de gestion de réseau évoluées», à la page 7.

Communications Server pour AIX V6.3

Communications Server pour AIX V6.3 relie les applications via les réseaux SNA et TCP/IP. Il convertit un poste de travail AIX en nœud SNA en l'équipant de ressources et de protocoles SNA. Le poste de travail peut ainsi communiquer avec d'autres postes de travail et des systèmes hôte sur le réseau SNA. Il fournit également des fonctions TCP/IP permettant l'utilisation de Communications Server pour AIX au sein de votre réseau TCP/IP ou à la frontière entre les réseaux TCP/IP et SNA.

CS/AIX offre les services suivants :

Support de réseau

CS/AIX prend en charge les réseaux articulés autour d'un système hôte et les réseaux d'égal à égal :

Réseaux SNA articulés autour d'un système hôte

Ces réseaux sont organisés de manière hiérarchique. Ainsi, un ou plusieurs systèmes hôte contrôlent les communications entre les ordinateurs, gèrent le réseau et fournissent des services de traitement et de stockage de gros volumes de données. Tous les autres nœuds du réseau sont sous le contrôle d'un système hôte.

Les ordinateurs AIX configurées comme des nœuds dépendants de l'hôte peuvent participer à un réseau d'hôte intermédiaire.

Réseaux d'égal à égal

Pour les environnements de traitement réparti, CS/AIX V6.3 prend en charge les réseaux APPN et TCP/IP. Dans ces réseaux d'égal à égal, les ordinateurs AIX utilisent moins leurs fonctions de traitement et communiquent directement entre eux, d'égal à égal. Ces réseaux exploitent toutes les fonctions des ordinateurs AIX, qui concurrencent aujourd'hui les systèmes hôte coûteux.

Un réseau APPN est constitué de nœuds d'égal à égal de différents types :

- Nœud de réseau APPN (qui contrôle le trafic, calcule et sélectionne les routes de manière dynamique et gère le réseau)
- Nœud d'extrémité APPN (qui utilise les services des nœuds de réseau APPN pour communiquer avec d'autres nœuds homologues)
- Nœud LEN (qui communique directement avec des nœuds adjacents ou des nœuds configurés comme tels)

Remarque : Les ordinateurs hôte peuvent jouer le rôle de nœuds homologues dans un réseau APPN en utilisant des LU 6.2 indépendantes pour communiquer avec des ordinateurs AIX et d'autres hôtes du réseau.

Utilisation de fonctions de système hôte dans un réseau APPN
La fonction de demandeur de LU dépendantes (DLUR) permet de faire circuler des données entre des systèmes hôte et des nœuds dépendants d'un système hôte, dans un réseau APPN.

Options de contrôle de liaison de données
CS/AIX offre un grand nombre d'options de connectivité destinées à répondre aux besoins liés à la taille, au débit, à la sécurité et au coût du réseau. (Vous pouvez consulter la liste exhaustive des types de liaisons supportées à la section «Conditions requises pour l'installation», à la page 22.) CS/AIX prend en charge les liaisons de données dans des types de réseau différents tels que les suivants :

Réseaux locaux
Pour assurer la connectivité des réseaux locaux, vous pouvez installer les liaisons destinées à communiquer à l'aide des protocoles Token Ring, Ethernet standard et Ethernet 802.3. (L'interface de réseau local émulé permet d'accéder au mode de transfert asynchrone (ATM) sur un réseau en anneau à jeton ou Ethernet.

Réseaux longue distance
Pour assurer la connectivité des réseaux longue distance, vous pouvez choisir l'une des liaisons synchrones suivantes, destinées à communiquer via les lignes téléphoniques installées :

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

CS/AIX prend également en charge le contrôle de liaison de données à commutation de paquets X.25 (ces types de liaison nécessitent des produits supplémentaires, qui peuvent être commandés séparément)

Intégration IP
Si le réseau de base de votre entreprise est fondé sur le protocole IP, vous pouvez utiliser la fonction Enterprise Extender (HPR/IP) de CS/AIX pour l'intégrer à SNA, ce qui permet aux applications SNA de communiquer via le réseau IP.

Support de LU
Les unités logiques (LU) sont des ressources réseau propres aux applications, situées dans chaque nœud d'un réseau SNA. Chaque LU joue le rôle d'une interface que les applications utilisent pour accéder aux liaisons, afin de communiquer sur le réseau avec les applications partenaires des autres nœuds.

CS/AIX prend en charge différents types de LU, correspondant à différentes classes d'applications.

- Dans un réseau articulé autour d'un système hôte, CS/AIX prend en charge les LU dépendantes, qui appartiennent à l'un des types suivants :
  - LU 0
  - LU 1
  - LU 2
  - LU 3
  - LU 6.2

  La LU 0 assure la communication de programme à programme à l'aide d'une primitive. En règle générale, elle est utilisée pour les transactions sur le lieu de vente, dans le commerce de détail et la banque. LU 2 prend en charge les applications d'émulation de terminal, qui permettent à l'ordinateur AIX d'émuler un terminal de la famille IBM 3270. Les autres types de LU permettent d'utiliser des applications pour le traitement réparti, ou de communiquer avec différents types d'imprimantes ou de terminaux interactifs.

  CS/AIX prend en charge des systèmes hôte qui ont recours à la définition dynamique de LU dépendantes (DDDLU),une fonction de système hôte qui permet d'ajouter à la configuration du système hôte des LU dépendantes appartenant au système SNA, une fois que la liaison entre le système SNA et le système hôte est établie. Grâce à la fonction DDDLU, il n'est plus nécessaire de configurer les LU de manière statique sur le système hôte. (Néanmoins, il est toujours nécessaire de définir les LU dépendantes dans le nœud CS/AIX.) Cette fonction contribue à réduire la configuration initiale du système hôte et à faciliter les extensions futures.

  CS/AIX peut aussi bien communiquer avec des systèmes hôte qui assurent cette fonction qu'avec des systèmes hôte qui ne l'assurent pas, sans que la configuration requise ne s'en trouve affectée. Une fois que la liaison entre le nœud CS/AIX et le système hôte est établie, un système hôte doté de la fonction DDDLU informe le nœud qu'il prend en charge cette fonction ; le nœud envoie ensuite les informations requises pour définir les LU dépendantes qui vont utiliser la liaison. Si le système hôte concerné n'est pas doté de la fonction DDDLU, CS/AIX n'envoie pas ces informations ; le nœud considère que les LU ont déjà été définies de manière statique sur le système hôte.
- La LU 6.2 indépendante prend en charge le trafic sur les réseaux APPN. La LU 6.2 indépendante prend en charge la gestion autonome des communications et du réseau, ainsi que le traitement réparti.

  De plus, la fonction de DLUR de CS/AIX permet aux données provenant de LU dépendantes de passer par un réseau APPN.
- La prise en charge d'interface RUI principale permet à une application CS/AIX de gérer les unités des unités de LU dépendantes reliées au réseau LAN/WAN en aval comme s'il s'agissait d'un grand système. Cette fonction présente des restrictions en termes de connectivité, mais elle permet aux applications de transférer des données entre les unités des LU dépendantes sans utiliser d'application de grand système.

Support de session

Une session est un canal logique provisoire qui relie des LU partenaires. En règle générale, les applications partenaires associées à chaque LU communiquent par cette session. CS/AIX peut prendre en charge des milliers de sessions. CS/AIX peut également prendre en charge des sessions de type U (ou «transparence locale/éloignée»), dans lesquelles les LU principales et secondaires résident sur le même ordinateur AIX. Cette

fonction permet de mettre au point et de tester les programmes de transaction par paire (source et cible) sur un seul et même ordinateur, sans connexion.

Les données transférées lors d'une session entre deux LU partenaires peuvent être compressées, afin de réduire la bande passante nécessaire.

- Sous CS/AIX, vous pouvez définir l'utilisation de la compression pour les LU de type 6.2 dans la configuration du mode utilisé durant la session. Vous pouvez définir plusieurs algorithmes de compression à utiliser selon le niveau de compression souhaité (RLE, LZ9 ou LZ10). Vous pouvez également définir différents niveaux de compression des données selon le sens dans lequel elles sont transférées durant une session, ou bien appliquer la compression dans un sens et pas dans l'autre.
- Pour les LU de type 0–3, CS/AIX vous permet de définir l'utilisation de la compression dans la configuration du poste de liaison ou de l'unité physique utilisé durant la session. La compression RLE est utilisée pour le flux entrant et la compression LZ9 pour le flux sortant.

Support d'API

CS/AIX contient des interfaces de programmes d'applications (API) permettant de développer des applications destinées à certains types de LU, au traitement réparti, à la gestion de réseau et à l'administration de CS/AIX proprement dite. Dans la présente version, CS/AIX offre un ensemble d'API compatibles avec celles que fournissent les produits de la famille Communications Server tournant sur d'autres systèmes d'exploitation.

Une API est une interface qui permet de faire communiquer un programme de transactions (TP) avec la LU qui le prend en charge. Elle est constituée d'une bibliothèque d'instructions (également appelées fonctions, appels et sous-programmes), dans laquelle le TP choisit ceux qui doivent être transmis à la LU pour solliciter une action, telle que SEND_DATA. Ensuite, la LU procède au traitement des instructions, puis crée une séquence de données selon le protocole approprié, lui attribue un en-tête indiquant l'adresse de destination, et envoie les données aux LU partenaires, par la liaison.

L'interface CPI-C (interface commune de programmation d'applications de communication) est l'une des API les plus puissantes, du fait de sa portabilité. Conçue pour prendre en charge des LU 6.2 dépendantes et indépendantes, CPI-C est conforme aux spécifications de l'architecture SAA (Systems Application Architecture) visant à unifier des plateformes et des systèmes d'exploitation différents. CPI-C utilise un ensemble de règles syntaxiques communes à tous les systèmes. Elle est donc devenue une norme.

En plus de l'API CPI-C en langage C standard, CS/AIX comprend également une API CPI-C destinée aux applications Java. Pour plus d'informations, voir le manuel *Communications Server for AIX CPI-C Programmer's Guide*. Dans les manuels CS/AIX, toutes les références à CPI-C incluent CPI-C Java, sauf indication contraire.

Parmi les autres API de CS/AIX, on trouve :

- L'API APPC, destinée aux communications d'égal à égal entre des programmes d'applications utilisant des LU 6.2. Cette API dispose d'une option non bloquante. Ainsi, lorsqu'un TP utilise des instructions non

bloquantes, l'API peut renvoyer le contrôle au TP avant que l'action demandée ne soit exécutée. Le TP sera informé ultérieurement, une fois que l'action aura été exécutée.

- L'API LUA, destinée à la communication avec les applications de système hôte.
- L'API CSV (Common Service Verb), destinée aux fonctions utilitaires, telles que la conversion de caractères et le contrôle de trace d'application.

Par ailleurs, CS/AIX comprend les interfaces de programme propriétaires suivantes :

- Les API de gestion de services (MS), destinées aux fonctions de messagerie de réseau.
- L'API NOF (Node Operator Facility), destinée aux applications de configuration et de gestion des ressources CS/AIX.

Les applications utilisant les API CS/AIX peuvent être compilées et reliées de sorte qu'elles s'exécutent en mode 32 ou 64 bits.

Pour plus d'informations sur une API, reportez-vous au guide de programmation des API (voir la bibliographie).

Les API suivantes assurent la prise en charge des programmes de transaction (TP) écrits pour CS/AIX version 4 ou antérieure. Ces API n'existeront probablement plus dans les versions ultérieures ; il est donc recommandé de ne pas les utiliser pour créer de nouvelles applications :

- SNA générique
- LU 0
- Sous-programmes de système d'exploitation (LU de types 1, 2, 3 et 6.2).
- Sous-programmes de bibliothèque pour conversations de TP (LU de types 1, 2, 3 et 6.2).
- Sous-programmes de bibliothèque pour la gestion de réseau, utilisés pour échanger des transports de vecteurs de gestion de réseau (NMVT) dans des sessions SSCP-PU.
- Services de gestion (MS)

Pour plus d'informations sur ces API, voir le manuel *Communications Server for AIX Transaction Program Reference V4R2*.

Support client-serveur

Les ordinateurs exécutant CS/AIX peuvent être configurés de façon à communiquer via les protocoles client-serveur. Si vous utilisez les protocoles client-serveur sur un réseau, tous les ordinateurs utilisant ces protocoles pour communiquer sur ce réseau constituent un «domaine.»

Les ordinateurs exécutant CS/AIX dans une configuration client-serveur peuvent jouer les rôles suivants :

- Un serveur contient un nœud SNA et les composants de connectivité associés. Le serveur fournit la connectivité SNA aux applications sur le système local ou sur d'autres ordinateurs du domaine CS/AIX. Les serveurs doivent être des systèmes AIX.
- Un client Remote API Client ne contient pas les composants de nœud SNA, mais peut y accéder via un serveur. Un client peut accéder à un ou plusieurs serveurs en même temps et peut exécuter plusieurs applications simultanément si cela est nécessaire. Les clients peuvent exécuter AIX, Linux ou Windows. (Un ordinateur AIX peut être soit un

serveur soit un client, mais pas les deux : vous ne pouvez pas installer le serveur et le client sur le même ordinateur.)

Les serveurs et les clients communiquent par TCP/IP au sein d'un domaine CS/AIX. Ils peuvent également communiquer par HTTPS via un serveur WebSphere qui utilise les certificats de sécurité pour authentifier les connexions client. En général, HTTPS est utilisé si les clients se connectent sur un réseau public.

Dans un domaine contenant plusieurs serveurs CS/AIX, la copie principale du fichier de configuration du domaine CS/AIX se trouve sur l'un des serveurs. Ce serveur est appelé serveur maître. Vous pouvez définir les autres serveurs du domaine en tant que serveurs de secours, ou les laisser à l'état de serveurs homologues. Le fichier de configuration du domaine est copié sur les serveurs de secours, soit à leur démarrage, soit lors de la modification de la copie principale, afin que le contenu de la copie placée sur chaque serveur de secours soit à jour. Un serveur homologue récupère les données de configuration du domaine à partir du serveur maître lorsque cela est nécessaire, mais il ne peut pas jouer le rôle de serveur de secours.

En cas de défaillance du serveur maître, celui-ci est remplacé par le premier serveur de secours de la liste de serveurs définie pour le domaine. Le fichier de configuration du domaine placé sur ce serveur est utilisé comme copie principale et est copié sur les autres serveurs lorsque cela est nécessaire. Lors du redémarrage du serveur maître initial, celui-ci reçoit une copie de la configuration du domaine depuis le serveur de secours jouant temporairement le rôle de serveur maître, puis il reprend son rôle de serveur maître.

Support d'applications réparties

Sur un système CS/AIX client-serveur, les applications exécutées sur des clients Remote API Client coopèrent avec les ressources de connectivité sur les serveurs afin d'exécuter une tâche. Les applications exécutées sur d'autres ordinateurs (non CS/AIX) peuvent également coopérer avec les applications sur les ordinateurs CS/AIX afin d'effectuer le traitement réparti.

CS/AIX prend en charge des applications réparties de différents types, à savoir :

- APPC (APPC est également désigné par LU 6.2)
- Deux applications courantes de traitement réparti :
  - Customer Information Control System (CICS)
  - DATABASE 2 (DB/2)développée pour des LU 6.2 (dépendantes et indépendantes)

  CICS et DB2 (système de gestion de base de données relationnelle) sont des applications compatibles avec l'architecture SAA, mais elles peuvent être personnalisées rapidement pour n'importe quel environnement. Sur les 500 plus importantes sociétés classées par bénéfices, 90 % utilisent les applications CICS et DB2. Il s'agit de programmes de transactions puissants, qui peuvent servir des milliers de nœuds simultanément. En général, CICS et DB2 servent à accéder à des données situées dans plusieurs emplacements différents, à les mettre à jour et à les stocker dans un référentiel central.

Host Access Class Library

Host Access Class Library (Host Access API), inclus dans le support d'installation CS/AIX, permet de développer des applications Java pour

accéder aux applications 3270, 5250 ou VT sur un système hôte. Il fournit un ensemble fondamental de classes et de méthodes permettant de développer des applications indépendantes de la plateforme, qui peuvent accéder aux informations d'hôte au niveau du flot de données. Par exemple, vous pouvez développer une interface graphique (accessible à l'aide d'un navigateur Web) à une application hôte existante basée sur des caractères, de sorte que celle-ci soit plus facile à utiliser.

Fonctions de gestion de réseau évoluées

Le produit de base CS/AIX V6.3 est accompagné d'un ensemble de logiciels qui l'enrichissent de fonctions de réseau évoluées. Ces logiciels sont les suivants :

- La passerelle SNA permet de connecter des réseaux locaux à des réseaux SNA articulés autour d'un système hôte.
- Branch Extender simplifie les grands réseaux APPN en séparant les ressources des emplacements différents (par exemple, dans des filiales séparées d'une entreprise de grande taille). Cela réduit la quantité d'informations de topologie qui doivent être stockées tout en permettant un emplacement de ressources efficace.
- La suite d'applications APPC fournit des applications pour réseaux APPN.
- Enterprise Extender (EE, également appelé HPR/IP) permet le transport natif du trafic SNA via les réseaux IP.
- Le serveur TN fournit un accès hôte sur SNA aux clients TN3270 et TN3270E, désignés collectivement sous le nom de clients TN3270.
- Le Redirecteur TN assure des fonctions d'accès transparent TCP/IP aux clients TN3270, TN3270E, TN5250 et VT désignés collectivement par clients Telnet.

Passerelle SNA

Une passerelle est un dispositif transparent pour l'utilisateur qui permet de connecter des réseaux ou des systèmes informatiques différents, et compatible avec les deux environnements qu'il relie. Ainsi, les utilisateurs finals ont l'impression d'appartenir au même réseau.

Grâce à la passerelle SNA, un ordinateur CS/AIX peut jouer le rôle de passerelle reliant plusieurs ordinateurs en aval d'un réseau SNA, à une ou plusieurs unités physiques (PU), comme le montre la figure 1, à la page 8. Pour simplifier la connectivité au système hôte, et pour supprimer les liaisons excédentaires, la passerelle SNA joue le rôle de concentrateur de PU :—elle traite un groupe d'ordinateurs comme s'il s'agissait d'une seule PU (se trouvant sur le nœud de la passerelle SNA) et communique avec le système hôte par une connexion physique unique.

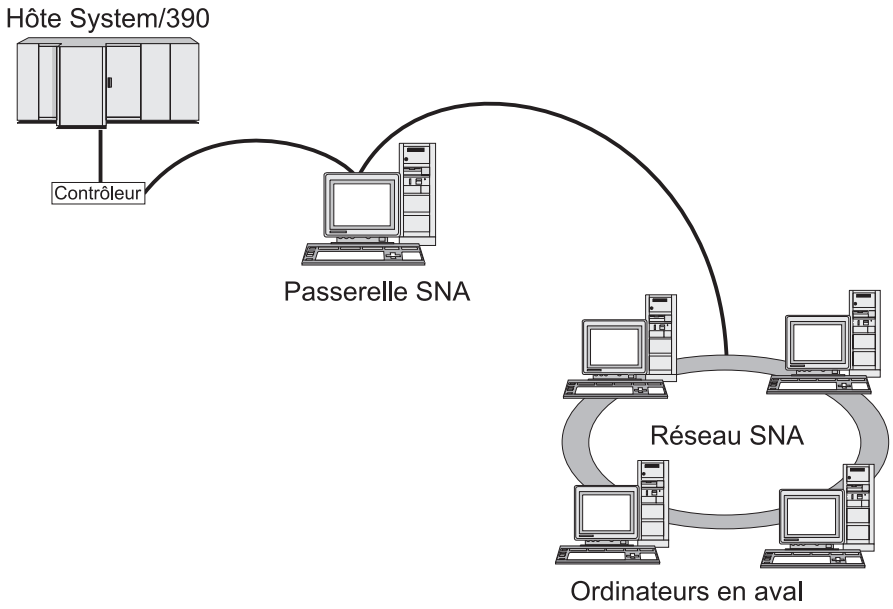

Figure 1. Passerelle SNA reliant plusieurs ordinateurs AIX aval à un ordinateur hôte

Branch Extender

Les nœuds d'un réseau APPN doivent stocker des informations de topologie (relatives à l'emplacements des autres nœuds du réseau et aux liaisons de communications entre eux) et acheminer ces informations dans le réseau lors du changement de la topologie. A mesure que la taille du réseau augmente, la quantité d'informations stockées et le trafic de réseau lié à la topologie peuvent s'agrandir et devenir difficiles à gérer.

Il est possible d'éviter ces problèmes en répartissant le réseau en sous-réseaux de sorte que chaque nœud ne stocke que les informations de topologie relatives aux nœuds de son propre sous-réseau. Cependant, il en résulte une augmentation du trafic de réseau lors de la tentative de localisation de ressources dans d'autres sous-réseaux.

La fonction Branch Extender d'APPN, illustrée dans la figure 2, à la page 9, apporte une solution à ces problèmes.

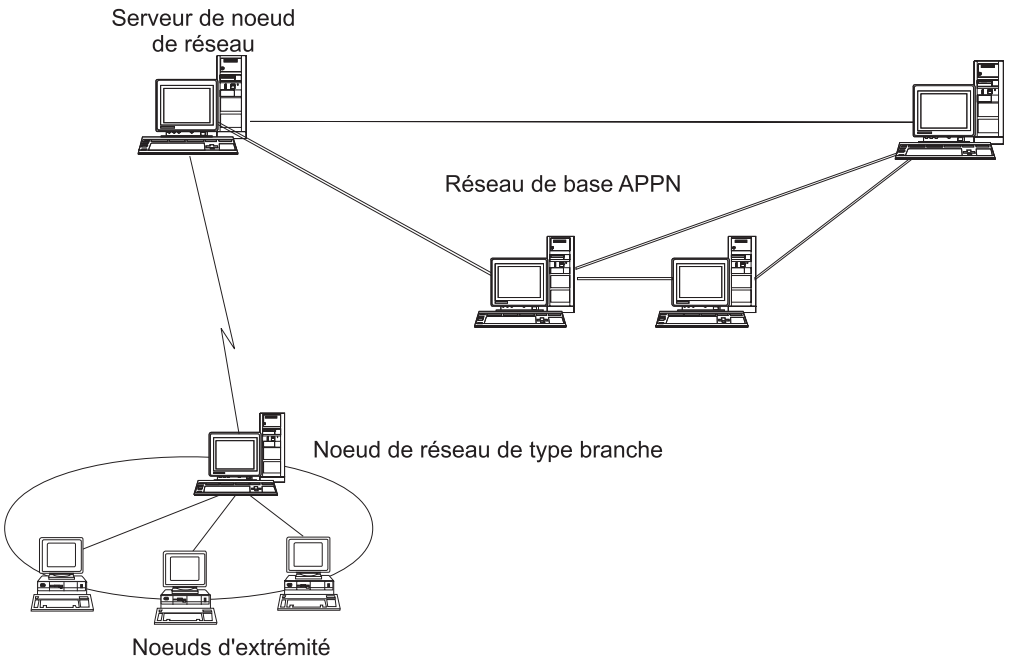

Figure 2. Branch Extender

Comme son nom l'indique, Branch Extender est conçu pour les réseaux qui peuvent être divisés en zones distinctes telles que des branches séparées d'une entreprise de grande taille. Il fonctionne grâce à la séparation des branches du réseau de base APPN principal (par exemple, le réseau du siège de l'entreprise).

Chaque branche contient un nœud d'un nouveau type appelé nœud de réseau de type branche (BrNN) qui est connecté à un nœud du réseau de base APPN principal. Le BrNN combine les fonctions d'un nœud de réseau APPN et d'un nœud d'extrémité APPN.

- Pour le réseau de base, le BrNN apparaît sous la forme d'un nœud d'extrémité connecté à son serveur de nœud de réseau (NNS) du réseau de base :
  - Les nœuds du réseau de base ne sont pas informés des nœuds de la branche, ce qui réduit la quantité d'informations de topologie qui doivent être stockées.
  - Dans la mesure où le BrNN apparaît sous la forme d'un nœud d'extrémité, il ne reçoit pas d'informations de topologie du réseau de base (celles-ci ne sont transmises qu'entre les nœuds de réseau).
  - Le BrNN enregistre toutes les sources de la branche auprès de son NNS comme si elles résidaient sur le BrNN lui-même. Cela signifie que les nœuds du réseau de base peuvent localiser des ressources de la branche sans qu'ils aient besoin d'être informés des nœuds séparés de la branche.
- Pour le réseau de type branche, le BrNN apparaît sous la forme d'un nœud de réseau jouant le rôle du NSS pour les nœuds d'extrémité de la branche. Chaque nœud de la branche considère que le reste du réseau est connecté via son NNS de la même manière que pour un NSS standard.

Suite d'applications APPC

La suite d'applications APPC est un ensemble de programmes qui témoignent des fonctions de traitement distribué des réseaux APPN et qui peuvent être utiles lors

d'une vérification de configuration et d'une résolution d'incidents. La suite d'applications APPC peut vous assister lors d'opérations fréquentes, telles que le transfert de fichiers.

La suite d'applications APPC contient les applications suivantes :

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

Ces applications sont accessibles depuis un serveur ou depuis un client AIX ou Windows.

Enterprise Extender

Enterprise Extender (également appelé HPR/IP) fournit une méthode permettant d'intégrer des applications SNA à un réseau IP.

Les applications SNA sont destinées à communiquer avec d'autres applications SNA sur des réseaux SNA, à l'aide de protocoles SNA. Installées dans un réseau TCP/IP à l'aide d'Enterprise Extender, les applications SNA peuvent néanmoins communiquer ; la fonction Enterprise Extender permet de transporter des protocoles SNA sur le réseau IP. En particulier, il fournit la fonctionnalité de routage hautes performances APPN (HPR) qui permet aux applications de tirer parti des connectivités APPN et IP.

La fonction Enterprise Extender de CS/AIX est mise en œuvre simplement comme une liaison de communication. Pour connecter deux applications SNA sur IP, définissez une liaison Enterprise Extender de la même manière que pour les autres types de liaison tels que SDLC ou Ethernet.

Serveur TN

Les programmes d'émulation 3270 qui fonctionnent sur réseau TCP/IP (plutôt que sur réseau SNA) sont appelés «programmes TN3270» (programmes d'émulation Telnet 3270).

Les programmes TN3270 peuvent également prendre en charge TN3270E (extensions standard de Telnet 3270). TN3270E prend en charge l'émulation de périphériques 3270 (terminaux et imprimantes) utilisant Telnet. Ces programmes permettent aux clients Telnet de choisir un périphérique (en précisant le nom de la LU ou celui d'un groupe de LU) et prennent en charge des fonctions variées, et en particulier la gestion des clés ATTN et SYSREQ et des réponses SNA.

Remarque : Dans le présent manuel, le terme TN3270 est utilisé pour des informations s'appliquant à la fois aux protocoles TN3270, TN3287 et TN3270E.

Le serveur TN de CS/AIX permet aux utilisateurs de TN3270 installés sur d'autres postes de travail d'accéder aux ordinateurs hôte 3270. Il permet également aux utilisateurs de TN3270 de partager une connexion hôte avec CS/AIX ou avec d'autres utilisateurs de TN3270, sans avoir recours à une liaison directe. Enfin, grâce au serveur TN, les utilisateurs de TN3270 peuvent accéder à des systèmes hôte n'exécutant pas TCP/IP.

La figure 3 illustre le rôle du serveur TN de CS/AIX.

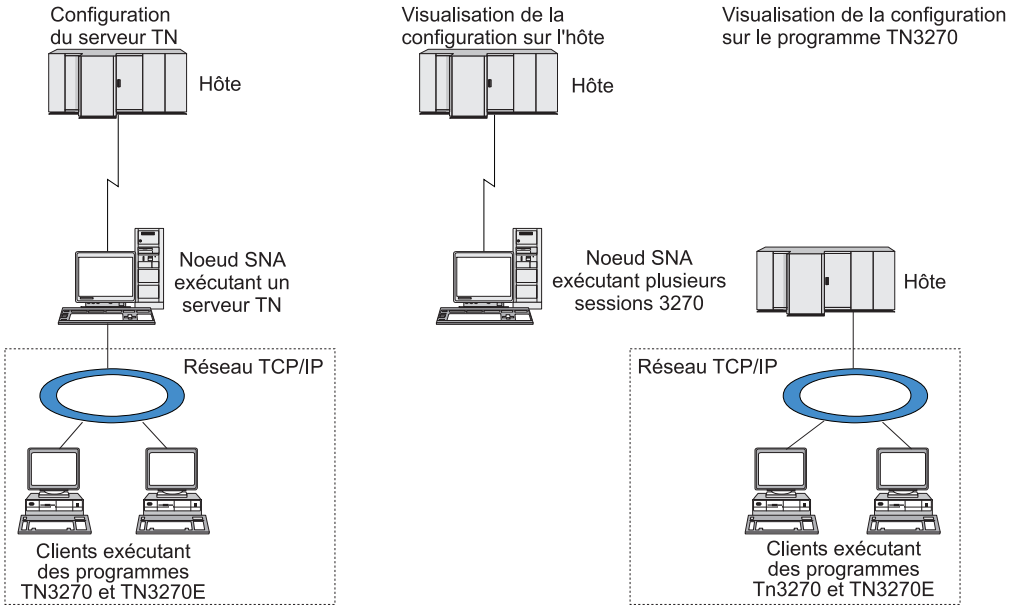

Figure 3. Serveur TN

Le serveur TN CS/AIX permet d'associer un utilisateur TN3270 et une LU 3270 CS/AIX. Toutes les données provenant de l'utilisateur TN3270 sont acheminées vers la LU. Cela signifie que la configuration de l'hôte et de l'utilisateur TN3270 est la même que s'ils étaient connectés directement ; aucun des deux éléments n'a besoin d'être informé du fait que les données sont acheminées par le serveur TN.

Le serveur TN CS/AIX prend en charge tous les programmes d'émulation client TN3270 qui mettent correctement en œuvre les protocoles définis dans les documents RFC 1123, 1576, 1646, 1647 et 2355 de l'IETF.

Fonctions de sécurité : Le serveur TN CS/AIX prend en charge le chiffrement, l'authentification serveur, l'authentification client et la connexion express, à l'aide du logiciel SSL (Secure Sockets Layer) :

- Le chiffrement de données signifie que le flux de données entre le serveur TN et l'émulateur TN3270 est au format chiffré.
- L'authentification du serveur permet à un client TN3270 de vérifier que le serveur TN auquel il est connecté est celui qui est prévu.
- L'authentification du client permet à un serveur TN de vérifier que le client TN3270 auquel il se connecte est celui qui est prévu. Le serveur TN peut également vérifier une liste de révocation sur un serveur d'annuaire externe pour s'assurer que l'autorisation du client n'a pas été révoquée.
- L'utilisation de la connexion express en association avec l'authentification client permet d'éviter aux clients TN3270 de devoir fournir l'ID utilisateur et le mot de passe pour se connecter à l'hôte. A la place, le certificat de sécurité du client permet de récupérer l'ID utilisateur et le mot de passe requis.

Ces fonctionnalités sont uniquement disponibles sur AIX 4.3.1 et versions ultérieures, et nécessitent certains logiciels supplémentaires en plus du produit CS/AIX standard. Pour plus de détails, reportez-vous à la section «Conditions requises pour l'installation», à la page 22.

Protocole SLP (Service Location Protocol) : Le serveur TN CS/AIX prend également en charge le protocole SLP (Service Location Protocol) qui fournit l'emplacement des services et des fonctions d'équilibre de charge. Si vous utilisez SLP, chaque serveur TN annonce :

- les fonctions qu'il prend en charge (dans ce cas, TN3270) ;
- sa charge en cours qui est fonction du pourcentage de ses LU hôte disponibles qui sont en cours d'utilisation mais qui peut être prise en compte pour permettre d'autres différences entre les serveurs TN.

Un client TN3270 prenant en charge SLP peut ensuite sélectionner le «meilleur» serveur auquel se connecter (le serveur le moins chargé qui fournit les fonctions qu'il requiert). Pour ce faire, il interroge les serveurs TN directement ou un agent de répertoire qui à son tour collecte des informations annoncées par les serveurs TN.

Un réseau SLP de grande taille peut être réparti en «secteurs» (généralement basés sur des départements ou des zones géographiques), de sorte que les informations relatives à un serveur TN ne soient annoncées qu'aux clients TN3270 et aux agents de répertoire qui ont le même secteur que le serveur TN. Cela vous permet de contrôler la tranche des clients TN3270 qui peuvent utiliser les services de chaque serveur TN.

Redirecteur TN

La fonction de redirection TN de CS/AIX fournit des services d'intercommunication pour les sessions 3270, 5250 ou VT sur TCP/IP. L'utilisateur Telnet communique avec CS/AIX via une connexion TCP/IP ; CS/AIX communique ensuite avec l'hôte via une autre connexion TCP/IP.

Le Redirecteur TN de CS/AIX prend en charge le chiffrement de données ainsi que l'authentification du serveur et du client, à l'aide du logiciel SSL (Secure Sockets Layer) de la même manière que le serveur TN pour 3270 : Cela permet d'utiliser le contrôle d'autorisation d'accès SSL (Secure Sockets Layer) uniquement lorsque cela est nécessaire, et non sur l'ensemble de la connexion entre l'utilisateur et l'hôte. Exemples :

- Si les postes client sont connectés à CS/AIX via un réseau local TCP/IP pour lequel aucune vérification n'est nécessaire et à un hôte éloigné qui nécessite SSL, vous pouvez utiliser SSL via la connexion TCP/IP entre CS/AIX et l'hôte. Cela signifie que la sécurité est vérifiée une fois pour tous les clients et que les clients individuels n'ont pas besoin de fournir des informations de sécurité.
- Si CS/AIX est installé sur le même site que l'hôte mais que les clients se connectent depuis des sites externes, vous pouvez utiliser SSL via les connexions client à CS/AIX sans avoir à installer le logiciel SSL sur l'hôte.

Fonctions et avantages

La gamme des fonctions et avantages de la famille CS/AIX s'étend de la simplification de la configuration à l'amélioration des performances du réseau, en passant par le perfectionnement des diagnostics de pannes.

Des produits polyvalents

CS/AIX est opérationnel dans la plupart des environnements et prend en charge pratiquement toutes les fonctions de nœuds. Dans tout type de réseau (basé sur un hôte ou APPN), il permet à un ordinateur AIX de jouer un ou plusieurs des rôles suivants :

- Nœud dépendant d'un système hôte
- Nœud homologue (pour plus d'informations sur les nœuds homologues, reportez-vous à la description des réseaux d'égal à égal dans la section «Communications Server pour AIX V6.3», à la page 1)
- Partenaire (source ou destination) dans les applications réparties
- Nœud passerelle pour l'interconnexion de réseaux SNA
- Nœud passerelle pour l'interconnexion de réseaux SNA et TCP/IP

A l'aide des API de gestion de réseau, l'ordinateur AIX peut également être configuré de façon à jouer le rôle de point d'entrée de services de gestion (MS) afin d'assurer la gestion du réseau réparti. L'ordinateur AIX peut être connecté à plusieurs réseaux locaux (LAN) et longue distance (WAN) à l'aide de l'une des liaisons prises en charge (voir leur description aux sections «Communications Server pour AIX V6.3», à la page 1 et «Conditions requises pour l'installation», à la page 22).

Fonctionnement client-serveur

La configuration client-serveur offre les avantages suivants :

- La concentration de ressources SNA sur les serveurs réduit la charge sur les clients, ce qui améliore les performances de ceux-ci et réduit la mémoire de stockage nécessaire à leur fournir les services SNA.
- Une même liaison de données peut être partagée par plusieurs utilisateurs sur différents ordinateurs : il n'est donc plus nécessaire d'avoir une connexion physique au réseau SNA sur chaque ordinateur.
- Plusieurs serveurs peuvent fournir une connectivité redondante (par exemple, plusieurs serveurs peuvent fournir l'accès au même hôte). La possibilité d'avoir plusieurs chemins d'accès à une ressource SNA permet l'équilibrage de la charge sur les différents serveurs et permet de disposer immédiatement d'une liaison ou d'un serveur de secours en cas de défaillance.
- L'utilisation de groupes de LU sur plusieurs serveurs permet à l'administrateur de configurer et d'ajouter aisément des serveurs et des utilisateurs.
- La réduction du nombre de liaisons et d'unités physiques utilisés pour la connexion à l'hôte permet de réduire la taille de la définition VTAM de l'hôte.
- Les utilitaires d'administration peuvent être utilisés pour configurer et gérer à la fois les ressources des nœuds (pour tout ordinateur du domaine) et les ressources partagées. Le support client-serveur fourni par les outils d'administration de CS/AIX permet l'administration transparente de toutes les ressources du domaine depuis n'importe quel ordinateur du domaine.
- Les applications SNA peuvent être reliées par TCP/IP et HTTPS de façon à traverser les pare-feu tout en permettant l'authentification et assurer la sécurité.

Une configuration simple

CS/AIX comprend des options et des fonctions permettant de réduire la durée de la configuration et la complexité du réseau. Exemples :

Programme d'administration Motif
Le moyen le plus simple pour définir et modifier la configuration CS/AIX est d'utiliser le programme d'administration Motif (**xsnaadmin**). Ce programme fournit une interface graphique qui vous permet de visualiser et de gérer les ressources CS/AIX. Il contribue également à simplifier la configuration, parce qu'il n'affiche que les zones dont les valeurs varient d'une installation à l'autre, et qu'il utilise les valeurs par défaut pour les autres zones.

Le programme d'administration Motif comprend des écrans d'aide offrant des informations générales sur SNA et CS/AIX, des informations de référence sur les boîtes de dialogue CS/AIX ainsi que des consignes sur l'exécution de certaines tâches.

Programme d'administration Web
CS/AIX comprend également un programme d'administration Web qui fournit des fonctions similaires au programme d'administration Motif. Il permet d'administrer CS/AIX à partir du navigateur sans qu'il soit nécessaire d'établir une session X ou telnet avec le serveur CS/AIX. Il est notamment utile lors des connexions sur des liaisons lentes ou non fiables.

Configuration dynamique des réseaux APPN
Grâce à la configuration dynamique du réseau APPN, il est plus facile de configurer un réseau ou un nœud. Par exemple, si les nœuds d'extrémité et les applications APPN enregistrent les données de configuration caractéristiques des sessions LU 6.2, la configuration des sessions devient facultative. De plus, si le point de contrôle du nœud joue le rôle de LU locale par défaut, la configuration des LU 6.2 n'est plus du tout nécessaire.

APPN prend également en charge la configuration dynamique du poste de liaison, si aucun poste de liaison n'est configuré.

Autres options d'interface pour l'administration

Le programme d'administration Motif est l'interface recommandée pour la configuration et la gestion de CS/AIX. Toutefois, CS/AIX vous laisse le choix de l'interface la mieux adaptée à votre équipement, à vos besoins et à vos goûts.

Programme d'administration par la ligne de commande
Le programme d'administration par la ligne de commande (**snaadmin**) peut être utilisé pour exécuter des commandes destinées à gérer les ressources individuelles CS/AIX. Vous pouvez entrer la commande **snaadmin** directement sur la ligne de commande AIX ou bien à partir d'un script shell.

Programme d'administration Web
Le programme d'administration Web permet d'administrer CS/AIX à partir du navigateur.

System Management Interface Tool (SMIT)
L'interface SMIT est disponible dans la version graphique de Motif pour l'environnement AIXwindows et en version texte pour les terminaux ASCII. Dans les deux versions, SMIT affiche des boîtes de dialogue destinées à faciliter la saisie des données de configuration et d'exploitation.

API NOF

Les API NOF de CS/AIX fournissent les mêmes fonctions de gestion que le programme d'administration par la ligne de commande, sous la forme d'une interface (plutôt qu'un script de commande) qui peut être utilisée dans un programme. Ainsi, il est possible de créer ses propres programmes d'application pour gérer CS/AIX.

De meilleures performances

CS/AIX améliore les performances déjà remarquables des réseaux SNA et optimise leur exploitation par l'utilisation de la classe de service. CS/AIX améliore également le débit du réseau, grâce à la compression SNA des données des sessions LU 0–3 et à différentes techniques de gestion du trafic qui contribuent à équilibrer le flux des données par rapport à la taille du réseau :

- Dans les réseaux APPN, CS/AIX prend en charge à la fois la fonction de routage hautes performances (HPR) et celle d'acheminement intermédiaire de session (ISR), et fournit des options de réseau de connexion. Si la fonction ISR est efficace sur les réseaux de petite taille, en revanche elle diminue les performances des réseaux de plus grande envergure.
- Pour les réseaux de plus grande envergure utilisant des options de connectivité de réseau local (par exemple, anneau à jeton ou Ethernet) ou Enterprise Extender, il est également possible d'utiliser l'option de réseau de connexion, afin d'améliorer l'efficacité des communications. L'option de réseau de connexion permet de créer une voie de communication directe entre les nœuds. Ainsi, le trafic évite les nœuds intermédiaires du réseau.
- Il existe un autre dispositif de contrôle du trafic, la régulation adaptative au niveau session, qui ajuste automatiquement le trafic en régulant la vitesse à laquelle les LU envoient les messages aux LU partenaires.

Options de sécurité

À l'heure où les réseaux gagnent en complexité et évoluent vers une architecture ouverte, la sécurité passe au premier plan des préoccupations. Dans les réseaux SNA mettant en œuvre CS/AIX, vous pouvez protéger vos biens en définissant différents niveaux de sécurité au cours de la configuration, et en utilisant certains types de liaisons. Exemples :

- Sur un système client/serveur, vous pouvez configurer un serveur WebSphere pour fournir aux clients Remote API Client l'accès HTTPS aux serveurs. Cela signifie que les connexions client sont authentifiées au moyen des certificats de sécurité. (Cette fonctionnalité requiert l'installation de logiciels supplémentaires en plus du produit CS/AIX standard. Pour plus de détails, reportez-vous à la section «Conditions requises pour l'installation», à la page 22.)
- Les utilisateurs de LU 6.2 peuvent définir jusqu'à trois niveaux de sécurité, à savoir : la session, la ressource et la conversation. Le premier niveau vérifie que la session implique les LU appropriées, le deuxième niveau restreint l'accès à toutes les applications associées à une LU particulière, et le troisième niveau restreint l'accès à une application particulière. La sécurité peut encore être renforcée à l'aide de programmes de chiffrement des données.
- Au niveau de la liaison, la fibre optique apporte des garanties supplémentaires de sécurité, puisqu'elle constitue un support qui, contrairement au câble électrique, est à l'abri des risques de pertes de signaux, et par conséquent, elle rend difficile l'écoute clandestine.
- Le serveur TN CS/AIX et le Redirecteur TN peuvent prendre en charge le chiffrement de données ainsi que l'authentification du serveur et du client entre le serveur CS/AIX et les clients TN3270 ou Telnet, à l'aide du logiciel SSL

(Secure Sockets Layer). (Cette fonctionnalité requiert l'installation de logiciels supplémentaires en plus du produit CS/AIX standard. Pour plus de détails, reportez-vous à la section «Conditions requises pour l'installation», à la page 22.)

Souplesse de la gestion du réseau

CS/AIX utilise deux types de programmes de gestion de réseau :

- Multiple Domain Support-Network Management Vector Transport (MDS-NMVT) peut jouer le rôle d'un programme de gestion centralisé, réparti ou hiérarchisé. Il se fonde sur une architecture point focal/point d'entrée, qui offre une grande souplesse.

  Les points focaux sont des nœuds de contrôle qui gèrent le réseau en fonction des données collectées par les points d'entrée (les applications de gestion qui résident sur tous les autres nœuds du réseau).

  – Dans un système de gestion centralisée, un point focal unique joue le rôle de point de contrôle pour la totalité du réseau.
  – Dans un système de gestion répartie, plusieurs points focaux se partagent les tâches de gestion du réseau.
  – Dans un système de gestion hiérarchisé, les points focaux sont regroupés par fonction.

  Il est possible d'adapter le programme MDS-NMVT, afin qu'il gère des réseaux articulés autour d'un système hôte, des réseaux APPN ordinaires ou des réseaux APPN très longue distance.
- Simple Network Management Protocol-Management Information Base (SNMP-MIB), qui est adapté aux réseaux APPN issus de TCP/IP, est un service de gestion répartie, qui repose sur une architecture agent-gestionnaire. Ce programme de gestion se compose de plusieurs éléments : au moins un agent SNMP, un gestionnaire et une base de données MIB, chacun résidant sur un nœud différent.

  – Un agent SNMP est un traitement exécuté sur le système en cours de gestion, et qui en contrôle l'état. Il assure la maintenance d'une base de données MIB pour ce système.
  – Le gestionnaire (une application) demande des informations MIB à l'agent, et traite ses réponses. Il peut également recevoir de l'agent des données qu'il n'a pas sollicitées (alarme SNMP). Le gestionnaire et l'agent communiquent à l'aide du protocole SNMP.

  Les gestionnaires de réseau APPN peuvent utiliser le programme SNMP-MIB pour rassembler les informations nécessaires à l'analyse du réseau et à la résolution des incidents.

  CS/AIX utilise un logiciel agent qui prend en charge la base MIB APPN. Pour plus d'informations sur la base MIB APPN, voir le manuel *Communications Server for AIX Administration Guide* et consultez la page d'accueil consacrée à l'AIW d'IBM à l'adresse suivante :
  http://www.networking.ibm.com/app/aiwhome.htm.

Fiabilité, disponibilité et facilité d'entretien

Pour vous aider à préserver la fiabilité du système d'exploitation, CS/AIX fournit un choix varié de fonctions d'affichage et d'outils de diagnostic des incidents.

- Le programme d'administration Motif fournit des outils évolués de configuration et de gestion, et notamment :

  – Mise à jour instantanée des informations de configuration
  – Informations d'état des liens, des sessions et des ressources de nœud

- Les commandes de requête et d'état fournissent des informations sur :
  - Les sessions LU-LU
  - Les sessions intermédiaires APPN
  - Les liaisons actives
  - Les bases de données sur la topologie APPN, qui stockent des informations sur les liaisons
- Les outils de diagnostic des incidents sont destinés à vous guider au cours des différentes phases de la configuration et de l'exploitation. Ces outils sont les suivants :
  - Un outil destiné à collecter les informations de diagnostic (**snagetpd**), afin que vous puissiez trouver plus facilement les informations de dépannage correspondantes
  - Des messages d'état et des messages d'erreur, destinés à vous aider à résoudre les problèmes affectant les programmes de configuration et le système d'exploitation
  - Des fichiers journaux destinés à recueillir les erreurs et incidents survenus sur le réseau, ainsi que les informations d'audit
  - Des outils de traçage destinés à rassembler et à formater des informations détaillées sur les incidents

D'autres fonctions permettent de tester la connectivité de la liaison et la communication entre les applications.

CS/AIX comprend également une API de services de gestion destinée à développer des outils permettant d'envoyer et de recevoir les alertes réseau et les données sur les incidents.

Tous ces outils de gestion et de diagnostic d'incidents sont intégrés au modèle client-serveur de CS/AIX, ce qui vous permet de gérer l'ensemble du domaine CS/AIX et de collecter les données de diagnostic à partir d'un point unique du réseau.

Intégration de réseaux, croissance et changements

Afin de prendre en charge l'intégration, le développement et les modifications du réseau, vous pouvez utiliser les API CS/AIX pour développer des applications destinées à une LU, à une plateforme ou à un système d'exploitation spécifique, pour répondre aux besoins de votre entreprise. CPI-C est une API particulièrement importante, parce qu'elle est compatible avec plusieurs plateformes et systèmes d'exploitation. Elle permet de développer des applications qui peuvent être exécutées sur n'importe quel système.

Enterprise Extender permet également l'intégration de réseaux SNA et TCP/IP.

Chapitre 2. Organisation du réseau et de Communications Server pour AIX

Ce chapitre présente les différentes étapes de l'organisation d'un réseau qui exploite CS/AIX. Il dresse également un récapitulatif des fonctions qui peuvent être configurées sur l'ordinateur AIX et fournit une estimation globale des ressources requises pour mettre en œuvre ces fonctions.

Étapes de l'organisation du réseau

Ce chapitre indique les grandes lignes à suivre pour organiser, configurer et gérer des réseaux à l'aide de divers utilitaires CS/AIX et AIX.

L'organisation d'un réseau nécessite un équilibrage des fonctions, des performances, des ressources et des coûts. Bien qu'il n'existe pas un modèle unique d'organisation de réseau, certaines lignes directrices et techniques pourront vous aider à vérifier que vous êtes sur la bonne voie. Pour organiser un réseau, procédez comme suit :

- Déterminez les fonctions futures de votre réseau (transfert de fichiers, émulation 3270, par exemple) et les résultats escomptés.
- Déterminez la configuration requise par CS/AIX pour exécuter ces fonctions.
- Évaluez les ressources nécessaires pour installer CS/AIX, aboutir aux résultats escomptés, assurer la capacité requise, prendre en charge les fonctions CS/AIX et identifier les coûts associés.

Identification des besoins fonctionnels du réseau

Pour déterminer les fonctions futures de votre réseau, vous devez vous poser les questions suivantes :

- Est-il nécessaire d'exécuter des applications APPC sur un réseau TCP/IP ?
- Le réseau doit-il être doté de la fonction APPN ?
- CS/AIX va-t-il être exécuté sur un système client-serveur ? Si oui, tous les ordinateurs vont-ils fonctionner dans le même domaine CS/AIX, ou bien est-il nécessaire de définir plusieurs domaines distincts ?
- Est-il nécessaire d'avoir plusieurs serveurs dans le domaine CS/AIX afin d'équilibrer la charge au niveau des ressources de connectivité ? Si oui, quel serveur choisir comme serveur de configuration maître ? Est-il nécessaire d'avoir plusieurs serveurs de configuration de secours ?
- La prise en charge d'une connexion HTTPS entre les clients Remote API Client et les serveurs CS/AIX est-elle nécessaire ?
- Les applications utilisateur vont-elles être exécutées sur le serveur ou bien sur les ordinateurs client AIX ?
- Le serveur va-t-il assurer les ressources de connectivité pour les applications Windows (telles que les programmes de transaction API) exécutées sur les clients Windows ?
- Chaque serveur doit-il constituer l'extrémité des sessions ou bien une passerelle de l'un des types suivants ?
  - APPN
  - LU 0

  - LU 2
  - Serveur TN ou Redirecteur TN
- Quels types de liaisons physiques le réseau utilisera-t-il ?

Les réponses à ces questions permettront de déterminer les fonctions CS/AIX requises par le réseau.

Choix de la configuration de CS/AIX

Pour déterminer le mode de fonctionnement de CS/AIX, définissez d'abord la manière dont les travaux vont circuler sur le réseau. Pour ce faire, posez-vous les questions suivantes :

- Quelles ressources (applications, par exemple) doivent être disponibles sur le réseau ?
- Combien d'utilisateurs doivent accéder aux ressources éloignées ?
- À quelle fréquence chaque ressource doit-elle être utilisée ?
- Comment les utilisateurs peuvent-ils accéder au réseau ?
- Comment les requêtes des utilisateurs seront-elles acheminées dans le réseau ?

Vous pouvez configurer CS/AIX pour prendre en charge de nombreuses fonctions, telles que :

- Nœud de réseau APPN pour la fonction d'acheminement intermédiaire de session (ISR)
- Nœud d'extrémité APPN (qui communique de manière autonome avec les nœuds adjacents, mais utilise les services d'un nœud de réseau APPN pour communiquer avec les nœuds homologues non adjacents)
- Nœud de réseau de niveau inférieur (LEN) (qui communique directement avec les nœuds adjacents ou configurés comme tels)
- Émulation de terminal de système hôte utilisant une LU 2
- Utilisation de LU 0, LU 1, LU 2, LU 3 et LU 6.2 (dépendantes et indépendantes)
- Connexion d'une passerelle SNA à l'hôte

Il est possible de configurer une ou plusieurs fonctions sur un nœud donné, si nécessaire. Par exemple, vous pouvez configurer CS/AIX pour qu'il joue le rôle d'un nœud de réseau APPN destiné à fournir des services de routage et la fonction ISR, et utiliser le même nœud comme passerelle SNA, pour l'acheminement de sessions LU dépendantes, telles que des LU 0 et des LU 2. De même, vous pouvez configurer CS/AIX de façon à exécuter le serveur TN et prendre en charge une base de données partagée, ainsi qu'une connexion LU 6.2 indépendante vers MQSeries sur l'hôte.

Identification des ressources requises pour l'installation et l'exploitation

Afin d'évaluer les ressources requises par les fonctions des produits CS/AIX, il faut se poser les questions suivantes :

- Quelles compétences sont nécessaires ?
- Quel modèle de poste de travail AIX est nécessaire ?
- Quel support de communication envisage-t-on d'utiliser ?
- Quelles sont les conditions requises pour l'installation dans la configuration choisie ?

- Quel volume d'espace mémoire et d'espace de pagination est nécessaire à l'exploitation ?
- Quel est le temps de réponse prévu, d'après le niveau de trafic envisagé ?

En répondant à ces questions, vous pourrez identifier les types de ressources utilisés par CS/AIX si celui-ci est configuré pour prendre en charge une ou plusieurs fonctions, parmi celles décrites dans la section «Identification des besoins fonctionnels du réseau», à la page 19. De plus, vous comprendrez mieux les relations qui existent entre les fonctions de CS/AIX, les ressources AIX et les ressources réseau.

L'affectation des ressources aux nœuds détermine les performances du réseau.

Personnel requis

L'installation, l'exploitation et l'adaptation de CS/AIX nécessitent l'intervention du personnel suivant :

- Des administrateurs de réseau qui organisent le réseau, ajoutent des périphériques, en assurent la maintenance et en améliorent les performances globales.
- Des administrateurs système, qui installent CS/AIX et le matériel sur lequel il fonctionne, en assurent la maintenance et configurent les systèmes en vue de leur connexion au réseau
- Des programmeurs, qui développent des applications personnalisées, telles que des programmes de transactions ou de gestion de réseau

Les administrateurs réseau et système doivent maîtriser parfaitement le matériel sur lequel fonctionne CS/AIX, ainsi que le système d'exploitation AIX. Ils doivent connaître les réseaux auxquels sont connectés les différents systèmes, et maîtriser les concepts généraux de l'architecture SNA. Ils doivent également se familiariser avec :

- l'interface Motif ou le System Management Interface Tool (SMIT) pour AIX
- TCP/IP, s'ils envisagent d'utiliser les fonctions client-serveur, le serveur TN, Enterprise Extender ou AnyNet
- Le système d'exploitation Linux, si le système CS/AIX comporte des clients Remote API Client sous Linux
- Le système d'exploitation Windows 2000, Windows XP ou Windows Server 2003, si le système CS/AIX comporte des clients Remote API Client sous Windows
- WebSphere Application Server, si le système CS/AIX comporte des clients Remote API Client reliés aux serveurs par HTTPS

Les programmeurs qui développent des applications personnalisées pour SNA doivent maîtriser le langage C (ou Java s'ils utilisent CPI-C Java), et connaître les API de CS/AIX.

Modèles IBM eServer pSeries

Communications Server pour AIX est conçu pour fonctionner sur un poste de travail AIX relié à un ou plusieurs réseaux. CS/AIX V6.3 peut fonctionner sur tout système IBM RISC System/6000 ou eServer pSeries pris en charge par AIX v5.2 ou v5.3.

Il existe plusieurs modèles de postes de travail IBM pSeries chacun ayant différentes capacités en termes de mémoire, d'espace disque, de cartes d'E-S et de vitesse UC. Ils contiennent les éléments suivants :

- Modèles Blade Center, tels que JS20. Ces modèles disposent de la capacité la plus faible en termes de mémoire, d'unités de disque et de cartes d'E-S (Ethernet, par exemple). Ils constituent d'excellents systèmes clients ou d'extrémité.
- Modèles de bureau et monté en armoire, tels que p5 520. Ces modèles disposent d'une capacité plus importante en termes de mémoire, d'unités de disque et de cartes d'E/S. Ils conviennent à des environnements à petit ou moyen serveur ou à utilisateurs multiples. Certains de ces systèmes peuvent également être partitionnés en partitions logiques (LPAR) afin de créer plusieurs instances de système d'exploitation sur le même matériel.
- Modèles montés sur châssis, tels que p5 590. Ces modèles disposent de la plus grande capacité en termes de mémoire, de disque et de carte d'E/S, et conviennent à des environnements multi-utilisateur et aux serveurs de grande taille. Ces modèles peuvent également être partitionnés en partitions logiques (LPAR).

Pour plus d'informations sur les vitesses des unités centrales des différents systèmes IBM eServer pSeries, voir http://www.ibm.com.eserver/pseries.

Supports de transport

Sous CS/AIX, il peut être nécessaire de partager le moyen de transport sous-jacent (tel que SDLC, anneau à jeton) avec les autres protocoles de communication. Par conséquent, la largeur de bande requise de la couche physique devra s'adapter à tous les protocoles et à toutes les applications qui se partageront le support de transport.

Remarque : CS/AIX peut partager les cartes en anneau à jeton, Ethernet et X.25 avec d'autres protocoles tels que TCP/IP. Vous devrez peut-être indiquer l'adresse d'un seul point d'accès au service (SAP) de chaque protocole. CS/AIX peut également partager une carte de MPQP (Multiprotocol Quad Port) , mais pas un port MPQP.

Conditions requises pour l'installation

Les fonctions attribuées à CS/AIX (voir la section «Identification des besoins fonctionnels du réseau», à la page 19) déterminent également les conditions requises pour l'installation. Cette section présente sommairement les ressources informatiques requises pour l'installation des produits CS/AIX. Pour plus de détails, consultez la documentation fournie avec chaque produit (vous trouverez la liste des manuels dans la bibliographie).

Matériel de liaison

Le matériel de liaison n'est requis que sur un serveur et non sur un client.

Pour installer un poste de travail AIX ou Power Series sur un ou plusieurs réseaux, il faut que les liaisons soient conformes au protocole de communication réseau choisi. Le matériel de liaison comprend une carte de communication installée sur l'ordinateur et le câble de connexion au réseau correspondant (un pilote de périphérique est également requis).

Remarque :

1. Les cartes de communication doivent être installées avec les câbles appropriés. Par exemple, une carte Ethernet doit être associée à un câble Ethernet pour que la liaison puisse fonctionner.
2. Si vous utilisez uniquement la liaison Enterprise Extender ou uniquement la fonction AnyNet APPC sur TCP/IP de CS/AIX, les cartes répertoriées dans la présente section ne sont pas nécessaires. Vous devez en revanche disposer d'une des cartes requises pour AIX TCP/IP.

CS/AIX prend en charge les cartes de communication correspondant aux protocoles de liaison suivants :

- Token Ring (anneau à jeton)
- Ethernet (standard ou IEEE 802.3)
- SDLC
  - IBM PCI à 2 ports
  - IBM MPQP à 4 ports

Les protocoles de liaison suivants requièrent des produits ou des fonctions supplémentaires non fournis avec CS/AIX :

- X.25 (requiert le produit AIXLink/X.25)
- ATM utilisant une interface LAN (anneau à jeton ou Ethernet) sur une carte ATM IBM AIX
- Frame Relay (relais de trames) utilisant une interface en anneau à jeton

Pour plus d'informations sur les cartes testées avec CS/AIX, voir

http://www.ibm.com/software/network/commserver/aix/sysreqs/

adapter_csaix.html

Pour toute question concernant la carte ou le matériel adaptés à vos besoins, adressez-vous au représentant commercial IBM local.

Logiciels : serveur AIX

Pour installer et utiliser CS/AIX sur votre poste de travail AIX, celui-ci doit être équipé des logiciels suivant :

- Système d'exploitation de base AIX (BOS) version 5.2 ou ultérieure.
- Support DLC (contrôle de liaison de données) approprié (non requis pour l'installation, mais nécessaire à l'utilisation de CS/AIX). Pour plus d'informations sur les DLC, reportez-vous à la section «Installation des ensembles de fichiers du DLC», à la page 33.
- Support Motif niveau 1.2 (élément du système d'exploitation de base AIX, requis pour les fonctions SSL du serveur TN CS/AIX et/ou du Redirecteur TN, ainsi que pour le programme d'administration Motif).
- Java version 1.4.2 ou ultérieure (requis pour utiliser CPI-C Java). L'environnement JRE (Java Runtime Environment) est nécessaire. Pour compiler des nouvelles classes Java à utiliser avec l'application CPI-C Java, le kit de développement SDK Java est nécessaire.

  Vous pouvez télécharger la dernière version du kit SDK Java sur le site suivant : http://www.ibm.com/developerworks/java/jdk. Java est disponible en 64 bits, mais l'API CPI-C Java requiert la machine JVM 32 bits.

  Installez le kit SDK Java à l'aide de la commande **installp**

- L'option AIX **bos.64bit** est requise si vous envisagez d'exécuter les applications à l'aide des API CS/AIX en mode 64 bits. En plus de l'installation de cette option, vous devez la configurer à l'aide de la commande **smit load64bit** pour vous assurer qu'elle est chargée avant d'exécuter des applications 64 bits. Pour compiler et connecter des applications 64 bits sur ce poste et les exécuter sur un autre poste (par exemple, si vous utilisez des postes distincts pour développer et tester des applications), l'option **bos.64bit** n'est pas requise.
- Un serveur Web prenant en charge les servlets Java (requis pour le programme d'administration Web). Le serveur IBM HTTP (IHS) v6.0.1 a été testé avec CS/AIX.

  Si vous envisagez d'utiliser un autre serveur Web ou si vous installez un de ces serveurs Web après CS/AIX, vous devez configurer des liaisons entre les répertoires CS/AIX et les répertoires du serveur Web; pour plus de détails, reportez-vous à la section «Configuration d'un serveur Web pour le programme d'administration Web», à la page 43. (Si un ou plusieurs des serveurs Web ci-dessus sont déjà installés, le processus d'installation CS/AIX configure automatiquement les liaisons requises.)
- Un navigateur Web prenant en charge Java (requis pour le programme d'administration Web). Les navigateurs Web suivants ont été testés avec CS/AIX :
  - MicrosoftInternet Explorer version 4 SP1 ou ultérieure
  - Netscape Navigator version 4.06 ou ultérieure

WebSphere Application Server (pour l'accès HTTPS)

Si vous utilisez un système client-serveur sur lequel les clients Remote API Client se connectent aux serveurs CS/AIX par HTTPS, vous devez exécuter WebSphere Application Server afin d'assurer l'accès HTTPS entre les clients et les serveurs.

CS/AIX fonctionne avec WebSphere Application Server Version 5, lequel peut être installé sur un ordinateur muni de tout système d'exploitation pris en charge par WebSphere. (Au besoin, vous pouvez l'installer sur le même ordinateur AIX que le serveur CS/AIX.) Pour plus d'informations sur son installation, consultez la documentation de WebSphere Application Server. Pour utiliser WebSphere avec CS/AIX, vous devez également installer un plug-in CS/AIX sur cet ordinateur (voir «Configuration de WebSphere Application Server», à la page 39).

Mémoire et espace disque

Pour prendre en charge l'ensemble des configurations et services disponibles, une poste de travail exécutant CS/AIX requiert 32 Mo de mémoire et 32 à 36 Mo d'espace disque (selon les fonctions facultatives installées). De plus, lors de l'installation, 2 Mo de mémoire temporaire sont requis.

Les messages et le texte d'aide sont fournis dans plusieurs versions de langues différentes. Les ensembles de fichiers doivent être installés au moins pour une langue ; vous pouvez en installer plusieurs si nécessaire. Un espace disque 2,5 à 4 Mo est requis pour chaque langue (la quantité de l'espace disque varie selon les différentes versions de langue).

Pour installer la documentation de CS/AIX sous forme de copie électronique (HTML), un espace disque supplémentaire est nécessaire. Différentes versions en langue nationale sont disponibles. Pour installer l'ensemble des manuels électroniques, un espace disque de 9 à 15 Mo est requis (en fonction des versions de langue installées).

Remarque : La mémoire et l'espace disque nécessaires au stockage et à l'exécution d'autres programmes sous licence, des applications utilisateur, des données, etc. n'est pas pris en compte ici. Pour évaluer précisément les conditions requises au niveau du système, de la mémoire et de l'espace disque, contactez votre partenaire commercial IBM ou le revendeur agréé.

Configurations évoluées

Si vous envisagez d'exécuter des applications nécessitant une configuration avancée, vous devrez prévoir des ressources supplémentaires.

En règle générale, les besoins en mémoire et en espace disque pour l'exécution de CS/AIX dépendent de nombreux facteurs, qui varient selon la fonction du poste de travail AIX et son environnement. Toutefois, si l'on admet que les LU, les liaisons actives et les sessions en cours sont les premières consommatrices de ressources informatiques, il est possible d'évaluer le volume de mémoire et d'espace disque nécessaire pour la mise en œuvre des applications les plus gourmandes en mémoire.

Pour plus d'informations sur l'utilisation, l'affectation et l'optimisation des ressources en fonction du rôle des nœuds, accédez à l'adresse http://www.ibm.com/software/network/commserver.

Mémoire et espace disque requis pour l'exploitation

Cette section présente une évaluation de la mémoire et de l'espace de stockage requis pour l'exécution de CS/AIX sur un poste de travail.

Mémoire tampon

AIX utilise des tampons (mbufs) pour permettre la communication entre les sous-systèmes de communication et les fonctions DLC d'AIX. Le pool de mémoires tampons constitue une ressource partagée qui doit être gérée au niveau du système. CS/AIX utilise ces mémoires pour envoyer et recevoir des données sur le réseau, mais seul un des sous-systèmes utilise des mémoires tampons. L'exploitation des ressources de mémoire tampon par CS/AIX risque d'altérer les performances des autres sous-systèmes, tels que TCP/IP, NFS ou DCE. Pour définir la capacité de mémoire tampon requise, demandez conseil à votre administrateur réseau.

Mémoire, espace disque et espace de pagination

CS/AIX utilise la mémoire principale — ou mémoire vive ou RAM —, l'espace disque permanent et l'espace disque de pagination (ou espace de pagination) de la manière suivante :

- Les blocs de contrôle des ressources SNA, tels que les LU, les liaisons et les sessions, consomment la mémoire principale.
- Les tampons consomment uniquement la mémoire principale.
- Les exécutables de CS/AIX, les fichiers de configuration et les publications en ligne consomment la mémoire disque permanente.
- Les programmes d'application, les sessions et autres traitements de ce type consomment l'espace disque permanent.

Les besoins en mémoire et en espace disque dépendent de divers facteurs, qui varient d'un environnement à l'autre. Les programmes de transactions (TP) et les sessions SNA sont les plus gros consommateurs de mémoire et d'espace disque.

Un programme TP utilise l'interface de programme d'application (API) SNA pour accéder au réseau. Une session est un canal logique provisoire

qui relie deux LU sur des nœuds partenaires. Les programmes de transactions utilisent ce canal pour communiquer entre eux.

La consommation de mémoire et d'espace disque dépend très largement du nombre global de sessions, du nombre de sessions allouées (conversations), de l'intensité du trafic des conversations et du nombre de TP utilisateurs actifs. Les besoins en mémoire varient surtout en fonction de l'intensité du trafic de données et de l'utilisation de tampons qui en résulte. Les besoins en espace disque dépendent des besoins en espace de pagination des TP, des sessions et autres traitements de ce type.

Pour tous les types de LU, on distingue les sessions inactives et les sessions allouées. Une session inactive est une session active mais qui n'est pas en cours d'utilisation. Une session allouée prend en charge une conversation en cours. Pour évaluer le volume total de mémoire requise, il vous faut établir une estimation moyenne de l'intensité du trafic et du nombre de sessions à allouer, à un moment donné. Vous pouvez également choisir de configurer le système de sorte qu'il traite les pics de demande. Ces estimations varient en fonction des environnements.

Si la charge de la session dépasse la capacité de la mémoire système, le coût de la pagination risque d'augmenter.

Traitements

CS/AIX nécessite au moins 20 processus AIX. Contrairement à CS/AIX V4R2 et aux versions précédentes, aucun traitement supplémentaire n'est requis en fonction du nombre de sessions. Selon le nombre de serveurs principaux et secondaires actifs, la fonction de LU 0 peut créer jusqu'à 33 traitements (sans compter les traitements nécessaires à CS/AIX).

Temps de réponse

Il est impossible d'évaluer le temps de réponse en fonction des prévisions du trafic, en raison de la variété des conditions d'exploitation du réseau qui existent. Puisque le temps de réponse ne peut être exprimé en une formule simple, il est plus facile de le calculer à partir de données expérimentales, et d'extrapoler pour le réseau concerné.

Pour vous aider dans vos estimations, les pages Web d'IBM Communications Server à l'adresse http://www.ibm.com/software/network/commserver présentent différentes configurations réseau, et montrent l'influence de facteurs tels que le modèle du poste de travail AIX et le nombre de sessions en cours sur le temps de réponse de chaque réseau.

Garantie de compatibilité inter-plateforme des configurations

Les produits SNA compatibles avec plusieurs plateformes, par exemple IBM Personal Communications ou Communications Server pour Windows, ou VTAM NCP sur un hôte, peuvent fonctionner avec CS/AIX si certaines conditions requises sont remplies.

En règle générale, l'édition en cours d'un produit de réseau SNA peut fonctionner avec CS/AIX tant qu'elle prend en charge les nœuds de PU 2.1 et au moins un des types de liaisons prises en charge par CS/AIX. Toutefois, il se peut que certaines versions très anciennes (telles que VTAM V2) ne fonctionnent pas de façon fiable. Les fonctions de chaque produit de réseau sont décrites dans les guides de l'utilisateur correspondants.

D'autres facteurs entrent en ligne de compte :

- Si vous utilisez des LU 6.2 indépendantes et que votre réseau n'est pas de type APPN, assurez-vous que les LU partenaires sont définies dans le système local.
- Puisque les valeurs par défaut définissant la taille des fenêtres de DLC et les temporisateurs varient d'un périphérique à l'autre, vérifiez que les périphériques éloignés utilisent la valeur correcte. Par exemple, si une taille de fenêtre de DLC donne de bons résultats avec un nœud Communications Server pour Windows NT elle ne conviendra pas nécessairement à un nœud 3172. Pour plus de détails sur les tailles de fenêtres, consultez les pages Web d'IBM Communications Server à l'adresse http://www.ibm.com/software/network/commserver.
- Lorsque vous travaillez dans un environnement hétérogène (protocoles TCP/IP et SNA sur le même réseau local) comprenant plusieurs segments de réseau local, assurez-vous que les périphériques d'interconnexion de réseau local peuvent acheminer simultanément des trames TCP/IP et SNA.

Conventions d'appellation

Vous pouvez utiliser les ID du réseau pour découper le réseau physique en segments logiques. De plus, si vous envisagez de vous connecter à d'autres réseaux, il est vivement recommandé d'enregistrer les ID de votre réseau, afin d'éviter tout conflit de noms de réseau.

Pour définir les noms de réseau et de LU, procédez comme suit :

Noms de réseau

Vous pouvez définir différents noms de réseau (ID réseau) pour segmenter les réseaux APPN. La segmentation permet de limiter la taille des bases de données de topologie de réseau et la fréquence des requêtes LOCATE de diffusion, au sein de chaque réseau.

Pour vérifier qu'un ID réseau est unique, l'administrateur réseau peut l'enregistrer à l'aide du registre mondial IBM. Aucun des ID réseau répertoriés dans le registre IBM ne peut être utilisé deux fois. Les normes de registre sont compatibles avec les normes d'interconnexion des systèmes ouverts (OSI), y compris les codes pays OSI, tels qu'ils ont été définis par l'Organisation internationale de normalisation (ISO). Pour plus d'informations sur l'enregistrement, reportez-vous au manuel *User's Guide for SNA Network Registry*.

Noms de LU

Vous pouvez utiliser des caractères génériques dans les noms de LU, afin de limiter la définition du système et les recherches du réseau.

Chapitre 3. Installation de CS/AIX sur des serveurs AIX

Ce chapitre explique comment installer CS/AIX sur des ordinateurs AIX. Il fournit également des instructions relatives à la mise à jour des informations de configuration du système CS/AIX.

Remarque :

1. Vous devez disposer de droits d'accès de niveau superutilisateur (root) pour installer CS/AIX.
2. Vous devez en outre ajouter un DLC (contrôle de liaison de données) pour pouvoir utiliser CS/AIX. Le DLC gère en effet la carte de communication. Pour plus d'informations, voir la description de la commande **mkdev** dans le manuel *AIX Commands Reference*, ou bien utilisez l'option **Communications** du menu **Unités** de l'outil SMIT (System Management Interface Tool). (Pour plus d'informations, consultez le manuel *AIX Communications Programming Concepts*.)

Octroi de licence CS/AIX et conditionnement

La présente section explique comment le produit CS/AIX est accordé sous licence et conditionné.

Principe de l'octroi de licences CS/AIX

La présente section décrit en détail les principes d'octroi de licence. Le document *Informations sur la licence* de CS/AIX contient l'ensemble des termes et conditions applicables au produit. En outre, des exemples de scénarios permettent de clarifier les principes d'octroi de licence de la plupart des différents types de connectivité et de fonctionnalité fournis par CS/AIX. Pour de plus amples informations, accédez à l'adresse http://www.ibm.com/software/network/commserver.

CS/AIX comprend plusieurs composants décrits ci-dessous.

Logiciel sous licence Communications Server pour AIX

Une licence logiciel CS/AIX distincte est requise pour chaque ordinateur ou nœud SP comportant un ou plusieurs composants inclus.

L'octroi de licence pour CS/AIX comporte la licence du programme (serveur) et les licences utilisateur.

- Un utilisateur est défini comme une personne. Vous devez acquérir une autorisation pour chaque utilisateur concurrent qui va accéder et utiliser CS/AIX directement ou indirectement. Exemple d'utilisation indirecte : si un programme de multiplexage ou un serveur d'applications (par exemple, CICS, DB2, WebSphere, ou votre propre application d'entreprise) est relié à CS/AIX afin de fournir l'accès à plusieurs utilisateurs simultanément, une licence utilisateur est requise pour chacun de ces utilisateurs.
- En outre, pour les programmes d'application qui ne sont pas associés à des utilisateurs réels, une autorisation utilisateur est requise pour chaque connexion active en amont ou en aval établie vers le nœud CS/AIX. Dans un environnement APPN, une connexion est une liaison active à un nœud adjacent.

Activation de CS/AIX à l'aide d'une licence nodelock

L'activation et l'invalidation de CS/AIX s'effectuent par l'octroi de licences d'utilisation mettant en œuvre un mécanisme de verrouillage au niveau du nœud (licences dites nodelock). Les licences de ce type sont gérées au niveau d'un nœud spécifique et non par un serveur de licences faisant partie du réseau.

Une licence nodelock peut être permanente ou provisoire. Dans ce dernier cas, CS/AIX est activé et utilisable pendant une durée limitée (par exemple, dans le cas d'une offre d'essai ou à des fins de démonstration). L'acquisition du produit CS/AIX accorde la licence d'utilisation nodelock permanente, installée automatiquement dans le fichier de licence **nodelock** du système, en même temps que le reste du produit.

Si CS/AIX est installé à partir du support de démonstration, par exemple CD Showcase, sa clé de licence sera temporaire. Pour activer pleinement le produit, vous devez acquérir une licence CS/AIX en vous adressant à votre représentant IBM. Pour passer d'une licence d'essai à une licence permanente, installez simplement la clé correspondante à partir du support d'installation de CS/AIX. Il n'est donc pas nécessaire de réinstaller le produit.

Pour extraire la clé du CD d'installation de CS/AIX, suivez la procédure ci-après :

1. Saisissez la commande **smit bffcreate** et utilisez la boîte de dialogue SMIT qui apparaît pour extraire le composant **sna.rte** du support d'installation. Notez le nom du fichier créé.
2. Utilisez les commandes suivantes pour extraire le fichier clé de l'image LPP **sna.rte** :

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

3. Utilisez la commande suivante pour copier la clé dans le fichier **/var/ifor/nodelock**. Veillez à bien utiliser l'opérateur de "concaténation" >> pour concaténer la clé dans le fichier (n'utilisez **pas** l'opérateur > qui écraserait toutes les clés précédentes).

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

Contrôle de l'utilisation des ressources CS/AIX

Les licences CS/AIX étant fonction des utilisateurs concurrents du produit, il est difficile pour CS/AIX de mesurer ou signaler réellement le nombre d'utilisateurs de la plupart des différents types de ressources de communications qu'il fournit. Cependant, il peut être utile de contrôler l'utilisation des différents types de ressources sous la forme d'un indicateur des changements d'utilisation globale ou maximale qui risquent de se produire. Ces informations peuvent être utiles lorsque vous traitez les exemples de scénarios présentés à l'adresse http://www.ibm.com/software/network/commserver, afin de mieux comprendre le nombre de licences d'utilisateurs CS/AIX concurrents qui sont requises.

CS/AIX contrôle l'utilisation des types de ressources de communications suivants qu'il fournit :

- Applications utilisant les API APPC ou CPI-C (par exemple, DB2 ou WebSphere)
- Applications utilisant l'API LUA (généralement développées par l'utilisateur)
- Postes de liaison actifs (vers un hôte, un nœud LEN ou APPN adjacent, Enterprise Extender, ou un client passerelle SNA ou DLUR en aval)

- Les sessions Telnet qui se connectent au composant serveur TN3270E de CS/AIX, qu'elles utilisent ou non le chiffrement de données SSL ou l'authentification client-serveur
- Les sessions Telnet qui se connectent au composant Redirecteur TN de CS/AIX (par exemple des sessions VT réacheminées) afin d'utiliser le chiffrement de données SSL ou l'authentification client-serveur
- Sessions de données SNA actives (sessions actives vers des LU de type 1, 2 ou 3. Sessions LU6.2 actives, à l'exclusion de celles utilisées pour le contrôle du réseau.)

L'utilisation de chaque ressource est mesurée à des intervalles périodiques et l'utilisation de CS/AIX mesurée à ce stade est enregistrée dans un «fichier journal d'utilisation» qui est ensuite disponible à des fins d'analyse et d'utilisation. Lors de chaque échantillonnage, l'utilisation en cours de la ressource et l'utilisation maximale (depuis le dernier redémarrage du système) sont enregistrées.

Pour plus d'informations sur la consignation, voir le manuel *Communications Server for AIX Diagnostics Guide*.

Composition du programme sous licence CS/AIX

Le programme sous licence (LPP) CS/AIX est constitué de plusieurs modules (images installables), chacun contenant un ou plusieurs ensembles de fichiers. Un ensemble de fichiers est la plus petite unité installable du produit. AIX conserve des informations relatives à la version et au niveau de chaque ensemble de fichiers (voir la description de la commande AIX **lslpp** dans «Affichage des caractéristiques d'installation des produits», à la page 34). Un programme sous licence peut également contenir des fichiers mis à jour.

Remarque : Pour plus d'informations sur l'espace requis, reportez-vous à la section «Conditions requises pour l'installation», à la page 22.

Les ensembles de fichiers suivants sont requis pour l'installation de CS/AIX :

composant sna

sna.rte Programme de base de CS/AIX.

composant sna.msg.*Langue*

Catalogue des messages de CS/AIX. Il contient les fichiers de messages du produit et les boîtes de dialogue de l'aide dans la langue choisie pour l'environnement d'exécution. L'ensemble de fichiers suivant est requis :

sna.msg.*Langue***.rte**

Fichiers de messages et d'aide en ligne des fonctions CS/AIX de base. *Langue* indique la langue d'affichage des messages. Choisissez un des identificateurs de langue suivants :

Identificateur	Langue
en_US	Anglais (États-Unis)
Ja_JP	Japonais (PC)
de_DE	Allemand
es_ES	Espagnol
fr_FR	Français
ko_KR	Coréen
pt_BR	Portugais
zh_CN	Chinois (simplifié)

Identificateur	Langue
zh_TW	Chinois (traditionnel)

Si vous installez le support de plusieurs langues pour un produit, veillez à installer d'abord celui de la langue principale. Ainsi, pour installer le français comme langue principale, indiquez :

sna.msg.fr_FR.rte

L'installation préalable de **sna.rte** est requise pour **sna.msg.***Langue***.rte**.

Ensembles de fichiers du support SSL
Les ensembles de fichiers suivants sont inclus pour la prise en charge de SSL (Secure Sockets Layer) avec le serveur TN ou du Redirecteur TN :

gskta.rte
AIX Certificate and SSL Base Runtime.

Composants compris dans CS/AIX

Les composants suivants font partie de CS/AIX. Leur installation est facultative.

sna.xsna
Programme d'administration Motif.

sna.xsna exige l'installation préalable de **sna.rte**, **X11.base.rte** et **X11.Dt.helprun**.

sna.wa
Programme d'administration Web.

sna.wa exige l'installation préalable de **sna.rte**.

sna.lu0
Fonctions LU 0.

sna.lu0 exige l'installation préalable de **sna.rte**.

sna.docs.*Langue***.data**
Documentation en ligne. *Langue* indique la langue dans laquelle les documents doivent s'afficher (par exemple, `fr_FR` pour le français).

sna.man.fr_FR.rte.data, sna.man.fr_FR.xsna.data, sna.man.fr_FR.lu0.data
Pages d'aide d'AIX sur les commandes CS/AIX.

sna.msg.*Langue***.snapi, sna.msg.***Langue***.xsna, sna.msg.***Langue***.wa**
Fichiers de messages du produit et boîtes de dialogue de l'aide pour les composants CS/AIX facultatifs. Vous devez installer ces ensembles de fichiers uniquement si vous installez les ensembles de fichiers correspondants des composants facultatifs. *Langue* indique la langue dans laquelle les messages doivent s'afficher (par exemple, `fr_FR` pour le français).

sna.snapi
SNA Application Development Toolkit (SNAPI).

sna.snapi exige l'installation préalable de **sna.rte**.

sna.rte64
Ensembles de fichiers destinés au support d'API 64 bits.

sna.rte64 exige l'installation préalable de **sna.rte**.

sna.dlcmpc
SNA Channel Data Link.

sna.ecl
Host Access Class Library.

Communications.Bnd
Définition du progiciel à utiliser pour l'installation rapide (Easy-Install) selon la procédure décrite dans la section «Méthodes d'installation», à la page 36.

Préparation à l'installation de CS/AIX

Pour installer CS/AIX, vous devez exécuter AIX 5.2 ou une version ultérieure. Procédez comme suit :

- Installez et configurez tous les DLC requis pour communiquer à travers le réseau, comme indiqué à la section «Installation des ensembles de fichiers du DLC». (Vous devez installer et configurer les DLC avant d'utiliser CS/AIX, mais vous pouvez les installer après CS/AIX.)
- Si des versions antérieures de CS/AIX sont installées sur votre système, vous pouvez consulter l'historique d'installation du produit, comme indiqué à la section «Affichage des caractéristiques d'installation des produits», à la page 34. Vous pouvez également revoir le processus de migration, comme décrit à la section «Migration de CS/AIX V4R2 ou version antérieure vers CS/AIX V6.3», à la page 34.
- Si vous voulez utiliser le programme d'administration Web et que vous n'avez pas encore installé un serveur Web approprié, installez-le à présent. Les serveurs Web pris en charge par CS/AIX sont répertoriés dans la section «Conditions requises pour l'installation», à la page 22. Suivez les instructions d'installation fournies avec le logiciel de serveur Web.
- Pour un traitement correct des boîtes de dialogue et des messages du produit, assurez-vous que la variable d'environnement `LANG` est bien configurée, comme indiqué à la section «Modification de la variable d'environnement relative à la langue», à la page 34.

Installation des ensembles de fichiers du DLC

CS/AIX requiert au moins un ensemble de fichiers de contrôle de liaison de données (DLC) AIX pour communiquer sur le réseau. Les ensembles de fichiers de DLC sont les suivants :

- **bos.dlc.token** pour les postes de liaison en anneau à jeton (Token ring)
- **bos.dlc.ether** pour les postes de liaison Ethernet standard
- **bos.dlc.8023** pour les postes de liaison Ethernet 802.3
- **bos.dlc.qllc** pour les postes de liaison X.25
- **bos.dlc.sdlc** pour les postes de liaison SDLC

Tous les ensembles de fichiers **bos.dlc** sont fournis avec le package **bos.dlc.usr** du système d'exploitation AIX de base. Les DLC doivent être installés séparément.

Remarque : Pour plus d'informations sur le contrôle de liaison de données AIX, voir le manuel *AIX Communications Programming Concepts*.

Affichage des caractéristiques d'installation des produits

Pour afficher l'historique d'installation de CS/AIX (et de certains produits associés) entrez l'une des commandes suivantes :

Entrez :	Pour le produit :
lslpp -h sna.rte	Communications Server pour AIX

Pour afficher les PTF (modifications provisoires du logiciel) qui ont été appliquées aux produits depuis leur installation, entrez la commande avec l'option **-ha** à la place de l'option **-h**.

Migration de CS/AIX V4R2 ou version antérieure vers CS/AIX V6.3

Dans le cas d'une mise à niveau de CS/AIX V4R2 (ou de l'un des produits antérieurs, SNA Server pour AIX ou SNA Server/6000), vous pouvez faire migrer les informations de configuration. Aucune migration n'est requise si la mise à niveau est effectuée à partir de V5, V6 ou V6.1, car CS/AIX V6.3 peut utiliser les informations de configuration existantes sans modification.

Lors de l'installation de CS/AIX V6.3, l'utilitaire d'installation sauvegarde automatiquement les anciens fichiers de configuration dans le répertoire **/etc/sna**. Vous pouvez ensuite exécuter la commande **snamig** pour convertir vos anciens profils de configuration au format de fichier texte utilisé par CS/AIX version 6.3. Après avoir migré les informations de configuration, vous pouvez exécuter la commande **postsnamig** pour supprimer les anciennes bases de données ODM et les fichiers de configuration de niveau antérieur.

Le processus de migration est décrit en détail dans le manuel *Communications Server for AIX Migration Guide*.

Avant d'installer la nouvelle version, arrêtez CS/AIX et la fonction LU 0 et toutes les applications qui utilisent CS/AIX :

1. Si la fonction LU 0 s'exécute en arrière-plan, recourez à la commande interactive **X** pour désactiver les serveurs LU 0. Entrez alors la commande suivante :

   lu0sndmsg *x*
2. Si CS/AIX est utilisé par une application, cette dernière doit être arrêtée. Si nécessaire, reportez-vous à la documentation des applications.
3. Si CS/AIX est actif, utilisez la commande **sna** pour le désactiver :

   sna stop

Modification de la variable d'environnement relative à la langue

Lorsque vous utilisez CS/AIX, vérifiez que la valeur de la variable `LANG` n'est pas `C`.

Pour afficher la valeur de la variable `LANG` utilisée ou la modifier, procédez comme suit :

1. Dans le menu SMIT principal, sélectionnez **Environnements système**.
2. Dans le menu SMIT suivant, sélectionnez **Gestion des langues**.

3. Dans le menu SMIT suivant, sélectionnez **Modif./Aff. environnement de la langue principale**.
4. Dans le menu SMIT suivant, sélectionnez **Choix des conventions, de la langue et du clavier**.
5. Sélectionnez la langue voulue. Par exemple, si vous utilisez des messages en français, sélectionnez `fr_FR`.

Installation du programme sous licence CS/AIX

Après avoir installé les logiciels prérequis, vous pouvez installer CS/AIX. Procédez comme suit :

1. Connectez-vous avec les droits d'accès "root".
2. Installez et configurez le contrôle de liaison de données (DLC) AIX correspondant à la carte de communication sélectionnée. Pour configurer le DLC, utilisez la commande **mkdev** (décrite dans le manuel *AIX Commands Reference*) ou l'option **Communications** du menu **Unités** de l'outil SMIT (décrite dans le manuel *AIX Communications Programming Concepts*).
3. Installez CS/AIX selon la procédure décrite dans la section «Méthodes d'installation», à la page 36. Sélectionnez les fonctions que vous voulez installer (y compris les ensembles de fichiers de messages appropriés) ou sélectionnez l'option `tous` pour installer CS/AIX avec toutes les fonctions disponibles.

   Si vous sélectionnez une fonction et choisissez `oui` dans la zone *Installation automatique des logiciels requis*, le système installe également **sna.rte** (programme de base de CS/AIX).
4. Dans le cas d'une mise à niveau d'une version antérieure de CS/AIX (ou de l'un des produits antérieurs, SNA Server pour AIX ou SNA Server/6000), vous pouvez faire migrer les informations de configuration (voir «Migration de CS/AIX V4R2 ou version antérieure vers CS/AIX V6.3», à la page 34 ou consultez le manuel *Communications Server for AIX Migration Guide*).
5. Si vous avez installé le logiciel AIX Certificate and SSL Base Runtime afin d'utiliser le serveur TN ou le redirecteur TN avec la fonction SSL, vous devez configurer le logiciel SSL après l'installation de CS/AIX. Pour plus de détails, reportez-vous à la section «Configuration de SSL aux fins d'utilisation avec le serveur TN ou le Redirecteur TN», à la page 42.
6. Personnalisez les informations de configuration CS/AIX selon vos besoins (voir Chapitre 9, «Configuration et utilisation de CS/AIX», à la page 83 ou consultez le manuel *Communications Server for AIX Administration Guide*).

   L'utilitaire d'installation lance automatiquement CS/AIX en fin d'installation.

Remarque :

1. L'installation de CS/AIX reconfigure automatiquement les pilotes de périphérique SNA sur le nœud local. Si CS/AIX v6.1 est déjà installé sur AIX 5.3, lorsque vous effectuez la mise à niveau V6.3, vous devez réamorcer le système après l'installation de CS/AIX afin de pouvoir lancer le nœud SNA. Dans les autres cas, il n'est pas nécessaire de relancer, réamorcer ou reconfigurer le noyau du système d'exploitation avant de démarrer CS/AIX.
2. Vous pouvez installer les cartes après installation de CS/AIX. Il n'est pas nécessaire de réinstaller CS/AIX après l'ajout d'une carte ; mais il est impossible d'utiliser cette carte avant d'avoir installé le DLC approprié.

Méthodes d'installation

Vous pouvez installer le programme sous licence CS/AIX en utilisant l'une des méthodes ci-dessous :

- Installation rapide
- Installation sur le système local
- Installation via le réseau (si le nœud local est un serveur de réseau).

Installation rapide de CS/AIX

Vous pouvez installer les logiciels plus facilement grâce aux progiciels. Il s'agit de listes de produits logiciels adaptés à un usage particulier. Les sections suivantes indiquent comment installer CS/AIX à l'aide de cette fonction. La fonction d'installation rapide peut être exécutée sur la console système ou à distance, sous X-Windows ou à partir d'un terminal ASCII.

Installez CS/AIX sur le nœud local, selon les instructions des sections «Installation rapide à l'aide de SMIT» ou «Installation rapide à l'aide de Common Desktop Environment».

Installation rapide à l'aide de SMIT :

1. Connectez-vous avec les droits d'accès ″root″.
2. Entrez la commande suivante :
   - **smit install_bundle**
3. Appuyez sur PF4 ou cliquez sur le bouton Liste de l'interface Motif, pour afficher la liste des unités et répertoires d'installation.
4. Sélectionnez `Media-defined` et appuyez sur **Entrée**.
5. Sélectionnez l'unité d'entrée voulue et appuyez sur **Entrée**.

L'utilitaire d'installation lance automatiquement CS/AIX en fin d'installation.

Installation rapide à l'aide de Common Desktop Environment :

1. À partir du Tableau de bord, ouvrez le Gestionnaire d'applications.
2. Ouvrez le dossier **Administration_système**.
3. Ouvrez **Installation rapide**.
4. Sélectionnez l'unité d'entrée.
5. Sélectionnez `Media-defined`.
6. Cliquez sur **Installation/Mise à jour**.

L'utilitaire d'installation lance automatiquement CS/AIX en fin d'installation.

Installation manuelle sur le nœud local

Installez CS/AIX sur le système local, selon les instructions des sections «Installation manuelle à l'aide de SMIT» ou «Installation manuelle à l'aide de Common Desktop Environment», à la page 38.

Installation manuelle à l'aide de SMIT :

1. Insérez le support d'installation dans l'unité appropriée du poste de travail AIX.
2. Connectez-vous avec les droits d'accès ″root″.
3. Assurez-vous que la variable d'environnement `LANG` de votre système n'est pas configurée avec la valeur `C`. Si vous optez pour les messages en français, donnez à la variable `LANG` la valeur `fr_FR`. Pour plus d'informations sur

l'affichage ou la modification de la variable d'environnement LANG, reportez-vous à la section «Modification de la variable d'environnement relative à la langue», à la page 34.

4. Entrez la commande suivante sur la ligne de commande AIX :

   smit install

   Cette commande appelle le programme SMIT qui offre un environnement fondé sur les menus, lors de l'installation.

5. Sélectionnez les options suivantes, dans les menus d'installation SMIT, pour effectuer une installation standard des logiciels sélectionnables avec mises à jour :

   a. **Installation et mise à jour de logiciel**

   b. **Installation/Mise à jour logiciels (installation personnalisée)**

   c. **Installation/Mise à jour de tous les logiciels disponibles**

   Cette séquence de sélection de menus est comparable à la commande d'accès rapide suivante :

   smit install_selectable_all

6. Dans la boîte de dialogue qui apparaît, sélectionnez le nom de l'unité du support d'installation en tant qu'unité source pour la procédure d'installation. (Pour obtenir la liste des noms d'unité, utilisez la touche **PF4** de l'interface ASCII pour SMIT ou le bouton **Liste** de l'interface Motif.)

7. Sélectionnez **sna.rte**, le programme de base CS/AIX, **sna.msg.***Langue***.rte** (catalogue de messages de CS/AIX), ainsi que toutes fonctions et mises à jour supplémentaires du programme sous licence (y compris tout autre ensemble de fichiers de messages applicable). Pour installer toutes les fonctions du support d'installation, sélectionnez l'option all (tous).

   L'utilitaire d'installation affiche des messages d'état à mesure que l'installation de chaque élément aboutit.

8. Pour installer le logiciel AIX Certificate and SSL Base Runtime afin d'utiliser le serveur TN Server ou le redirecteur TN avec la fonction SSL, sélectionnez également l'ensemble de fichiers AIX Certificate and SSL Base Runtime.

   L'utilitaire d'installation affiche des messages d'état à mesure que l'installation de chaque élément aboutit.

   Si vous avez installé ce logiciel, vous devez configurer le logiciel SSL après avoir installé CS/AIX. Pour plus de détails, reportez-vous à la section «Configuration de SSL aux fins d'utilisation avec le serveur TN ou le Redirecteur TN», à la page 42.

9. Personnalisez les informations de configuration CS/AIX (voir Chapitre 9, «Configuration et utilisation de CS/AIX», à la page 83 ou consultez le manuel *Communications Server for AIX Administration Guide*).

L'utilitaire d'installation lance automatiquement CS/AIX en fin d'installation.

Remarque :

1. L'installation de CS/AIX reconfigure automatiquement les pilotes de périphérique SNA sur le nœud local. Si CS/AIX v6.1 est déjà installé sur AIX 5.3, lorsque vous effectuez la mise à niveau V6.3, vous devez réamorcer le système après l'installation de CS/AIX afin de pouvoir lancer le nœud SNA. Dans les autres cas, il n'est pas nécessaire de relancer, réamorcer ou reconfigurer le noyau du système d'exploitation avant de démarrer CS/AIX.

2. Pour plus d'informations sur l'octroi de licences utilisateur pour CS/AIX, reportez-vous à la section «Principe de l'octroi de licences CS/AIX», à la page 29.

Installation manuelle à l'aide de Common Desktop Environment :

1. Insérez le support d'installation dans l'unité appropriée du poste de travail AIX.
2. Connectez-vous avec les droits d'accès "root".
3. Assurez-vous que la variable d'environnement `LANG` de votre système n'est pas configurée avec la valeur `C`. Si vous optez pour les messages en français, donnez à la variable `LANG` la valeur `fr_FR`. Pour plus d'informations sur l'affichage ou la modification de la variable d'environnement `LANG`, reportez-vous à la section «Modification de la variable d'environnement relative à la langue», à la page 34.
4. À partir du Tableau de bord, ouvrez le Gestionnaire d'applications.
5. Ouvrez le dossier **Administration_système**.
6. Ouvrez le dossier **Gestionnaire d'installation**.
7. Sélectionnez l'unité d'entrée.
8. Sélectionnez tous les objets affichés pour installer tous les éléments sur le support ou agrandissez et sélectionnez des objets particuliers pour personnaliser les options de Communications Server pour AIX à installer.
9. Cliquez sur l'icône **Installation** pour lancer l'installation.
10. Personnalisez les informations de configuration CS/AIX (voir Chapitre 9, «Configuration et utilisation de CS/AIX», à la page 83 ou consultez le manuel *Communications Server for AIX Administration Guide*).

L'utilitaire d'installation lance automatiquement CS/AIX en fin d'installation.

Remarque :

1. L'installation de CS/AIX reconfigure automatiquement les pilotes de périphérique SNA sur le nœud local. Si CS/AIX v6.1 est déjà installé sur AIX 5.3, lorsque vous effectuez la mise à niveau V6.3, vous devez réamorcer le système après l'installation de CS/AIX afin de pouvoir lancer le nœud SNA. Dans les autres cas, il n'est pas nécessaire de relancer, réamorcer ou reconfigurer le noyau du système d'exploitation avant de démarrer CS/AIX.
2. Pour plus d'informations sur l'octroi de licences utilisateur pour CS/AIX, reportez-vous à la section «Principe de l'octroi de licences CS/AIX», à la page 29.

Installation via un réseau à l'aide de la fonction NIM (Network Installation Management)

Utilisez cette procédure pour installer CS/AIX via un réseau :

1. Pour plus d'informations sur la configuration du serveur NIM (Network Installation Management) et le téléchargement des fichiers vers le client, consultez le manuel *AIX Version 5.3 Installation Guide and Reference*.
2. Assurez-vous que la variable d'environnement `LANG` de votre système n'est pas configurée avec la valeur `C`. Si vous optez pour les messages en français, donnez à la variable `LANG` la valeur `fr_FR`. Pour plus d'informations sur l'affichage ou la modification de la variable d'environnement `LANG`, reportez-vous à la section «Modification de la variable d'environnement relative à la langue», à la page 34.

3. Entrez la commande suivante sur la ligne de commande AIX :

   smit nim

   Cette commande appelle le programme SMIT qui offre un environnement fondé sur les menus, lors de l'installation.
4. Suivez les instructions et répondez aux invites dans les menus SMIT consacrés à l'installation sur le réseau. Sélectionnez les fichiers contenant **sna.rte** et les éventuels éléments et mises à jour supplémentaires pour le programme sous licence. L'utilitaire d'installation affiche des messages d'état à mesure que l'installation de chaque élément aboutit.

Remarque :

1. Le catalogue de messages CS/AIX, **sna.msg.***Langue***.rte** , est automatiquement installé avec CS/AIX si l'option *Inclusion des ensembles de fichiers de langue correspondante ?* contient la réponse `oui` (choix par défaut).
2. L'installation de CS/AIX reconfigure automatiquement les pilotes de périphérique SNA sur le nœud local. Si CS/AIX v6.1 est déjà installé sur AIX 5.3, lorsque vous effectuez la mise à niveau V6.3, vous devez réamorcer le système après l'installation de CS/AIX afin de pouvoir lancer le nœud SNA. Dans les autres cas, il n'est pas nécessaire de relancer, réamorcer ou reconfigurer le noyau du système d'exploitation avant de démarrer CS/AIX.
3. Pour plus d'informations sur l'octroi de licences utilisateur pour CS/AIX, reportez-vous à la section «Principe de l'octroi de licences CS/AIX», à la page 29.

Configuration de WebSphere Application Server

Si vous utilisez un système client-serveur sur lequel les clients Remote API Client se connectent aux serveurs par HTTPS, vous devez disposer d'un ordinateur exécutant WebSphere Application Server pour assurer l'accès HTTPS entre les clients et les serveurs (voir «Conditions requises pour l'installation», à la page 22).

Cette section explique comment configurer WebSphere pour l'utiliser avec CS/AIX :

- Configuration d'un certificat sécurisé destiné aux clients sur le serveur WebSphere
- Configuration de WebSphere Application Server pour l'utiliser avec CS/AIX
- Installation du fichier de configuration du serveur sur le serveur WebSphere

Vous devez également configurer le certificat de sécurité du client et le fichier de données réseau du client sur chaque client Remote API Client pour accéder à WebSphere Application Server. Pour plus d'informations, voir la section relative à l'installation du type de client approprié.

Configuration du certificat sécurisé de WebSphere Application Server

Pour obtenir des instructions sur la configuration d'un certificat sécurisé sur le serveur, consultez la documentation de WebSphere Application Server. Il s'agit du certificat du serveur qui sera présenté à un client Remote API Client lors du processus d'authentification lors de la tentative de connexion par HTTPS.

Il est recommandé de configurer WebSphere afin qu'il applique l'authentification du client. Pour plus d'informations, consultez la documentation de WebSphere Application Server. Cela signifie que WebSphere va demander des certificats de sécurité aux clients Remote API Client lors du processus d'authentification, et acceptera une connexion entrante d'un client Remote API Client uniquement lorsqu'il pourra vérifier l'authenticité du certificat de celui-ci.

Configuration de WebSphere Application Server

Pour configurer WebSphere Application Server de façon à l'utiliser avec CS/AIX, procédez comme suit. Pour plus d'informations, consultez la documentation de WebSphere Application Server.

1. Copiez (ou récupérer par FTP) les fichiers **snahttpsrv.ear** et **snahttpsrv.cfg** qui se trouvent dans le répertoire **ibm-commserver-https** du CD d'installation de Remote API Client vers un répertoire de l'ordinateur où est exécutée la console d'administration WebSphere, ou bien dans un répertoire réseau accessible depuis cet ordinateur.

   Si la console d'administration est exécutée sous Windows, la copie des fichiers n'est pas nécessaire, car vous pouvez accéder à ces fichiers directement sur le CD. Insérez le CD d'installation de Remote API Client dans l'unité de CD de l'ordinateur Windows.
2. Lancez la console d'administration WebSphere.
3. Suivez les instructions indiquées dans la documentation de WebSphere pour créer un hôte virtuel qui soit accessible uniquement par connexion SSL sécurisée. Cet hôte virtuel sera utilisé pour le plug-in Java qui gère les connexions HTTPS SNA.
4. Dans la barre de menus, sélectionnez Applications, puis Installation d'une nouvelle application.
5. Indiquez l'emplacement du fichier **snahttpsrv.ear**. Sélectionnez le bouton Suivant.
6. Sur les deux premières fenêtres, vous devez indiquer le nom d'hôte : entrez le nom de l'hôte virtuel que vous avez défini pour HTTPS. Pour tous les autres paramètres, vous pouvez accepter les options par défaut sauf si vous souhaitez utiliser une configuration WebSphere particulière. Dans les boîtes de dialogue suivantes, sélectionnez le bouton Suivant, puis le bouton Terminer dans la dernière boîte de dialogue. Un message doit indiquer que l'**Application** a été **installée avec succès**.
7. Cliquez sur Sauvegarde dans la configuration maîtresse puis cliquez sur le bouton Sauvegarder.
8. Dans la barre de menus, sélectionnez Applications, puis Applications d'entreprise.
9. Recherchez **SnaHttpTransport** dans la liste d'applications, cochez la case qui l'accompagne, puis cliquez sur le bouton Démarrer pour lancer l'application. (par la suite, l'application sera automatiquement lancée lors du démarrage de WebSphere Application Server.)
10. Dans la barre de menus, sélectionnez Environnement, Mise à jour du plug-in du serveur Web, puis cliquez sur le bouton OK. Cela permet de mettre à jour la configuration WebSphere.

Installation du fichier de configuration de serveur

Pour faire fonctionner WebSphere Application Server avec CS/AIX, il est nécessaire de créer la liste des serveurs CS/AIX accessibles par HTTPS. Pour créer et installer cette liste, procédez de la manière suivante.

1. Dans la barre de menus de la console d'administration WebSphere, sélectionnez Environnement, Gestion des Variables WebSphere.
2. Recherchez la variable **USER_INSTALL_ROOT** dans cette liste et notez sa valeur (chemin d'accès au répertoire sur le serveur WebSphere). La liste de variables d'environnement peut s'étendre sur plusieurs pages, vous pouvez les faire défiler avec le bouton Suivant.
3. Copiez le fichier **snahttpsrv.cfg** de l'emplacement où vous l'avez sauvegardé à l'étape «Configuration de WebSphere Application Server», à la page 40 (ou à partir du cd d'installation) vers le répertoire défini par la variable **USER_INSTALL_ROOT**, puis ouvrez ce fichier dans un éditeur de texte afin d'y insérer la liste des serveurs CS/AIX auxquels peuvent accéder les clients Remote API Client par HTTPS. Indiquez chaque serveur sur une ligne distincte, sous la forme suivante :

   server=*nomserveur.nomdomaine.com*

Procédures post-installation

La présente section explique comment exécuter des tâches de maintenance qui peuvent s'avérer nécessaires après l'installation de CS/AIX.

Fonctionnement client-serveur

Après l'installation, CS/AIX fonctionne en mode serveur autonome (tous les composants se trouvent sur le même système AIX). Pour l'exécuter en tant que serveur dans un domaine client-serveur, consultez les instructions indiquées dans la section Managing CS/AIX Client-Server Systems dans le manuel *Communications Server for AIX Administration Guide*.

Affichage des manuels HTML

Les manuels fournis avec le support d'installation de ce produit sont au format copie électronique HTML (Hypertext Markup Language). Le format copie électronique permet de rechercher ou de parcourir les informations plus facilement, à l'aide de liens hypertexte vers les informations connexes. Il facilite également l'utilisation partagée de la bibliothèque à travers un site.

Si vous choisissez d'installer les manuels HTML lors de l'installation du produit, ceux-ci sont installés dans le répertoire **/usr/share/man/info/***Langue***/sna**, où *Langue* représente la variante de langue des manuels. Par exemple, les manuels en français sont installés dans le répertoire **/usr/share/man/info/fr_FR/sna**.

Vous pouvez consulter les manuels HTML à l'aide de tout navigateur prenant en charge HTML version 3.2.

- Si un navigateur Web est installé sur votre système AIX, consultez les manuels HTML à l'adresse URL suivante :

  file:/usr/share/man/info/*langue***/sna/SNABOOKS.htm**

  langue indique la langue des manuels, par exemple `fr_FR` pour le français.
- Si un navigateur Web est installé sur votre système AIX, publiez le répertoire **/usr/share/man/info** sous la forme **doc_link**. Vous pouvez ensuite consulter les manuels HTML à l'adresse URL suivante :

  http://*nomserveur***/doc_link/***langue***/sna/SNABOOKS.htm**

  nomserveur défini le nom d'hôte TCP/IP du serveur AIX.

  langue indique la langue des manuels, par exemple `fr_FR` pour le français.

Affichage des manuels PDF

Les manuels fournis avec le support d'installation de ce produit sont au format PDF (Portable Document Format). Le format copie électronique facilite l'impression du document ainsi que la recherche d'informations dans le document par navigation à l'aide des liens hypertexte. Il facilite également l'utilisation partagée de la bibliothèque sur votre site, car des afficheurs PDF sont disponibles pour les différentes plateformes.

Si vous installez les manuels PDF lors de l'installation du produit, ils sont placés dans le répertoire **/usr/lib/sna/docs**. Les manuels se trouve également dans le répertoire **/DOCS** du support d'installation de CS/AIX.

Vous pouvez lire les manuels PDF à l'aide d'un afficheur PDF, par exemple Adobe Acrobat sous Windows ou **xpdf** sous Intel Linux.

Consultation des informations sur l'édition actuelle

Située dans le répertoire **/usr/lpp/sna/**, la dernière mise à jour du fichier **README de ce produit contient des informations sur les éventuelles modifications apportées au produit après publication de la bibliothèque CS/AIX. Consultez le fichier README** à chaque mise jour du produit.

Vous pouvez accéder au fichier **README** par l'intermédiaire de SMIT, en procédant de la manière suivante :

1. Après avoir installé CS/AIX version 6.3, accédez au menu SMIT principal du produit, en entrant la commande suivante sur la ligne de commande :

   smit sna

   Le menu SMIT principal de CS/AIX apparaît.
2. Sélectionnez l'option **Infos produit** à partir de ce menu. SMIT affiche la boîte de dialogue correspondante.
3. Sélectionnez l'une des options du menu pour visualiser le fichier **README** associé.

Configuration de SSL aux fins d'utilisation avec le serveur TN ou le Redirecteur TN

Si vous avez installé le logiciel AIX Certificate and SSL Base Runtime afin d'utiliser le serveur TN ou le redirecteur TN avec la fonction SSL, vous devez configurer le logiciel SSL après l'installation de CS/AIX.

Le logiciel SSL requiert les deux composants suivants :

- Une paire de clés est requise pour le chiffrement et le déchiffrement des données.
- Un certificat est requis pour l'authentification du serveur.

Le certificat et la paire de clés forment un seul enregistrement dans une base de données de fichiers de clés qui est stockée sur le serveur CS/AIX exécutant le serveur TN ou le Redirecteur TN. CS/AIX utilise la base de données pour mettre en œuvre SSL.

Pour gérer la base de données de fichiers de clés, entrez la commande suivante sur l'invite de commande AIX :

snakeyman

La commande **snakeyman** lance un programme Java. Pour plus de détails, reportez-vous à l'aide fournie avec ce programme.

Chaque enregistrement de la base de données est identifiée par un nom unique désigné par libellé. Si vous devez utiliser au moins deux enregistrements sur des sessions de serveur TN ou de Redirecteur TN différentes, vous devez noter les libellés que vous affectez lors de la configuration de la base de données ; ces libellés servent à identifier l'enregistrement à utiliser pour chaque session. Vous pouvez également identifier un des enregistrements comme enregistrement par défaut, de sorte que ce dernier soit utilisé par les sessions, sauf si vous indiquez explicitement le libellé d'un autre enregistrement.

Après avoir mis à jour les certificats serveur à l'aide de **snakeyman**, quittez le programme **snakeyman**, puis arrêtez et relancez le nœud CS/AIX afin d'utiliser les certificats mis à jour. Pour arrêter et relancer le nœud, utilisez la commande suivante :

```
snaadmin term_node
snaadmin init_node
```

Configuration d'un serveur Web pour le programme d'administration Web

Si vous utilisez le programme d'administration Web avec un serveur Web qui n'est pas répertorié dans la section «Conditions requises pour l'installation», à la page 22, ou si vous installez le serveur Web après CS/AIX, vous devez configurer des liaisons entre les répertoires CS/AIX et les répertoires du serveur Web de sorte que ce dernier puisse trouver les fichiers requis. Pour créer ces liaisons, utilisez la commande **ln**.

- Le répertoire de «servlets» du serveur Web doit être relié à **/usr/lib/sna/WebAdmin/Server**.
- Le sous-répertoire **SnaAdmin** du répertoire «public HTML» du serveur Web doit être relié à **/usr/lib/sna/WebAdmin/Client**.

Pour plus d'informations sur la configuration d'un serveur Web, consultez le fichier texte **/usr/lpp/sna.wa/README**, qui a été installé lors de l'installation du package d'administration Web de CS/AIX.

Host Access Class Library

Si vous choisissez d'installer les fichiers Host Access Class Library lors de l'installation du produit, ceux-ci sont installés dans le répertoire **/usr/share/lib/sna/ecl**. Pour plus de détails sur ces fichiers, consultez le fichier **readme.htm** dans le même répertoire.

Sauvegarde des fichiers de configuration de CS/AIX

CS/AIX sauvegarde automatiquement les fichiers de configuration du nœud, du domaine et du TP, lors de toute modification (à l'aide des outils d'administration de CS/AIX). Par exemple, lorsque vous apportez une modification qui affecte le fichier de configuration du nœud (**sna_node.cfg**), CS/AIX crée un fichier de sauvegarde intitulé **sna_node.bk** *n*, où *n* représente 1 ou 2 :

- Lors de la première modification du fichier, la configuration existante est sauvegardée dans **sna_node.bk1**.
- Lors de la deuxième modification du fichier, la configuration existante est sauvegardée dans **sna_node.bk2** et **sna_node.bk1** reste inchangé.

- Lors des modifications ultérieures du fichier, **sna_node.bk1** est ignoré, **sna_node.bk2** est renommé en **sna_node.bk1** et la configuration existante est sauvegardée dans **sna_node.bk2**.

Ce processus indique qu'il existe un maximum de deux fichiers de sauvegarde pour le fichier de configuration du nœud à un moment donné. La même procédure est utilisée pour générer les suffixes des autres fichiers de sauvegarde.

En complément des sauvegardes automatiques, il est recommandé de sauvegarder les fichiers de configuration afin d'éviter les pertes de données dans les circonstances suivantes :

- Avant d'installer un nouveau niveau du système d'exploitation AIX
- Avant installation d'une nouvelle édition de CS/AIX ;
- Après création d'une configuration.

Vous pouvez sauvegarder les fichiers de configuration à l'aide des commandes suivantes :

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

Dans ces commandes, *nom_unité* désigne le chemin et le nom de l'unité destinée à recevoir les données des fichiers sauvegardés. Il est recommandé de sauvegarder les fichiers vers des supports externes, tels qu'une disquette ou une bande.

Restauration d'une copie de sauvegarde des fichiers de configuration CS/AIX

Pour restaurer les fichiers de configuration CS/AIX sauvegardés lors de l'étape «Sauvegarde des fichiers de configuration de CS/AIX», à la page 43, procédez comme suit :

1. Vérifiez que CS/AIX n'est pas actif. Pour ce faire, entrez la commande suivante :

   snaadmin status_node

   Si CS/AIX est actif, la commande affiche des informations relatives à l'état du nœud local ; sinon, elle affiche un message indiquant que CS/AIX est inactif.

   Si CS/AIX est actif, entrez la commande suivante pour le désactiver :

   sna stop
2. Entrez les commandes suivantes :

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

   Dans cette commande, *num_unité* désigne le chemin et le nom de l'unité que vous avez utilisée pour la sauvegarde des fichiers.

   Cette commande remplace les fichiers de configuration existants portant le même nom dans le répertoire **/etc/sna**.

Réinitialisation des fichiers de configuration

Si, à la suite d'une modification par inadvertance, les fichiers de configuration de CS/AIX ne sont plus utilisables, il peut être nécessaire de réinitialiser les fichiers

pour pouvoir reconfigurer CS/AIX comme s'il venait d'être installé. Effectuez cette opération uniquement si vous êtes sûr de ne plus pouvoir récupérer les données de configuration.

Remarque : Si vous disposez de fichiers de configuration de sauvegarde valides, vous pouvez les copier dans le répertoire **/etc/sna/** et les utiliser pour initialiser le nœud à l'aide de la commande **sna start**.

Vous pouvez réinitialiser les fichiers de configuration suivants :

- Fichier de configuration du nœud **sna_node.cfg**
- Fichier de configuration du domaine **sna_domn.cfg**
- Fichier de configuration du TP **sna_tps**
- Fichier de base de données de fichiers de clés SSL et fichier de mot de passe secret

Pour réinitialiser les fichiers de configuration, suivez les étapes ci-après :

1. Quittez le programme d'administration s'il est actif et désactivez CS/AIX en exécutant la commande suivante :

   sna stop
2. Sauvegardez les fichiers de configuration existants en copiant tout fichier réinitialisé vers un emplacement différent.
3. Supprimez les fichiers que vous réinitialisez.
4. Si vous avez supprimé le fichier de configuration du domaine, lancez la commande suivante pour le créer à nouveau (en copiant l'exemple de fichier de configuration fourni avec CS/AIX) :

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

   Cette commande permet de créer un nouveau fichier de configuration de domaine, lequel est nécessaire pour lancer CS/AIX.
5. Si vous avez supprimé le fichier de base de données de fichiers de clés, recréez-le à l'aide de la commande suivante (en copiant l'exemple de fichier fourni avec CS/AIX) :

   cp -p /usr/lib/sna/samples/ibmcs.* /etc/sna
6. Utilisez la commande suivante pour redémarrer CS/AIX :

   sna start
7. Lancez le programme d'administration Motif :

   xsnaadmin &

   Si le fichier **sna_node.cfg** n'existe pas, le programme d'administration vous invite à configurer le nœud. Vous pouvez poursuivre en configurant le nœud et les autres ressources, comme indiqué dans Chapitre 9, «Configuration et utilisation de CS/AIX», à la page 83 ou dans le manuel *Communications Server for AIX Administration Guide*.

   Si vous avez utilisé un fichier **sna_node.cfg** valide, le nœud est initialisé à l'aide du nouveau fichier de configuration.

Chapitre 4. Installation des clients IBM Remote API Client sous Linux

Ce chapitre explique comment installer IBM Remote API Client sous Linux, lequel permet d'exécuter des applications SNA sur un poste de travail Linux sans devoir effectuer une installation SNA complète en pile. Un client Remote API Client sous Linux peut se connecter à un ou plusieurs serveurs CS/AIX (ou serveurs CS Linux) via un réseau TCP/IP.

Nous vous recommandons de lire le fichier README d'IBM Remote API Client avant d'installer ce logiciel. Ce fichier se trouve dans le répertoire **/ibm-commserver-clients/linux** du CD d'installation.

Configuration matérielle et logicielle

Configuration matérielle

IBM Remote API Client requiert au minimum un système Intel Pentium II 32 bits, ou un système Opteron, pris en charge par l'une des distributions Linux répertoriées ci-dessous.

Version du système d'exploitation Linux

La version en cours d'IBM Remote API Client a été testée avec les versions suivantes du système d'exploitation Linux. Elle peut également fonctionner de façon satisfaisante sur les autres distributions Linux.

- RedHat Enterprise Linux 2.1 (RHEL2.1)
- RedHat Enterprise Linux 3 (RHEL3)
- RedHat Enterprise Linux 4 (RHEL4)
- SUSE Linux Enterprise Server 8 (SLES8)
- SUSE Linux Enterprise Server 9 (SLES9)

Pour obtenir des informations sur les packages en option nécessaires, consultez le fichier **README** dans le répertoire **/ibm-commserver-clients/linux** du CD d'installation.

Java

Pour utiliser l'API CPI-C Java, le logiciel Java est nécessaire. Pour plus d'informations, consultez le fichier **README** dans le répertoire **/ibm-commserver-clients/linux** sur le CD d'installation.

GSKIT

Si le client se connecte aux serveurs CS/AIX par HTTPS, le logiciel GSKIT est nécessaire pour l'accès HTTPS aux serveurs via un serveur WebSphere. Le logiciel GSKIT est fourni sur le CD d'installation, mais certains packages en option du système d'exploitation Linux peuvent s'avérer nécessaires pour l'installer. Pour plus d'informations sur les packages en option nécessaires, consultez le fichier **README** dans le répertoire **/ibm-commserver-clients/linux** du CD d'installation.

Si tous les packages prérequis sont installés lorsque vous exécutez le processus d'installation du client (décrit ultérieurement dans ce chapitre), le logiciel GSKIT est automatiquement installé durant ce processus. Sinon, vous pouvez également l'installer plus tard.

Affichage des caractéristiques d'installation des produits

Vous pouvez afficher des informations sur Remote API Client et les packages logiciels associés déjà installés. Pour afficher la liste de tous les packages installés, utilisez la commande suivante :

rpm -q -a

Pour afficher des informations détaillées sur un package particulier, utilisez la commande suivante :

rpm -q -i *nom_package*

nom_package est le nom de base du package installé, par exemple **ibm-commserver-client**.

Configuration de la variable d'environnement relative à la langue

A l'aide de la commande suivante, modifiez la variable `LANG` afin d'indiquer la langue que vous souhaitez utilisez :

export LANG=*langue*

Remplacez *langue* par l'identifiant de la langue que vous souhaitez utiliser, parmi les identificateurs suivants :

Identificateur	Langue
en_US	Anglais (États-Unis)
ja_JP	Japonais (PC)
de_DE	Allemand
es_ES	Espagnol
fr_FR	Français
ko_KR	Coréen
pt_BR	Portugais
zh_CN	Chinois (simplifié)
zh_TW	Chinois (traditionnel)

Installation de Remote API Client sous Linux

Après avoir installé les logiciels prérequis, vous pouvez installer IBM Remote API Client.

Si un niveau antérieur d'IBM Remote API Client est déjà installé, suivez la procédure décrite dans la section «Désinstallation de Remote API Client sous Linux», à la page 51 pour le désinstaller avant d'installer le nouveau niveau. Toutes les données de configuration seront conservées pour être utilisées avec la nouvelle installation.

1. Connectez-vous avec les droits d'accès ″root″.
2. Montez le CD et utilisez-le comme répertoire de travail.

Pour RHEL2.1 ou RHEL3 :

mount /dev/cdrom
cd /mnt/cdrom

Pour SLES ou RHEL4 :

mount /dev/cdrom
cd /media/cdrom

Le nom du répertoire **/media/cdrom** peut être différent sur une unité de DVD. Utilisez la commande **df** pour déterminer où est monté le CD sous Linux.

3. Accédez à IBM Remote API Client dans le sous-répertoire Linux du CD et exécutez le script shell pour installer le client.

   cd
   ibm-commserver-clients/linux
   ./installibmcscli

   Le script shell vérifie certains prérequis et génère des messages d'avertissement si les conditions requises ne sont pas remplies. Vous êtes ensuite invité à lire et à accepter le contrat de licence, puis le script installe les RPM. Si les prérequis sont déjà installés, le script installe également le logiciel GSKIT.

4. Ajoutez les répertoires binaires d'IBM Remote API Client à la variable PATH. Pour effectuer cette opération automatiquement, vous pouvez modifier le profil :

   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

   Vous devez également définir la variable d'environnement suivante pour les applications CPI-C Java :

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

   Pour certaines applications, vous devez également définir la variable d'environnement `LD_PRELOAD`, mais il est préférable de ne pas effectuer de modification globale dans votre profil :

   export LD_PRELOAD=/usr/lib/libpLiS.so

5. Lancez IBM Remote API Client. Après l'installation, le démarrage est automatiquement effectué lors de l'amorçage de l'ordinateur. Veillez à ne pas effectuer cette opération à partir d'un répertoire du CD.

   cd /
   sna start

Remarque : Pour connecter IBM Remote API Client aux serveurs par HTTPS, vous devez utiliser le programme de gestion des clés GSKIT pour configurer les certificats de sécurité sur le client. Pour plus de détails, reportez-vous à la section «Configuration des certificats de sécurité HTTPS à l'aide de GSKIT», à la page 50.

Vous devez également mettre à jour le fichier de données de réseau du client afin d'indiquer les serveurs CS/AIX auxquels le client peut se connecter et le nom du serveur WebSphere qui assure le support HTTPS. Pour plus d'informations, voir la section sur la gestion des clients Remote API Client dans le manuel *Communications Server for AIX Administration Guide*.

Configuration des certificats de sécurité HTTPS à l'aide de GSKIT

Un client peut se connecter aux serveurs CS/AIX par HTTPS si le logiciel de gestion des clés GSKIT est installé sur le client. En principe il est installé lors de l'installation du client si les prérequis nécessaires au système d'exploitation Linux sont installés, comme décrit dans le fichier **README** du CD d'installation. Si GSKIT n'a pas été installé lors de l'installation du client, vous pouvez l'installer maintenant (si les produits prérequis sont installés), en procédant comme suit.

1. Connectez-vous avec les droits d'accès ″root″.
2. Montez le CD et utilisez-le comme répertoire de travail.

   Pour RHEL2.1 ou RHEL3 :

   mount /dev/cdrom
   cd /mnt/cdrom

   Pour SLES ou RHEL4 :

   mount /dev/cdrom
   cd /media/cdrom

   Le nom du répertoire **/media/cdrom** peut être différent sur une unité de DVD. Utilisez la commande **df** pour déterminer où est monté le CD sous Linux.
3. Accédez à IBM Remote API Client dans le sous-répertoire Linux du CD, et lancez le script shell pour installer le logiciel GSKIT.

   cd
   ibm-commserver-clients/linux
   ./installgskit

Pour connecter IBM Remote API Client aux serveurs par HTTPS, vous devez utiliser le logiciel de gestion des clés GSKIT pour configurer les certificats de sécurité sur le client. Procédez comme suit.

1. Lancez le gestionnaire de clés GSKIT à l'aide de la commande suivante :

   /opt/ibm/sna/bin/snakeyman

   Sur l'interface utilisateur du gestionnaire de clés, ouvrez le fichier de base de données de clés **/etc/opt/ibm/sna/ibmcs.kdb**, qui est au format CMS.
2. Le mot de passe initial de la base de données de clés est `ibmcs`. Avant de configurer les certificats de sécurité, **modifiez ce mot de passe** afin d'assurer la sécurité de votre configuration. Dans la boîte de dialogue de modification du mot de passe, cochez la case 'Stocker le mot de passe dans un fichier ?' pour sauvegarder le nouveau mot de passe afin que le client puisse ouvrir la base de données de clés.
3. Récupérez une copie du certificat de l'autorité de certification utilisé pour signer le certificat de sécurité du serveur Web, puis installez-la dans la base de données de clés. Pour cela, sélectionnez Certificats signataires sur l'interface utilisateur du gestionnaire de clés et cliquez sur Ajouter.
4. Si le serveur WebSphere est configuré de façon à rendre obligatoire les certificats de sécurité du client, celui-ci doit disposer d'un certificat fourni par une autorité de certification ayant elle-même un certificat répertorié dans la base de données des certificats de sécurité du serveur Web. Pour demander un nouveau certificat :
   a. Sélectionnez Créer, Nouvelle demande de certificat sur l'interface utilisateur du gestionnaire de clés, puis indiquez les informations demandées.

b. Enregistrez le certificat, extrayez-le dans un fichier et envoyez-le à l'autorité de certification.
c. Lorsque le certificat est généré, placez-le dans la base de données du serveur Web. Pour cela, sélectionnez Certificats personnels sur l'interface utilisateur du gestionnaire de clés et cliquez sur Recevoir.

Pour effectuer un contrôle interne, vous pouvez créer un certificat client auto-signé au lieu de récupérer un certificat auprès de l'autorité de certification. Cependant, cela n'assure pas le niveau de sécurité optimal et ne doit pas être appliqué sur un système connecté. Pour créer un certificat auto-signé :

a. Sélectionnez Créer, Nouveau certificat auto-signé sur l'interface du gestionnaire de clés, et indiquez les informations demandées.
b. Enregistrez le certificat et extrayez-le dans un fichier.
c. Placez le fichier du certificat dans la base de données du serveur Web. Pour cela, sélectionnez Certificats personnels sur l'interface utilisateur du gestionnaire de clés et cliquez sur Recevoir.

5. Quittez le gestionnaire de clés GSKIT à la fin de la configuration des certificats.

Désinstallation de Remote API Client sous Linux

Pour désinstaller Remote API Client sous Linux, vous pouvez utiliser la commande suivante.

```
/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
```

Les packages affichés par ces commandes ne sont pas tous installés sur chaque système.

Lors de la désinstallation d'IBM Remote API Client sous Linux, les données de configuration personnalisées sont conservées en vue d'être utilisées lors d'une installation ultérieure.

Chapitre 5. Installation d'IBM Remote API Clients sous Linux pour zSeries

Ce chapitre explique comment installer IBM Remote API Client sous Linux, lequel permet d'exécuter des applications SNA sur un grand système zSeries sans devoir effectuer une installation SNA complète en pile. Un client Remote API Client sous Linux pour zSeries peut se connecter à un ou plusieurs serveurs CS/AIX (ou serveurs CS Linux) via un réseau TCP/IP.

Nous vous recommandons de lire le fichier README d'IBM Remote API Client avant d'installer ce logiciel. Ce fichier se trouve dans le répertoire **/ibm-commserver-clients/linux-zseries** du CD d'installation.

Configuration matérielle et logicielle

Configuration matérielle

IBM Remote API Client requiert un système zSeries 31 bits ou 64 bits pris en charge par l'une des distributions Linux répertoriées dans «Version du système d'exploitation Linux».

A l'aide de la commande **uname -m**, vérifiez les classes d'unité centrale. Elle doit indiquer `s390` dans le cas d'un environnement 31 bits ou bien `s390x` dans le cas d'un environnement 64 bits.

Version du système d'exploitation Linux

La version en cours d'IBM Remote API Client a été testée avec les versions suivantes du système d'exploitation Linux. Elle peut également fonctionner de façon satisfaisante sur les autres distributions Linux.

- RedHat Enterprise Linux 3 pour S/390 (RHEL3–s390)
- RedHat Enterprise Linux 3 pour zSeries (RHEL3–s390x)
- RedHat Enterprise Linux 4 pour S/390 (RHEL4–s390)
- RedHat Enterprise Linux 4 pour zSeries (RHEL4–s390x)
- SUSE Linux Enterprise Server 8 pour grand système IBM (SLES8–s390*)
- SUSE Linux Enterprise Server 9 pour grand système IBM (SLES9–s390*)

Pour obtenir des informations sur les packages en option nécessaires, consultez le fichier **README** sur le CD d'installation.

Java

Pour utiliser l'API CPI-C Java, le logiciel Java est nécessaire. Pour plus d'informations, consultez le fichier **README** sur le CD d'installation.

GSKIT

Si le client se connecte aux serveurs CS/AIX par HTTPS, le logiciel GSKIT est nécessaire pour l'accès HTTPS aux serveurs via un serveur WebSphere. Le logiciel GSKIT est fourni sur le CD d'installation, mais certains packages en option du système d'exploitation Linux peuvent s'avérer nécessaires pour l'installer. Pour

plus d'informations sur les packages en option nécessaires, consultez le fichier **README** dans le répertoire **/ibm-commserver-clients/linux-zseries** du CD d'installation.

Si tous les packages prérequis sont installés lorsque vous exécutez le processus d'installation du client (décrit ultérieurement dans ce chapitre), le logiciel GSKIT est automatiquement installé durant ce processus. Sinon, vous pouvez également l'installer plus tard.

Affichage des caractéristiques d'installation des produits

Vous pouvez afficher des informations sur Remote API Client et les packages logiciels associés déjà installés. Pour afficher la liste de tous les packages installés, utilisez la commande suivante :

rpm -q -a

Pour afficher des informations détaillées sur un package particulier, utilisez la commande suivante :

rpm -q -i *nom_package*

nom_package est le nom de base du package installé, par exemple **ibm-commserver-client**.

Configuration de la variable d'environnement relative à la langue

A l'aide de la commande suivante, modifiez la variable `LANG` afin d'indiquer la langue que vous souhaitez utilisez :

export LANG=*langue*

Remplacez *langue* par l'identifiant de la langue que vous souhaitez utiliser, parmi les identificateurs suivants :

Identificateur	Langue
en_US	Anglais (États-Unis)
ja_JP	Japonais (PC)
de_DE	Allemand
es_ES	Espagnol
fr_FR	Français
ko_KR	Coréen
pt_BR	Portugais
zh_CN	Chinois (simplifié)
zh_TW	Chinois (traditionnel)

Installation de Remote API Client sous Linux pour zSeries

Après avoir installé les logiciels prérequis, vous pouvez installer IBM Remote API Client.

Si un niveau antérieur d'IBM Remote API Client est déjà installé, suivez la procédure décrite dans la section «Désinstallation de Remote API Client sous Linux

pour zSeries», à la page 57 pour le désinstaller avant d'installer le nouveau niveau. Toutes les données de configuration seront conservées pour être utilisées avec la nouvelle installation.

1. Copiez (ou récupérez par FTP) le fichier **ibm-commserver-client–6.3.0.0–s390.tgz** qui se trouve dans le répertoire **/ibm-commserver-clients/linux-zseries** du CD-ROM vers le système Linux zSeries. Veillez à utiliser le mode binaire pour copier le fichier ou le transférer par FTP.
2. Connectez-vous au système Linux zSeries en tant qu'utilisateur root.
3. Décompressez le fichier tar dans un répertoire temporaire vide :

   mkdir /tmp/ibmcs

   cd /tmp/ibmcs

   tar —xzf ibm-commserver-client–6.3.0.0–s390.tgz
4. Exécutez le script shell **installibmcscli** :

   ./installibmcscli

   Ce script shell vérifie certains prérequis et génère des messages d'avertissement si les conditions requises ne sont pas remplies. Vous êtes ensuite invité à lire et à accepter le contrat de licence, puis le script installe les RPM. Pour ne pas utiliser cette invite, vous pouvez définir des paramètres supplémentaires avec la commande **installibmcscli**, comme décrit ci-dessous. Le script shell installe ensuite les packages **rpm**. Si les prérequis sont déjà installés, le script installe également le logiciel GSKIT.
5. Ajoutez les répertoires binaires d'IBM Remote API Client à la variable PATH. Pour effectuer cette opération automatiquement, vous pouvez modifier le profil :

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

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

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

   Si vous envisagez d'exécuter des applications 64 bits, utilisez :

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

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

   Vous devez également définir la variable d'environnement suivante pour les applications CPI-C Java :

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

   Pour certaines applications, vous devez également définir la variable d'environnement `LD_PRELOAD`, mais il est préférable de ne pas effectuer de modification globale dans votre profil :

   export LD_PRELOAD=/usr/lib/libpLiS.so
6. Lancez IBM Remote API Client. Après l'installation, le démarrage est automatiquement effectué lors de l'amorçage de l'ordinateur. Veillez à ne pas effectuer cette opération à partir d'un répertoire du CD.

   cd /
   sna start
7. Une fois l'installation effectuée, vous pouvez supprimer le fichier **tgz** et le répertoire temporaire créés durant le processus d'installation.

Remarque : Pour connecter IBM Remote API Client aux serveurs par HTTPS, vous devez utiliser le programme de gestion des clés GSKIT pour configurer les certificats de sécurité sur le client. Pour plus de détails,

reportez-vous à la section «Configuration des certificats de sécurité HTTPS à l'aide de GSKIT».

Vous devez également mettre à jour le fichier de données de réseau du client afin d'indiquer les serveurs CS/AIX auxquels le client peut se connecter et le nom du serveur WebSphere qui assure le support HTTPS. Pour plus d'informations, voir la section sur la gestion des clients Remote API Client dans le manuel *Communications Server for AIX Administration Guide*.

Configuration des certificats de sécurité HTTPS à l'aide de GSKIT

Un client peut se connecter aux serveurs CS/AIX par HTTPS si le logiciel de gestion des clés GSKIT est installé sur le client. En principe il est installé lors de l'installation du client si les prérequis nécessaires au système d'exploitation Linux sont installés, comme décrit dans le fichier **README** du CD d'installation. Si GSKIT n'a pas été installé lors de l'installation du client, vous pouvez l'installer maintenant (si les produits prérequis sont installés), en procédant comme suit.

1. Copiez (ou récupérez par FTP) le fichier **ibm-commserver-client–6.3.0.0–s390.tgz** qui se trouve dans le répertoire **/ibm-commserver-clients/linux-zseries** du CD-ROM vers le système Linux zSeries. Veillez à utiliser le mode binaire pour copier le fichier ou le transférer par FTP.
2. Connectez-vous au système Linux zSeries en tant qu'utilisateur root.
3. Décompressez le fichier tar dans un répertoire temporaire vide :

   mkdir /tmp/ibmcs

   cd /tmp/ibmcs

   tar —xzf ibm-commserver-client–6.3.0.0–s390.tgz
4. Exécutez le script shell **installgskit** :

   ./installgskit
5. Une fois l'installation effectuée, vous pouvez supprimer le fichier **tgz** et le répertoire temporaire créés durant le processus d'installation.

Pour connecter IBM Remote API Client aux serveurs par HTTPS, vous devez utiliser le logiciel de gestion des clés GSKIT pour configurer les certificats de sécurité sur le client. Procédez comme suit.

1. Lancez le gestionnaire de clés GSKIT à l'aide de la commande suivante :

   /opt/ibm/sna/bin/snakeyman

   Sur l'interface utilisateur du gestionnaire de clés, ouvrez le fichier de base de données de clés **/etc/opt/ibm/sna/ibmcs.kdb**, qui est au format CMS.
2. Le mot de passe initial de la base de données de clés est `ibmcs`. Avant de configurer les certificats de sécurité, **modifiez ce mot de passe** afin d'assurer la sécurité de votre configuration. Dans la boîte de dialogue de modification du mot de passe, cochez la case 'Stocker le mot de passe dans un fichier ?' pour sauvegarder le nouveau mot de passe afin que le client puisse ouvrir la base de données de clés.
3. Récupérez une copie du certificat de l'autorité de certification utilisé pour signer le certificat de sécurité du serveur Web, puis installez-la dans la base de données de clés. Pour cela, sélectionnez Certificats signataires sur l'interface utilisateur du gestionnaire de clés et cliquez sur Ajouter.
4. Si le serveur WebSphere est configuré de façon à rendre obligatoire les certificats de sécurité du client, celui-ci doit disposer d'un certificat fourni par

une autorité de certification ayant elle-même un certificat répertorié dans la base de données des certificats de sécurité du serveur Web. Pour demander un nouveau certificat :

a. Sélectionnez Créer, Nouvelle demande de certificat sur l'interface utilisateur du gestionnaire de clés, puis indiquez les informations demandées.
b. Enregistrez le certificat, extrayez-le dans un fichier et envoyez-le à l'autorité de certification.
c. Lorsque le certificat est généré, placez-le dans la base de données du serveur Web. Pour cela, sélectionnez Certificats personnels sur l'interface utilisateur du gestionnaire de clés et cliquez sur Recevoir.

Pour effectuer un contrôle interne, vous pouvez créer un certificat client auto-signé au lieu de récupérer un certificat auprès de l'autorité de certification. Cependant, cela n'assure pas le niveau de sécurité optimal et ne doit pas être appliqué sur un système connecté. Pour créer un certificat auto-signé :

a. Sélectionnez Créer, Nouveau certificat auto-signé sur l'interface du gestionnaire de clés, et indiquez les informations demandées.
b. Enregistrez le certificat et extrayez-le dans un fichier.
c. Placez le fichier du certificat dans la base de données du serveur Web. Pour cela, sélectionnez Certificats personnels sur l'interface utilisateur du gestionnaire de clés et cliquez sur Recevoir.

5. Quittez le gestionnaire de clés GSKIT à la fin de la configuration des certificats.

Désinstallation de Remote API Client sous Linux pour zSeries

Pour désinstaller Remote API Client sous Linux pour zSeries, vous pouvez utiliser les commandes suivantes.

```
/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
```

Les packages affichés par ces commandes ne sont pas tous installés sur chaque système.

Lors de la désinstallation d'IBM Remote API Client sous Linux pour zSeries les données de configuration personnalisées sont conservées en vue d'être utilisées lors d'une installation ultérieure.

Chapitre 6. Installation d'IBM Remote API Clients sous Linux pour pSeries

Ce chapitre explique comment installer IBM Remote API Client sous Linux pour pSeries, lequel permet d'exécuter des applications SNA sur un ordinateur pSeries sans devoir effectuer une installation SNA complète en pile. Un client Remote API Client sous Linux pour pSeries peut se connecter à un ou plusieurs serveurs CS/AIX (ou serveurs CS Linux) via un réseau TCP/IP.

Nous vous recommandons de lire le fichier README d'IBM Remote API Client avant d'installer ce logiciel. Ce fichier se trouve dans le répertoire **/ibm-commserver-clients/linux-ppc64** du CD d'installation.

Configuration matérielle et logicielle

Configuration matérielle

IBM Remote API Client requiert un système pSeries POWER5 ou OpenPower pris en charge par l'une des distributions Linux répertoriées dans «Version du système d'exploitation Linux».

A l'aide de la commande **uname -m**, vérifiez les classes d'unité centrale. Elle doit indiquer `ppc64` dans le cas d'un système pSeries POWER5 ou OpenPower

Version du système d'exploitation Linux

La version en cours d'IBM Remote API Client a été testée avec les versions suivantes du système d'exploitation Linux. Elle peut également fonctionner de façon satisfaisante sur les autres distributions Linux.

- RedHat Enterprise Linux 4 (RHEL4)
- SUSE Linux Enterprise Server 9 (SLES9)

Pour obtenir des informations sur les packages en option nécessaires, consultez le fichier **README** sur le CD d'installation.

Java

Pour utiliser l'API CPI-C Java, le logiciel Java est nécessaire. Pour plus d'informations, consultez le fichier **README** sur le CD d'installation.

GSKIT

Si le client se connecte aux serveurs CS/AIX par HTTPS, le logiciel GSKIT est nécessaire pour l'accès HTTPS aux serveurs via un serveur WebSphere. Le logiciel GSKIT est fourni sur le CD d'installation, mais certains packages en option du système d'exploitation Linux peuvent s'avérer nécessaires pour l'installer. Pour plus d'informations sur les packages en option nécessaires, consultez le fichier **README** dans le répertoire **/ibm-commserver-clients/linux-ppc64** du CD d'installation.

Si tous les packages prérequis sont installés lorsque vous exécutez le processus d'installation du client (décrit ultérieurement dans ce chapitre), le logiciel GSKIT est automatiquement installé durant ce processus. Sinon, vous pouvez également l'installer plus tard.

Affichage des caractéristiques d'installation des produits

Vous pouvez afficher des informations sur Remote API Client et les packages logiciels associés déjà installés. Pour afficher la liste de tous les packages installés, utilisez la commande suivante :

rpm -q -a

Pour afficher des informations détaillées sur un package particulier, utilisez la commande suivante :

rpm -q -i *nom_package*

nom_package est le nom de base du package installé, par exemple **ibm-commserver-client**.

Configuration de la variable d'environnement relative à la langue

A l'aide de la commande suivante, modifiez la variable `LANG` afin d'indiquer la langue que vous souhaitez utilisez :

export LANG=*langue*

Remplacez *langue* par l'identifiant de la langue que vous souhaitez utiliser, parmi les identificateurs suivants :

Identificateur	Langue
en_US	Anglais (États-Unis)
ja_JP	Japonais (PC)
de_DE	Allemand
es_ES	Espagnol
fr_FR	Français
ko_KR	Coréen
pt_BR	Portugais
zh_CN	Chinois (simplifié)
zh_TW	Chinois (traditionnel)

Installation de Remote API Client sous Linux pour pSeries

Après avoir installé les logiciels prérequis, vous pouvez installer IBM Remote API Client.

Si un niveau antérieur d'IBM Remote API Client est déjà installé, suivez la procédure décrite dans la section «Désinstallation de Remote API Client sous Linux pour pSeries», à la page 63 pour le désinstaller avant d'installer le nouveau niveau. Toutes les données de configuration seront conservées pour être utilisées avec la nouvelle installation.

1. Connectez-vous avec les droits d'accès ″root″.
2. Montez le CD et utilisez-le comme répertoire de travail.

mount /dev/cdrom
cd /media/cdrom

Le nom du répertoire **/media/cdrom** peut être différent sur une unité de DVD. Utilisez la commande **df** pour déterminer où est monté le CD sous Linux.

3. Accédez à IBM Remote API Client dans le sous-répertoire OpenPower du CD et exécutez le script shell pour installer le client.

   cd ibm-commserver-clients/linux-ppc64
   ./installibmcscli

   Le script shell vérifie certains prérequis et génère des messages d'avertissement si les conditions requises ne sont pas remplies. Vous êtes ensuite invité à lire et à accepter le contrat de licence, puis le script installe les RPM. Si les prérequis sont déjà installés, le script installe également le logiciel GSKIT.

4. Ajoutez les répertoires binaires d'IBM Remote API Client à la variable PATH. Pour effectuer cette opération automatiquement, vous pouvez modifier le profil :

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

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

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

   Si vous envisagez d'exécuter des applications 64 bits, utilisez :

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

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

   Vous devez également définir la variable d'environnement suivante pour les applications CPI-C Java :

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

   Pour certaines applications, vous devez également définir la variable d'environnement `LD_PRELOAD`, mais il est préférable de ne pas effectuer de modification globale dans votre profil :

   export LD_PRELOAD=/usr/lib/libpLiS.so

5. Lancez IBM Remote API Client. Après l'installation, le démarrage est automatiquement effectué lors de l'amorçage de l'ordinateur. Veillez à ne pas effectuer cette opération à partir d'un répertoire du CD.

   cd /
   sna start

Remarque : Pour connecter IBM Remote API Client aux serveurs par HTTPS, vous devez utiliser le programme de gestion des clés GSKIT pour configurer les certificats de sécurité sur le client. Pour plus de détails, reportez-vous à la section «Configuration des certificats de sécurité HTTPS à l'aide de GSKIT», à la page 62.

Vous devez également mettre à jour le fichier de données de réseau du client afin d'indiquer les serveurs CS/AIX auxquels le client peut se connecter et le nom du serveur WebSphere qui assure le support HTTPS. Pour plus d'informations, voir la section sur la gestion des clients Remote API Client dans le manuel *Communications Server for AIX Administration Guide*.

Configuration des certificats de sécurité HTTPS à l'aide de GSKIT

Un client peut se connecter aux serveurs CS/AIX par HTTPS si le logiciel de gestion des clés GSKIT est installé sur le client. En principe il est installé lors de l'installation du client si les prérequis nécessaires au système d'exploitation Linux sont installés, comme décrit dans le fichier **README** du CD d'installation. Si GSKIT n'a pas été installé lors de l'installation du client, vous pouvez l'installer maintenant (si les produits prérequis sont installés), en procédant comme suit.

1. Connectez-vous avec les droits d'accès ″root″.
2. Montez le CD et utilisez-le comme répertoire de travail.

   mount /dev/cdrom
   cd /media/cdrom

   Le nom du répertoire **/media/cdrom** peut être différent sur une unité de DVD. Utilisez la commande **df** pour déterminer où est monté le CD sous Linux.
3. Accédez à IBM Remote API Client dans le sous-répertoire OpenPower du CD et installez le logiciel GSKIT à l'aide de la commande suivante.

   cd ibm-commserver-clients/linux-ppc64
   ./installgskit

Pour connecter IBM Remote API Client aux serveurs par HTTPS, vous devez utiliser le logiciel de gestion des clés GSKIT pour configurer les certificats de sécurité sur le client. Procédez comme suit.

1. Lancez le gestionnaire de clés GSKIT à l'aide de la commande suivante :

   /opt/ibm/sna/bin/snakeyman

   Sur l'interface utilisateur du gestionnaire de clés, ouvrez le fichier de base de données de clés **/etc/opt/ibm/sna/ibmcs.kdb**, qui est au format CMS.
2. Le mot de passe initial de la base de données de clés est `ibmcs`. Avant de configurer les certificats de sécurité, **modifiez ce mot de passe** afin d'assurer la sécurité de votre configuration. Dans la boîte de dialogue de modification du mot de passe, cochez la case 'Stocker le mot de passe dans un fichier ?' pour sauvegarder le nouveau mot de passe afin que le client puisse ouvrir la base de données de clés.
3. Récupérez une copie du certificat de l'autorité de certification utilisé pour signer le certificat de sécurité du serveur Web, puis installez-la dans la base de données de clés. Pour cela, sélectionnez Certificats signataires sur l'interface utilisateur du gestionnaire de clés et cliquez sur Ajouter.
4. Si le serveur WebSphere est configuré de façon à rendre obligatoire les certificats de sécurité du client, celui-ci doit disposer d'un certificat fourni par une autorité de certification ayant elle-même un certificat répertorié dans la base de données des certificats de sécurité du serveur Web. Pour demander un nouveau certificat :
   a. Sélectionnez Créer, Nouvelle demande de certificat sur l'interface utilisateur du gestionnaire de clés, puis indiquez les informations demandées.
   b. Enregistrez le certificat, extrayez-le dans un fichier et envoyez-le à l'autorité de certification.
   c. Lorsque le certificat est généré, placez-le dans la base de données du serveur Web. Pour cela, sélectionnez Certificats personnels sur l'interface utilisateur du gestionnaire de clés et cliquez sur Recevoir.

   Pour effectuer un contrôle interne, vous pouvez créer un certificat client auto-signé au lieu de récupérer un certificat auprès de l'autorité de certification.

Cependant, cela n'assure pas le niveau de sécurité optimal et ne doit pas être appliqué sur un système connecté. Pour créer un certificat auto-signé :

a. Sélectionnez Créer, Nouveau certificat auto-signé sur l'interface du gestionnaire de clés, et indiquez les informations demandées.
b. Enregistrez le certificat et extrayez-le dans un fichier.
c. Placez le fichier du certificat dans la base de données du serveur Web. Pour cela, sélectionnez Certificats personnels sur l'interface utilisateur du gestionnaire de clés et cliquez sur Recevoir.

5. Quittez le gestionnaire de clés GSKIT à la fin de la configuration des certificats.

Désinstallation de Remote API Client sous Linux pour pSeries

Pour désinstaller Remote API Client sous Linux pour pSeries, vous pouvez utiliser les commandes suivantes.

```
/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
```

Les packages affichés par ces commandes ne sont pas tous installés sur chaque système.

Lors de la désinstallation d'IBM Remote API Client sous Linux pour pSeries, les données de configuration personnalisées sont conservées en vue d'être utilisées lors d'une installation ultérieure.

Chapitre 7. Installation d'IBM Remote API Client sur des systèmes AIX

Ce chapitre indique comment installer IBM Remote API Client sous AIX, lequel permet d'exécuter des applications SNA sur un poste de travail AIX sans devoir effectuer une installation SNA complète en pile. Un client Remote API Client sous AIX peut se connecter à un ou plusieurs serveurs CS/AIX (ou serveurs CS Linux) via un réseau TCP/IP.

Nous vous recommandons de lire le fichier README d'IBM Remote API Client avant d'installer ce logiciel. Ce fichier se trouve dans le répertoire **/ibm-commserver-clients/aix** du CD d'installation.

Configuration matérielle et logicielle

Configuration matérielle

IBM Remote API Client requiert un système pSeries pris en charge par l'un des systèmes d'exploitation AIX répertoriés dans «Version du système d'exploitation».

Version du système d'exploitation

La version en cours d'IBM Remote API Client a été testée avec les versions ci-dessous du système d'exploitation.

- AIX v5.2–ML5
- AIX v5.3–ML1

Java

Pour utiliser l'API CPI-C Java, le logiciel Java est nécessaire. Le kit SDK Java 1.4.2 disponible à l'adresse http://www.ibm.com/developerworks/java/jdk est conforme à toutes les conditions requises. Java est disponible en 64 bits, mais l'API CPI-C Java requiert la machine JVM 32 bits.

Installez le package SDK Java avec la commande **installp**.

GSKIT

Si le client se connecte aux serveurs CS/AIX par HTTPS, le logiciel GSKIT est nécessaire pour l'accès HTTPS aux serveurs via un serveur WebSphere. Pour plus d'informations, voir le fichier **README** dans le répertoire **/ibm-commserver-clients/aix** du CD d'installation. Le logiciel GSKIT est installé lors du processus d'installation du client principal (procédure décrite plus loin dans ce chapitre).

Modification de la variable d'environnement relative à la langue

Lorsque vous utilisez Remote API Client, vérifiez que la valeur de la variable `LANG` n'est pas `C`.

Pour afficher la valeur de la variable `LANG` utilisée ou la modifier, procédez comme suit :

1. Dans le menu SMIT principal, sélectionnez **Environnements système**.

2. Dans le menu SMIT suivant, sélectionnez **Gestion des langues**.
3. Dans le menu SMIT suivant, sélectionnez **Modif./Aff. environnement de la langue principale**.
4. Dans le menu SMIT suivant, sélectionnez **Choix des conventions, de la langue et du clavier**.
5. Sélectionnez la langue voulue. Par exemple, si vous utilisez des messages en français, sélectionnez `fr_FR`.

Installation de Remote API Client sous AIX

Après avoir installé les logiciels prérequis, vous pouvez installer IBM Remote API Client.

Si un niveau antérieur d'IBM Remote API Client est déjà installé, suivez la procédure décrite dans la section «Désinstallation de Remote API Client sous AIX», à la page 69 pour le désinstaller avant d'installer le nouveau niveau. Toutes les données de configuration seront conservées pour être utilisées avec la nouvelle installation.

Installation de Remote API Client en copiant les fichiers sur votre poste de travail AIX

Pour installer Remote API Client, procédez comme suit.

1. Copiez (ou récupérez par FTP) le fichier **sna.client.6.3.0.0.bff** qui se trouve dans le répertoire **/ibm-commserver-clients/aix** du CD-ROM vers le poste de travail AIX. Veillez à utiliser le mode binaire pour copier le fichier ou le transférer par FTP.

   Si le client va se connecter aux serveurs CS/AIX par HTTPS, vous devez également copier (ou transférer par FTP) les fichiers **gskta.*.I** et **gsksa.*.I** placés dans le même répertoire du CD. Ces fichiers contiennent le logiciel GSKIT requis pour l'accès HTTPS depuis le client.
2. Connectez-vous au poste de travail AIX en tant qu'utilisateur root.
3. Installez le client AIX avec **installp** ou **smit**.

   Pour effectuer l'installation avec **installp**, utilisez la commande suivante. (L'option `Y` accepte le contrat de licence.)

   installp -aYd sna.client.6.3.0.0.bff all

   Pour effectuer l'installation avec **smit**, utilisez la commande suivante pour lancer le programme d'installation.

   smit install_selectable_all
4. Si le client va se connecter aux serveurs CS/AIX par HTTPS, installez les fichiers GSKIT de façon similaire.
5. A la fin du processus d'installation, vous pouvez supprimer le fichier **sna.client.6.3.0.0.bff** et les fichiers GSKIT du répertoire de travail.
6. Lancez IBM Remote API Client. Après l'installation, le démarrage est automatiquement effectué lors de l'amorçage de l'ordinateur.

   cd /
   sna start

Remarque : Pour connecter IBM Remote API Client aux serveurs par HTTPS, vous devez utiliser le programme de gestion des clés GSKIT pour configurer les certificats de sécurité sur le client. Pour plus de détails,

reportez-vous à la section «Configuration des certificats de sécurité HTTPS à l'aide de GSKIT», à la page 68.

Vous devez également mettre à jour le fichier de données de réseau du client afin d'indiquer les serveurs CS/AIX auxquels le client peut se connecter et le nom du serveur WebSphere qui assure le support HTTPS. Pour plus d'informations, voir la section sur la gestion des clients Remote API Client dans le manuel *Communications Server for AIX Administration Guide*.

Installation de Remote API Client à partir du CD

Pour installer Remote API Client, procédez comme suit.

1. Connectez-vous au poste de travail AIX en tant qu'utilisateur root.
2. Montez le CD sur le poste de travail AIX à l'aide de la commande suivante.

   mount -o ro /dev/cd0 /mnt
3. Installez le client AIX avec **installp** ou **smit**.

   Pour effectuer l'installation avec **installp**, utilisez la commande suivante. (L'option `Y` accepte le contrat de licence.)

   installp -aYd /mnt/ibm-commserver-clients/aix sna.client

   Pour effectuer l'installation avec **smit**, utilisez la commande suivante pour lancer le programme d'installation.

   smit install_selectable_all
4. Si le client va se connecter aux serveurs CS/AIX par HTTPS, installez les fichiers GSKIT de façon similaire.
5. A la fin du processus d'installation, démontez le CD à l'aide de la commande suivante.

   unmount /mnt
6. Lancez IBM Remote API Client. Après l'installation, le démarrage est automatiquement effectué lors de l'amorçage de l'ordinateur. Veillez à ne pas effectuer cette opération à partir d'un répertoire du CD.

   cd /
   sna start

Remarque : Pour connecter IBM Remote API Client aux serveurs par HTTPS, vous devez utiliser le programme de gestion des clés GSKIT pour configurer les certificats de sécurité sur le client. Pour plus de détails, reportez-vous à la section «Configuration des certificats de sécurité HTTPS à l'aide de GSKIT», à la page 68.

Vous devez également mettre à jour le fichier de données de réseau du client afin d'indiquer les serveurs CS/AIX auxquels le client peut se connecter et le nom du serveur WebSphere qui assure le support HTTPS. Pour plus d'informations, voir la section sur la gestion des clients Remote API Client dans le manuel *Communications Server for AIX Administration Guide*.

Configuration des certificats de sécurité HTTPS à l'aide de GSKIT

Pour connecter IBM Remote API Client aux serveurs par HTTPS, vous devez utiliser le logiciel de gestion des clés GSKIT pour configurer les certificats de sécurité sur le client. Procédez comme suit.

1. Lancez le gestionnaire de clés GSKIT à l'aide de la commande suivante :

   /usr/bin/snakeyman

   Sur l'interface utilisateur du gestionnaire de clés, ouvrez le fichier de base de données de clés **/etc/sna/ibmcs.kdb**, qui est au format CMS.
2. Le mot de passe initial de la base de données de clés est `ibmcs`. Avant de configurer les certificats de sécurité, **modifiez ce mot de passe** afin d'assurer la sécurité de votre configuration. Dans la boîte de dialogue de modification du mot de passe, cochez la case 'Stocker le mot de passe dans un fichier ?' pour sauvegarder le nouveau mot de passe afin que le client puisse ouvrir la base de données de clés.
3. Récupérez une copie du certificat de l'autorité de certification utilisé pour signer le certificat de sécurité du serveur Web, puis installez-la dans la base de données de clés. Pour cela, sélectionnez Certificats signataires sur l'interface utilisateur du gestionnaire de clés et cliquez sur Ajouter.
4. Si le serveur WebSphere est configuré de façon à rendre obligatoire les certificats de sécurité du client, celui-ci doit disposer d'un certificat fourni par une autorité de certification ayant elle-même un certificat répertorié dans la base de données des certificats de sécurité du serveur Web. Pour demander un nouveau certificat :
   a. Sélectionnez Créer, Nouvelle demande de certificat sur l'interface utilisateur du gestionnaire de clés, puis indiquez les informations demandées.
   b. Enregistrez le certificat, extrayez-le dans un fichier et envoyez-le à l'autorité de certification.
   c. Lorsque le certificat est généré, placez-le dans la base de données du serveur Web. Pour cela, sélectionnez Certificats personnels sur l'interface utilisateur du gestionnaire de clés et cliquez sur Recevoir.

   Pour effectuer un contrôle interne, vous pouvez créer un certificat client auto-signé au lieu de récupérer un certificat auprès de l'autorité de certification. Cependant, cela n'assure pas le niveau de sécurité optimal et ne doit pas être appliqué sur un système connecté. Pour créer un certificat auto-signé :
   a. Sélectionnez Créer, Nouveau certificat auto-signé sur l'interface du gestionnaire de clés, et indiquez les informations demandées.
   b. Enregistrez le certificat et extrayez-le dans un fichier.
   c. Placez le fichier du certificat dans la base de données du serveur Web. Pour cela, sélectionnez Certificats personnels sur l'interface utilisateur du gestionnaire de clés et cliquez sur Recevoir.
5. Quittez le gestionnaire de clés GSKIT à la fin de la configuration des certificats.

Désinstallation de Remote API Client sous AIX

Pour désinstaller Remote API Client, vous pouvez utiliser les commandes suivantes.

1. Si le logiciel client est en cours d'exécution, arrêtez-le à l'aide de la commande suivante.

   sna stop

2. Connectez-vous avec les droits d'accès ″root″.
3. Supprimez le package Remote API Client et les packages logiciels associés à l'aide de l'une des commandes suivantes.

   Pour supprimer le package avec **installp** :

   installp —u sna.client

   Pour supprimer le package avec **smit** :

   smit remove

Désinstallation de Remote API Client sous AIX

Chapitre 8. Préparation et installation de Remote API Client sous Windows

Ce chapitre explique comment installer IBM Remote API Client sous Windows, lequel permet d'exécuter des applications SNA sur un PC sans devoir effectuer une installation SNA complète en pile sur le PC. Remote API Client sous Windows peut se connecter à un ou plusieurs serveurs CS/AIX (ou serveurs CS Linux) via un réseau TCP/IP.

Les interfaces disponibles avec IBM Remote API Client sous Windows sont compatibles avec celles d'IBM Communications Server pour Windows et Microsoft Host Integration Server.

Le kit SDK (Software Development Kit) IBM Remote API Client sous Windows (SDK) est un package en option qui permet d'utiliser Remote API Client pour développer les programmes d'application à l'aide des API APPC, CPI-C, LUA et CSV. Pour plus d'informations sur ces API, consultez le guide de programmation correspondant (Programmer's reference guide). Il n'est pas nécessaire d'installer ce package si vous utilisez Remote API Client uniquement pour exécuter des applications existantes (si vous n'en développez pas des nouvelles).

Configuration matérielle et logicielle

Pour exécuter le programme d'**installation** et Remote API Client sous Windows, l'ordinateur doit remplir les conditions suivantes :

- Il doit exécuter l'un des systèmes d'exploitation suivants :
  - Windows 2000
  - Windows XP
  - Windows Server 2003
- Il doit avoir accès à un ou plusieurs serveurs CS/AIX par l'un des moyens suivants :
  - Accès au serveur sur un réseau TCP/IP
  - Accès à un serveur WebSphere fournissant l'accès HTTPS aux serveurs CS/AIX (dans ce cas le logiciel GSKIT doit y être installé durant le processus d'installation du client).

Accès au programme d'installation

Remote API Client, le kit SDK, le logiciel GSKIT et le programme d'**installation** sont fournis sur le CD d'installation au format Windows. Vous pouvez donc les installer sur l'ordinateur Windows à partir du CD. Vous devez installer le logiciel Remote API Client sur chaque PC client Windows. Le kit SDK est nécessaire si vous envisagez d'utiliser le client pour développer de nouvelles applications à l'aide des API distantes Windows, mais pas si vous envisagez de l'utiliser uniquement pour exécuter des applications existantes. Le logiciel GSKIT est nécessaire uniquement pour permettre au client d'accéder aux serveurs CS/AIX par HTTPS.

L'image d'installation de Remote API Client sous Windows est un fichier exécutable ZIP auto-extractible appelé **i_w32cli.exe**, qui se trouve dans le répertoire **/ibm-commserver-clients/windows** du CD d'installation. Vous pouvez copier ce

fichier sur d'autres PC Windows par le réseau, et ainsi effectuer l'installation sans accès direct au CD CS/AIX. Lors de son exécution, ce fichier exécutable décompresse l'image d'installation et exécute automatiquement le programme d'**installation**. Si vous souhaitez simplement extraire l'image d'installation dans un répertoire temporaire, par exemple, pour exécuter le programme d'**installation** en ligne de commande, vous pouvez charger le fichier exécutable ZIP auto-extractible dans votre programme d'extraction.

Lors de la première exécution du programme d'**installation** sur un ordinateur particulier, le programme est exécuté à partir de la source sélectionnée. Le programme gère entièrement le processus d'installation, définit la configuration de base et il crée une icône de raccourci. Après l'installation, vous pouvez réinstaller le logiciel à l'aide du programme d'**installation** (en le sélectionnant dans le Gestionnaire de fichiers ou en sélectionnant son icône).

Une fois l'image d'installation de Remote API Client extraite dans un répertoire temporaire, vous pouvez installer le logiciel de deux manières :

- Exécutez le programme d'**installation** Windows, comme décrit dans «Installation de Remote API Client sous Windows à l'aide du programme d'installation». Utilisez cette méthode si vous souhaitez installer le kit SDK.
- Entrez la commande **setup** en ligne de commande, comme décrit dans «Installation du logiciel Remote API Client à partir de la ligne de commande», à la page 76. Cette méthode ne permet pas d'installer le kit SDK.

Remarque : Pour connecter IBM Remote API Client aux serveurs par HTTPS, installez le logiciel GSKIT et utilisez le programme de gestion des clés GSKIT pour définir la configuration des certificats de sécurité sur le client. Pour plus d'informations, voir «Installation du logiciel GSKIT et configuration des certificats de sécurité», à la page 78 et «Configuration des certificats de sécurité HTTPS à l'aide de GSKIT», à la page 79.

Vous devez également mettre à jour le fichier de données de réseau du client afin d'indiquer les serveurs CS/AIX auxquels le client peut se connecter et le nom du serveur WebSphere qui assure le support HTTPS. Pour plus d'informations, voir la section sur la gestion des clients Remote API Client dans le manuel *Communications Server for AIX Administration Guide*.

Installation de Remote API Client sous Windows à l'aide du programme d'installation

Exécutez le programme d'**installation**, soit automatiquement à partir du fichier exécutable ZIP auto-extractible **i_w32cli.exe**, soit manuellement en ligne de commande. Le premier programme affiche la fenêtre de sélection de la langue.

1. Sélectionnez la langue à utiliser pour l'installation et la configuration de Remote API Client, puis cliquez sur **OK**.

   Le programme affiche l'écran de bienvenue du programme d'**installation**.
2. Cliquez sur **Suivant** pour continuer l'installation.

   Le programme affiche le contrat de licence du logiciel que vous devez lire et accepter.
3. Si vous acceptez les termes du contrat de licence, cliquez sur **Accepter**.

Le programme vous invite ensuite à indiquer le répertoire de destination dans lequel installer les fichiers.

4. Entrez le répertoire de destination.

   Ensuite, choisissez le type d'installation :

   Typique
   Inclure les fichiers qui sont en général nécessaires à une utilisation normale. Cette option convient pour la plupart des utilisateurs.

   Compacte
   Inclure uniquement les ensembles de fichiers requis pour exécuter Remote API Client. Choisissez cette option pour réduire au maximum l'espace disque occupé par les fichiers du client.

   Personnalisée
   Personnaliser l'installation en sélectionnant les fichiers dont vous avez besoin.

   Remarque : Si vous souhaitez installer le kit SDK, choisissez **Personnalisée**.

5. Choisissez le type d'installation.

   Si vous choisissez **Personnalisée**, le programme permet de sélectionner les fichiers programme Remote API Client sous Windows, le kit SDK, ou les deux. Choisissez les fichiers à installer.

   Quel que soit le type d'installation choisi, le programme vous invite à entrer le nom du dossier de programmes dans lequel vous souhaitez placer les icônes de Remote API Client sous Windows.

6. Entrez le nom du dossier.

7. Si le répertoire système contient des fichiers **.DLL** d'autres programmes portant le même nom que certains fichiers utilisés par le programme d'**installation** de Remote API Client (par exemple, des fichiers d'un autre logiciel SNA), un message vous indique d'effectuer l'une des opérations suivantes :

   - Copier les fichiers **.DLL** de Remote API Client en remplaçant les fichiers **.DLL** existants
   - Copier les fichiers **.DLL** existants dans un sous-répertoire appelé **OTHERSNA** dans le répertoire d'installation, puis installer les fichiers **.DLL** de Remote API Client. Cette option vous permet de restaurer la configuration initiale tel qu'elle était avant l'installation de Remote API Client si vous désinstallez celui-ci ultérieurement (voir «Désinstallation du logiciel Remote API Client», à la page 81).
   - Annuler l'installation du logiciel client.

   Si les fichiers **.DLL** de Remote API Client sont déjà présents, le programme d'**installation** vous l'indique dans un message. Les nouveaux fichiers **.DLL** remplacent les fichiers **.DLL** existants uniquement si le numéro de version des fichiers existants est inférieur à celui des fichiers **.DLL** du programme d'**installation**.

8. A ce stade, le programme d'**installation** copie les fichiers depuis la source indiquée et les installe à l'emplacement approprié. Durant ce processus, une barre de progression de l'installation indique le pourcentage effectué. Les fichiers **.DLL** sont copiés dans le répertoire système, ou un répertoire équivalent, et les autres fichiers sont copiés dans le répertoire de destination que vous avez indiqué à l'étape 2. Le transfert de chaque fichier est consigné dans le fichier **setup.log** qui est créé dans le répertoire que vous avez indiqué. Si les fichiers dans lesquels des données doivent être écrites sont en «lecture

seule», ou si des fichiers ne peuvent pas être copiés pour une raison ou une autre, les nouveaux fichiers sont supprimés et un message vous indique de consulter le fichier **setup.log**.

9. Si la source à partir de laquelle vous exécutez le programme d'**installation** ne contient pas tous les fichiers nécessaires, le programme vous invite à indiquer le nom d'un répertoire. Entrez le nom du répertoire dans lequel se trouvent les fichiers nécessaires.

   Si les informations indiquées sont insuffisantes pour localiser les copies des fichiers Remote API Client, le programme affiche à nouveau cette fenêtre.

10. Une fois les fichiers nécessaires copiés, le programme d'**installation** affiche la fenêtre de Configuration.

    Les valeurs de la configuration par défaut proviennent du fichier de configuration du domaine. Pour plus d'informations, voir le manuel *Communications Server for AIX Administration Guide*. Si vous ne souhaitez pas utiliser ces valeurs par défaut, vous pouvez les configurer de la manière suivante :

    Domaine
    Indiquez le nom du domaine client-serveur CS/AIX.

    Les paramètres suivants sont facultatifs :

    Nom du serveur
    Cette fenêtre affiche une liste contenant jusqu'à neuf serveurs auxquels ce client peut se connecter. Les serveurs apparaissent dans la liste dans l'ordre selon lequel le client les sélectionne. Si le client ne peut pas se connecter au premier serveur de la liste, il tente de se connecter au suivant.

    - Pour ajouter un nouveau serveur à la liste, utilisez le bouton **Ajouter**.
    - Pour supprimer un serveur de la liste, sélectionnez le serveur et sélectionnez le bouton **Supprimer**.
    - Pour déplacer un serveur dans la liste vers le haut ou le bas, sélectionnez-le et faites glisser le curseur.

    Si le client se trouve sur le même réseau privé que ses serveurs et accède à ceux-ci par TCP/IP, chaque serveur est identifié simplement par son nom de serveur.

    Si le client accède aux serveurs par HTTPS, vous devez identifier chaque serveur en indiquant le nom du serveur WebSphere qui fournit le support HTTPS et le nom du serveur CS/AIX, au format suivant :

    nomserveurweb **:** *nomserveur1*

    Cela suppose que WebSphere est configuré de façon à utiliser le port par défaut 443 pour les connexions HTTPS. Si votre administrateur réseau a configuré WebSphere de façon à utiliser un autre numéro de port, indiquez celui-ci au format suivant :

    nomserveurweb **:** *numeroport* **:** *nomserveur1*

    Pour plus d'informations sur la configuration de WebSphere pour la prise en charge des connexions HTTPS, voir «Configuration de WebSphere Application Server», à la page 39.

    Diffusions UDP
    Indiquez si ce client va utiliser les diffusions UDP pour se connecter à

un serveur. Si vous sélectionnez cette option, le client envoie les diffusions UDP sur le réseau pour localiser une connexion serveur au lieu de tenter directement la connexion à un serveur particulier.

Par défaut, l'option de diffusions UDP est activée. Pour modifier ce paramètre, cliquez sur la case.

Avancé Pour indiquer d'autres valeurs supplémentaires à la place des paramètres par défaut définis par le programme d'**installation**, cliquez sur le bouton **Options avancées** au bas de la fenêtre. Le programme d'**installation** affiche la fenêtre Options avancées qui contient les paramètres de la configuration du client Windows. La plupart des utilisateurs peuvent utiliser les paramètres par défaut, il n'est donc pas nécessaire de les modifier.

Pour plus d'informations sur ces paramètres, voir «Options avancées de configuration de Remote API Client».

Pour plus d'informations sur les différents paramètres de configuration, cliquez sur **Aide**.

11. Une fois les paramètres de configuration définis dans cette fenêtre, cliquez sur **OK**. Si les paramètres de cette fenêtre ne sont pas correctement définis, le programme d'**installation** affiche un message.
12. Lorsque l'installation est correctement effectuée, la dernière fenêtre s'affiche. Vous pouvez choisir l'une ou l'autre des actions à effectuer après la fermeture du programme d'installation :

    Lire le fichier README
    Lire le fichier **README**.

    Lancer le client
    Lancer l'exécution du client CS/AIX.

    Sélectionnez **Terminer** pour quitter le programme d'installation.

Options avancées de configuration de Remote API Client

La fenêtre Options avancées vous permet de configurer certains paramètres avancés de Remote API Client. La plupart des utilisateurs n'ont pas besoin de modifier ces paramètres mais vous pouvez modifier les paramètres par défaut si cela est nécessaire.

Délai d'accès au réseau local
Indiquez le délai en secondes durant lequel la connexion entre un client et un serveur peut rester inactive avant d'être fermée. Si cette option n'est pas cochée, aucun délai d'accès au réseau local n'a été défini (aucune limite n'est donc appliquée). Si vous cochez cette option, vous pouvez indiquer une valeur en secondes dans la zone correspondante. La valeur minimale est `60` (60 secondes). Si vous n'indiquez aucune valeur ou si la valeur indiquée est inférieure à `60`, Remote API Client applique la valeur minimale `60`.

Nb maximal de tentatives de diffusion
Indiquez le nombre maximal de tentatives du client pour se connecter à un serveur par diffusion. Sur la fenêtre Options avancées, la valeur par défaut affichée est `5`. La valeur de cette option est appliquée uniquement lorsque l'option Diffusions UDP est cochée dans la fenêtre Configuration principale.

Délai avant reconnexion
Indiquez le délai en secondes durant lequel le client attend avant une tentative de reconnexion à un serveur lorsque celui-ci est devenu inactif. Sur la fenêtre Options avancées, la valeur par défaut affichée est `200`.

Pour plus d'informations sur ces paramètres, sélectionnez **Aide**.

Une fois les Options avancées définies, cliquez sur **OK**. Si les paramètres de cette fenêtre sont correctement définis, le programme d'**installation** affiche à nouveau la fenêtre Configuration. S'il s'agit de la première installation de Remote API Client, passez à l'étape 11, à la page 75. Sinon, cliquez sur **OK** dans la fenêtre Configuration pour terminer la configuration.

Installation du logiciel Remote API Client à partir de la ligne de commande

Remarque : Si vous souhaitez installer le kit SDK, vous devez utiliser le programme d'**installation** , comme décrit dans «Installation de Remote API Client sous Windows à l'aide du programme d'installation», à la page 72. Il est impossible d'installer le kit SDK à partir de la ligne de commande.

Après l'extraction de l'image d'installation de Remote API Client dans un répertoire temporaire, vous pouvez installer le logiciel à partir de la ligne de commande au lieu d'utiliser le programme d'**installation** sous Windows : Sur la ligne de commande, entrez la commande **setup** en indiquant une ou plusieurs options. Vous pouvez entrer ces options en majuscules ou en minuscules et insérer une barre oblique / ou un trait d'union - avant ces options. Si un paramètre, tel que *dossier*, est une chaîne contenant un espace, vous devez mettre la chaîne entre guillemets doubles.

Une fois la commande **setup** entrée, le programme d'**installation** vous invite à indiquer les données que vous n'avez pas indiquées sur la ligne de commande, puis il affiche les messages de confirmation lors des différentes étapes de l'installation et la configuration. Si vous ne souhaitez pas afficher les messages du programme d'**installation**, utilisez l'option **-accept -s** pour exécuter le programme en mode silencieux, en acceptant les termes du contrat de licence du logiciel.

Les options de la commande **setup** sont les suivantes :

-? Affiche la liste des options en ligne de commande. Cette option est équivalente à l'option **-h**.

-h Affiche la liste des options en ligne de commande. Cette option est équivalente à l'option **-?**

-accept -s
Exécuter l'installation en mode silencieux, en acceptant les termes du contrat de licence du logiciel. Vous pouvez consulter ce contrat dans le sous-répertoire **license** de l'image d'installation Windows.

L'option **-s** doit être placée en dernier sur la ligne de commande, et vérifiez bien le nom de domaine (indiqué à l'aide de l'option **-i**) ainsi que les autres paramètres indiqués. Lors d'une installation en mode silencieux, aucun paramètre n'est demandé et aucun message de confirmation n'est affiché. Les arguments indiqués après l'option **-s** sur la ligne de commande ne seront pas pris en compte.

-f2 Indiquez le chemin d'accès complet du fichier journal de l'installation qui va être créé lors de l'installation en mode silencieux (à l'aide de l'option **-s**).

Si vous ne définissez pas cette option, le fichier **setup.log** sera créé dans le répertoire où est exécuté le programme d'installation. Si l'installation est effectuée en mode silencieux à partir de l'unité de CD-ROM, vous devez définir cette option afin de créer le fichier sur votre ordinateur (car il ne pourra pas être créé sur l'unité de CD-ROM).

-k*dossier*
Indiquer le dossier du programme.

-p*répertoire*
Indiquer le répertoire d'installation.

-i*domaine*
Indiquer le nom de domaine de ce client. Ce paramètre est obligatoire, aucune valeur par défaut n'est définie.

-w*répertoire*
Indiquer le répertoire source contenant les fichiers du logiciel client CS/AIX si la source est placée sur un disque ou un CD. Sinon, utilisez l'option **-v**.

-v*serveur*
Indiquer le serveur à partir duquel les fichiers du logiciel doivent être téléchargés. Vous pouvez indiquer le nom du serveur ou bien l'adresse TCP/IP. Si vous copiez les fichiers source à partir d'un disque ou d'un CD, utilisez l'option **-w** à la place de l'option **-v**.

-l*serveur*
Indiquer le serveur à inclure dans la liste de serveurs auquel ce client peut accéder.

Si le client se trouve sur le même réseau privé que ses serveurs et accède à ceux-ci par TCP/IP, chaque serveur est identifié simplement par son nom de serveur.

Si le client accède aux serveurs par HTTPS, vous devez identifier chaque serveur en indiquant le nom du serveur WebSphere qui fournit le support HTTPS et le nom du serveur CS/AIX, au format suivant :

nomserveurweb **:** *nomserveur1*

Cela suppose que WebSphere est configuré de façon à utiliser le port par défaut 443 pour les connexions HTTPS. Si votre administrateur réseau a configuré WebSphere de façon à utiliser un autre numéro de port, indiquez celui-ci au format suivant :

nomserveurweb **:** *numeroport* **:** *nomserveur1*

Pour plus d'informations sur la configuration de WebSphere pour la prise en charge des connexions HTTPS, voir «Configuration de WebSphere Application Server», à la page 39.

-o Ecraser les fichiers **.DLL** existants. Si les fichiers **.DLL** de Remote API Client sont déjà présents, le programme d'**installation** les écrase même si leur numéro de version est supérieur à celui des fichiers **.DLL** du programme d'**installation**.

-y Enregistrer les fichiers **.DLL** existants. Si les fichiers **.DLL** de Remote API Client existent déjà dans les répertoires appropriés, le programme

d'**installation** copie ces fichiers **.DLL** dans un sous-répertoire du répertoire d'installation, puis installe les fichiers **.DLL** de Remote API Client. La copie dans le sous-répertoire permet de désinstaller le logiciel Remote API Client de façon complète.

-n Annuler l'installation si des fichiers **.DLL** de Remote API Client sont détectés dans le répertoire d'installation.

-a*délai* Indiquer le délai d'accès au réseau local en secondes. Il s'agit de la durée durant laquelle une connexion entre un client et un serveur peut rester inactive avant d'être fermée. Si vous indiquez la valeur `0`, aucun délai n'est appliqué.

-b*nb-max-diffusion*
Indiquer le nombre maximal de tentatives de diffusion UDP. La diffusion UDP permet à un client de tenter la connexion sur n'importe quel serveur du domaine au lieu de la tenter sur un serveur en particulier. Si vous indiquez la valeur `0`, aucune diffusion n'est tentée.

-j*délai-reconnexion*
Indiquer le délai en secondes durant lequel le client attend avant une tentative de reconnexion à un serveur lorsque celui-ci est devenu inactif.

-u N'installe pas certains fichiers requis pour la prise en charge HTTPS. Cette option peut être utilisée lorsque l'espace disque est limité et si HTTPS n'est pas nécessaire.

Installation du logiciel GSKIT et configuration des certificats de sécurité

Pour permettre la connexion d'IBM Remote API Client aux serveurs par HTTPS, vous devez installer le logiciel GSKIT pour gérer les certificats de sécurité. Procédez de la manière suivante :

1. Créez un répertoire temporaire sur l'ordinateur Windows destiné à recevoir les fichiers d'installation.
2. Sur une fenêtre de commande, accédez au répertoire dans lequel vous avez installé le logiciel client, c'est-à-dire **C:\IBMCS\w32cli** sauf si vous avez choisi un autre emplacement lors de l'installation du client.
3. Exécutez la commande suivante pour extraire les fichiers d'installation :

   gsk7bas *rep_temp* /D

   rep_temp est le chemin d'accès complet au répertoire temporaire que vous avez créé durant la première étape.
4. Accédez au répertoire temporaire et exécutez la commande suivante pour lancer le programme d'installation :

   setup sxclient

   Suivez les instructions à l'écran pour installer le logiciel GSKIT.
5. Une fois l'installation terminée, supprimez le répertoire temporaire que vous avez créé durant la première étape, ainsi que son contenu.

Vous pouvez maintenant configurer les certificats de sécurité comme décrit dans la section suivante.

Si vous devez effectuer une installation automatisée (par exemple, si vous installez le logiciel GSKIT sur plusieurs ordinateurs client et souhaitez créer un fichier de

commandes pour automatiser le processus), utilisez la commande suivante pour exécuter le programme d'installation en mode silencieux :

setup sxclient -s

Cette commande installe le logiciel sans afficher l'interface utilisateur du programme et sans que l'utilisateur ait besoin de saisir des données. Les paramètres par défaut de l'installation sont récupérés dans le fichier **SETUP.ISS**, qui se trouve parmi les fichiers extraits dans le répertoire temporaire au début du processus d'installation. Si vous souhaitez changer le répertoire d'installation du logiciel GSKIT, vous pouvez modifier le fichier **SETUP.ISS** avec un éditeur de texte après l'extraction des fichiers dans le répertoire temporaire. Vous pouvez utiliser les fichiers de ce répertoire, y compris ce fichier mis à jour, pour effectuer l'installation sur d'autres ordinateurs client au lieu d'extraire les fichiers et modifier le répertoire d'installation à chaque fois.

Configuration des certificats de sécurité HTTPS à l'aide de GSKIT

Pour connecter IBM Remote API Client aux serveurs par HTTPS, vous devez utiliser le logiciel de gestion des clés GSKIT pour configurer les certificats de sécurité sur le client. Procédez comme suit.

1. Lancez le programme de gestion des clés qui se trouve dans **C:\IBMCS\w32cli\snakeyman.exe** ou dans le répertoire que vous avez choisi lors de l'installation du client. .

   Sur l'interface utilisateur du gestionnaire de clés, ouvrez le fichier de base de données de clés *installdir***ibmcs.kdb**, qui est au format CMS. *installdir* représente le répertoire dans lequel vous avez installé le logiciel client, c'est-à-dire **C:\IBMCS\w32cli** ou l'emplacement que vous avez choisi lors de l'installation du client.
2. Le mot de passe initial de la base de données de clés est `ibmcs`. Avant de configurer les certificats de sécurité, **modifiez ce mot de passe** afin d'assurer la sécurité de votre configuration. Dans la boîte de dialogue de modification du mot de passe, cochez la case 'Stocker le mot de passe dans un fichier ?' pour sauvegarder le nouveau mot de passe afin que le client puisse ouvrir la base de données de clés.
3. Récupérez une copie du certificat de l'autorité de certification utilisé pour signer le certificat de sécurité du serveur Web, puis installez-la dans la base de données de clés. Pour cela, sélectionnez Certificats signataires sur l'interface utilisateur du gestionnaire de clés et cliquez sur Ajouter.
4. Si le serveur WebSphere est configuré de façon à rendre obligatoire les certificats de sécurité du client, celui-ci doit disposer d'un certificat fourni par une autorité de certification ayant elle-même un certificat répertorié dans la base de données des certificats de sécurité du serveur Web. Pour demander un nouveau certificat :
   a. Sélectionnez Créer, Nouvelle demande de certificat sur l'interface utilisateur du gestionnaire de clés, puis indiquez les informations demandées.
   b. Enregistrez le certificat, extrayez-le dans un fichier et envoyez-le à l'autorité de certification.
   c. Lorsque le certificat est généré, placez-le dans la base de données du serveur Web. Pour cela, sélectionnez Certificats personnels sur l'interface utilisateur du gestionnaire de clés et cliquez sur Recevoir.

   Pour effectuer un contrôle interne, vous pouvez créer un certificat client auto-signé au lieu de récupérer un certificat auprès de l'autorité de certification.

Cependant, cela n'assure pas le niveau de sécurité optimal et ne doit pas être appliqué sur un système connecté. Pour créer un certificat auto-signé :

a. Sélectionnez Créer, Nouveau certificat auto-signé sur l'interface du gestionnaire de clés, et indiquez les informations demandées.
b. Enregistrez le certificat et extrayez-le dans un fichier.
c. Placez le fichier du certificat dans la base de données du serveur Web. Pour cela, sélectionnez Certificats personnels sur l'interface utilisateur du gestionnaire de clés et cliquez sur Recevoir.

5. Quittez le gestionnaire de clés GSKIT à la fin de la configuration des certificats.

Personnalisation du logiciel Remote API Client après installation

Vous pouvez modifier chacun des paramètres personnalisés à tout moment après l'installation initiale en exécutant le programme **Utilitaire de configuration**, lequel se trouve dans le groupe de programmes CS/AIX. Le programme affiche la même fenêtre de configuration qui que celle affichée durant le processus d'installation initial. Vous pouvez changer les données dans chacune des zones en suivant la procédure indiquée dans «Installation de Remote API Client sous Windows à l'aide du programme d'installation», à la page 72.

Si vous n'avez pas installé les fichiers du kit SDK durant l'installation initiale, vous pouvez les ajouter maintenant en exécutant à nouveau le programme d'installation. Choisissez l'installation **Personnalisée** et sélectionnez le package SDK.

Réinstallation du logiciel Remote API Client

Vous pouvez réinstaller le logiciel Remote API Client à tout moment, par exemple pour mettre à niveau le logiciel.

Pour cela, exécutez le programme d'installation en suivant les instructions de la section «Installation de Remote API Client sous Windows à l'aide du programme d'installation», à la page 72 ou «Installation du logiciel Remote API Client à partir de la ligne de commande», à la page 76. Le programme d'**installation** indique l'emplacement à partir duquel ont été copiés les fichiers du logiciel client durant l'installation initiale. Cliquez sur **OK** pour obtenir une nouvelle copie des fichiers à partir du même emplacement. Si vous cliquez sur **OK**, le programme d'**installation** copie les fichiers et affiche la fenêtre Options.

Remarque : Lors d'une réinstallation du logiciel Remote API Client en mode silencieux (voir section «Installation du logiciel Remote API Client à partir de la ligne de commande», à la page 76), il peut être nécessaire de redémarrer l'ordinateur pour terminer l'installation. En effet, certains fichiers programme peuvent été utilisés durant le processus d'installation (par exemple, si Remote API Client est en cours d'exécution), dans ce cas ils n'ont pas été remplacés par les nouveaux fichiers. Les nouveaux fichiers sont alors copiés dans un répertoire temporaire et sont ensuite déplacés automatiquement lors du redémarrage de l'ordinateur.

Pour vérifier si vous devez redémarrer l'ordinateur, utilisez un éditeur de texte tel que **Notepad** pour visualiser le contenu du fichier journal de l'installation une fois le processus d'installation terminé. Le fichier journal d'installation (nommé **setup.log**) est créé dans le répertoire à partir duquel vous exécutez le programme d'installation, sauf si vous

avez utilisé l'option en ligne de commande **-f2** pour définir un autre chemin d'accès ou un autre nom de fichier.

A la fin du fichier, sous `Response Result`, le texte `Result Code` doit être suivi d'une ou deux valeurs `0` (zéro) ou `-12`. Si la valeur est `0`, il n'est pas nécessaire de redémarrer l'ordinateur. Si la valeur est `-12`, redémarrez l'ordinateur avant d'utiliser le client Windows.

Désinstallation du logiciel Remote API Client

Vous pouvez désinstaller le logiciel Remote API Client à tout moment, en utilisant l'option **Supprimer** du Panneau de configuration de Windows. Après la confirmation du processus de désinstallation, Windows effectue les opérations suivantes :

- Suppression de tous les fichiers installés.
- Si des fichiers **.DLL** ont été sauvegardés dans un sous-répertoire durant l'installation initiale, ces fichiers sont restaurés dans l'emplacement d'origine.
- Suppression du sous-répertoire dans lequel les fichiers **.DLL** ont été sauvegardés si ce sous-répertoire est vide.
- Suppression du dossier programme et du répertoire créé, s'ils sont vides.
- Si la désinstallation est réussie, suppression du fichier **setup.log**, lequel indique tous les fichiers transférés et supprimés.
- Affichage d'un message indiquant que la désinstallation est réussie ou bien que l'utilisateur doit vérifier le fichier **setup.log** car une erreur s'est produite durant l'installation.

Le bouton **Quitter** permet de retourner sous Windows.

Si vous avez installé le logiciel GSKIT pour l'utiliser avec Remote API Client sous Windows et si aucune autre application ne l'utilise, vous pouvez également désinstaller ce logiciel (voir «Désinstallation du logiciel GSKIT»).

Désinstallation du logiciel GSKIT

Si vous avez installé le logiciel GSKIT pour l'utiliser avec Remote API Client sous Windows et si aucune autre application ne l'utilise, vous pouvez désinstaller ce logiciel après la désinstallation de Remote API Client sous Windows. Procédez comme suit.

1. Dans une fenêtre de commande, accédez au répertoire où est installé Windows. En principe, il s'agit de **C:\Windows**.
2. Exécutez la commande suivante :

   gskbui sxclient

Si aucune autre application n'utilise GSKIT, Windows supprime les fichiers. Si le logiciel GSKIT est utilisé par d'autres applications, les fichiers sont conservés jusqu'à la désinstallation de ces applications.

Aide

Vous pouvez afficher l'aide à tout moment en appuyant sur la touche **F1**. Les fenêtres Configuration et Options avancées comportent également un bouton **Aide**.

Chapitre 9. Configuration et utilisation de CS/AIX

Le moyen le plus simple pour définir et modifier la configuration CS/AIX est d'utiliser le programme d'administration Motif (**xsnaadmin**). Ce programme fournit une interface graphique à partir de laquelle vous pouvez visualiser et gérer les ressources SNA sur le nœud local. Vous pouvez également utiliser d'autres outils d'administration tels que le programme d'administration Web ou le programme d'administration de la ligne de commande, mais le programme Motif est recommandé.

Le programme d'administration Motif comprend des écrans d'aide offrant des informations générales sur SNA et CS/AIX, des informations de référence sur les boîtes de dialogue CS/AIX ainsi que des consignes sur l'exécution de certaines tâches. Pour chaque tâche (telle que la configuration du nœud) ou type de communication (tel que TN3270 ou APPC), le programme vous guide durant la configuration des ressources requises.

Le programme d'administration Motif permet de configurer tous les paramètres requis pour les configurations CS/AIX standard. Pour les paramètres avancés, le programme d'administration Motif propose des valeurs par défaut. Vous pouvez établir rapidement et facilement des communications SNA, car seules les informations de configuration essentielles sont nécessaires.

Vous pouvez également utiliser le programme d'administration Motif pour gérer le système d'exploitation CS/AIX en cours d'exécution. Le programme d'administration vous permet d'effectuer et d'appliquer des modifications de configuration tandis que CS/AIX est activé. Il fournit, par ailleurs, un accès facile aux informations d'état pour les ressources du nœud.

Ce programme affiche automatiquement les informations d'état relatives aux ressources CS/AIX. La plupart des informations sont affichées dans la fenêtre Nœud (reportez-vous à la section «Gestion de CS/AIX à l'aide du programme d'administration Motif», à la page 86). De plus, vous pouvez gérer certaines ressources (telles que des postes de nœud ou de liaison), à l'aide des boutons **Lancement** et **Arrêt** de la fenêtre Nœud. Les autres ressources sont toujours lancées et arrêtées automatiquement. Il n'est donc pas nécessaire de les gérer manuellement.

Remarque :

1. Vous devez faire partie du groupe de connexion `system` afin de définir ou modifier des ressources pour CS/AIX.
2. Pour utiliser le programme d'administration Motif, vous devez disposer d'un terminal de bas niveau (LFT) ou d'un terminal X. Si tel n'est pas le cas, vous pouvez utiliser l'utilitaire SMIT (System Management Interface Tool) ou le programme d'administration Web qui fournit des fonctions similaires à celles du programme Motif. Pour plus d'informations, voir le manuel *Communications Server for AIX Administration Guide*.
3. Pour plus d'informations sur l'interface utilisateur du programme d'administration Motif, notamment les boutons et les icônes qui

apparaissent sur les fenêtres, consultez les écrans d'aide du programme ou le manuel *Communications Server for AIX Administration Guide*.

4. Les fenêtres et boîtes de dialogue du programme d'administration Motif peuvent différer des illustrations du présent manuel, en fonction des des choix effectués dans certaines boîtes de dialogue.

Pour plus d'informations sur les outils d'administration de CS/AIX, notamment les programmes d'administration Web, d'administration en ligne de commande et l'application NOF, consultez le manuel *Communications Server for AIX Administration Guide*, *Communications Server for AIX Administration Command Reference* ou *Communications Server for AIX NOF Programmer's Guide*.

Préparation à la configuration de CS/AIX

Il est primordial de préparer soigneusement toute modification de la configuration. En effet, les changements apportés peuvent provoquer des dysfonctionnements, non seulement pour les utilisateurs du nœud local, mais aussi sur l'ensemble du réseau.

Il peut s'avérer utile de dessiner un diagramme de toutes les modifications apportées à la topologie du réseau. Ainsi, si vous ajoutez ou supprimez des connexions à d'autres nœuds, il est recommandé de dessiner un graphique représentant l'ensemble des nœuds. Vous pouvez utiliser le programme d'administration Motif pour rassembler des données de configuration sur toutes les connexions et ajouter ces informations à votre diagramme.

Il est facile de vérifier s'il existe un doublon ou si un nom est déjà utilisé, à mesure que vous ajoutez des ressources à votre diagramme. De même, le diagramme peut vous aider à déterminer quelles ressources doivent être supprimées et lesquelles sont essentielles.

Pour configurer un système client-server CS/AIX avec plusieurs nœuds, veillez à inclure tous les nœuds CS/AIX et leurs ressources dans votre diagramme. Vous pouvez ensuite configurer chacun des nœuds, comme décrit dans ce chapitre, de la même manière qu'en mode autonome.

Après avoir décidé des modifications à apporter, rassemblez les informations de configuration nécessaires. Pour ce faire, vous pouvez utiliser les listes des opérations fournies dans l'aide en ligne du programme d'administration Motif ou les feuilles de travail du manuel *Communications Server for AIX Administration Guide*.

Le présent chapitre fournit des instructions relatives à la configuration des fonctions CS/AIX les plus fréquemment utilisées. Pour chaque tâche de configuration, ce manuel indique également les informations dont vous devez disposer avant de configurer la ressource.

Remarque : En revanche, les informations de configuration devant être entrées dans les boîtes de dialogue CS/AIX ne sont pas décrites en détail. Pour plus d'informations sur les zones d'une boîte de dialogue déterminée, consultez l'aide en ligne correspondant à celle-ci (dans le programme d'administration Motif ou dans SMIT).

Feuilles de travail

Avant de commencer à configurer les ressources de CS/AIX, rassemblez toutes les données de configuration correspondant aux nouvelles ressources. Pour enregistrer toutes les informations relatives à une fonction ou une application dont vous avez besoin, utilisez les feuilles de travail fournies dans le manuel *Communications Server for AIX Administration Guide*.

Vous aurez probablement besoin de rassembler les informations de configuration à partir de plusieurs sources (administrateurs réseau, administrateurs hôte, programmeurs d'application et utilisateurs finaux, par exemple).

Si vous tentez de vous connecter à un autre nœud, l'administrateur de ce nœud est un contact essentiel. Il est en effet en mesure de vous communiquer les nom, adresse et caractéristiques de toutes les ressources de ce nœud. Il est souvent nécessaire de vérifier que les paramètres de configuration entrés au niveau du nœud local et du nœud éloigné correspondent.

Liste des opérations

Les écrans de l'aide en ligne du programme d'administration Motif contiennent des listes des opérations destinées à vous guider dans certaines tâches de configuration. Ces listes contiennent des pointeurs renvoyant aux écrans d'aide des boîtes de dialogue que vous utiliserez pour entrer les informations de configuration. Ces pointeurs vous permettent de parcourir l'aide et de voir exactement les données dont vous avez besoin.

Les listes des opérations renvoient également à des rubriques d'aide plus détaillées pour chacune des fenêtres et boîtes de dialogue nécessaire à la saisie des informations de configuration. Ces écrans d'aide fournissent des explications sur chaque zone à remplir ou à sélectionner.

Utilisation du programme d'administration Motif

Avant d'utiliser le programme d'administration Motif, vous pouvez ajouter des informations sur le chemin d'accès à vos fichiers **.login** ou **.profile** pour permettre au système de trouver les programmes exécutables (reportez-vous à la section «Définition du chemin d'accès aux programmes CS/AIX»). De plus, vous devez activer le logiciel CS/AIX avant de pouvoir utiliser le programme d'administration (reportez-vous à la section «Activation de CS/AIX», à la page 86).

Pour plus d'informations sur l'activation du programme d'administration Motif et sur son utilisation, reportez-vous à la section «Gestion de CS/AIX à l'aide du programme d'administration Motif», à la page 86.

Définition du chemin d'accès aux programmes CS/AIX

Pour exécuter les programmes CS/AIX, vous devez indiquer le chemin du répertoire contenant les programmes exécutables de CS/AIX. Pour ce faire, vous pouvez soit ajouter ce répertoire à votre variable d'environnement `PATH` avant d'exécuter les programmes pour la première fois, soit indiquer le nom du répertoire chaque fois que vous exécutez les programmes.

Le programme d'administration Motif est stocké dans le répertoire **/usr/bin/X11** et les autres programmes dans **/usr/bin**. Si vous ajoutez ces répertoires à la définition de la variable d'environnement `PATH` de vos fichiers **.login** ou **.profile**, CS/AIX

localise les programmes automatiquement. Une autre méthode consiste à indiquer le nom du répertoire lorsque vous exécutez le programme, selon les exemples ci-dessous :

/usr/bin/sna start

/usr/bin/X11/xsnaadmin

Les exemples de lignes de commande présentés dans ce manuel supposent que vous avez ajouté les répertoires à votre variable d'environnement PATH et que vous n'avez pas inclus les noms de répertoire.

Activation de CS/AIX

Pour configurer ou gérer le nœud local, vous devez activer CS/AIX sur le système local. Comme pour toute application X/Motif, il peut être nécessaire de configurer la variable d'environnement DISPLAY afin de désigner un serveur X approprié.

En principe, CS/AIX est activé automatiquement après l'installation du logiciel. Si CS/AIX a été désactivé, vous pouvez le réactiver en entrant la commande suivante à l'invite de commande AIX :

sna start

Lorsque vous installez CS/AIX, l'utilitaire d'installation met à jour automatiquement le fichier de démarrage **/etc/inittab** pour ajouter une entrée pour **/etc/rc.sna** , qui comporte la commande **sna start** . Cela permet de lancer CS/AIX automatiquement au démarrage du système. Si vous ne souhaitez pas que CS/AIX soit lancé automatiquement, vous pouvez supprimer cette ligne ou la mettre en commentaire, puis suivre les instructions de cette section pour activer le logiciel CS/AIX manuellement.

CS/AIX envoie des messages vers la sortie erreur standard (généralement l'écran de votre terminal) pour indiquer l'état de l'initialisation.

Gestion de CS/AIX à l'aide du programme d'administration Motif

Avant d'utiliser le programme d'administration Motif pour CS/AIX, vérifiez que CS/AIX est initialisé selon la procédure décrite à la section«Activation de CS/AIX». (Il peut également être nécessaire de configurer la variable d'environnement DISPLAY afin de désigner un serveur X approprié.)

Pour lancer le programme d'administration Motif en arrière-plan, entrez la commande suivante :

xsnaadmin &

CS/AIX affiche la fenêtre Domaine. Cette fenêtre affiche tous les nœuds définis et vous permet d'ajouter, de supprimer et d'arrêter les nœuds. Pour afficher la fenêtre d'informations relative à un nœud, double-cliquez sur le nœud (voir figure 4, à la page 88).

Cette fenêtre affiche des informations relatives au nœud et à ses ressources. Si vous n'avez pas encore configuré le nœud, le programme d'administration vous invite à le faire, selon la méthode décrite à la section «Configuration du nœud», à la page 92.

Remarque : Le présent manuel utilise le terme fenêtre pour désigner les fenêtres Motif qui affichent les informations relatives aux ressources CS/AIX. Une fenêtre peut contenir une ou plusieurs sections ou sous-fenêtres. Une boîte de dialogue est une fenêtre Motif dans laquelle vous pouvez entrer des informations.

La fenêtre Nœud contient la plupart des informations nécessaires et permet d'accéder facilement à tout autre élément. Elle affiche toutes les ressources clés du nœud local.

Pour configurer un système CS/AIX client-serveur avec plusieurs nœuds, suivez les instructions de ce chapitre pour configurer chacun des nœuds (pour sélectionner le nœud suivant, retournez dans la fenêtre Domaine).

D'autres fenêtres sont accessibles à partir du menu **Fenêtres** de la fenêtre Nœud. C'est le cas, notamment, des fenêtres suivantes :

- Groupes de LU
- Noms de destination CPI-C

Le menu **Services** de la fenêtre Nœud permet d'ajouter rapidement des ressources et d'obtenir de l'aide sur les opérations de configuration et de gestion. Le menu **Diagnostics** donne accès aux boîtes de dialogue Consignation et Trace.

Fenêtre Nœud

Un exemple de fenêtre Nœud est présenté dans la figure 4, à la page 88. La barre de titre indique le nom du système AIX.

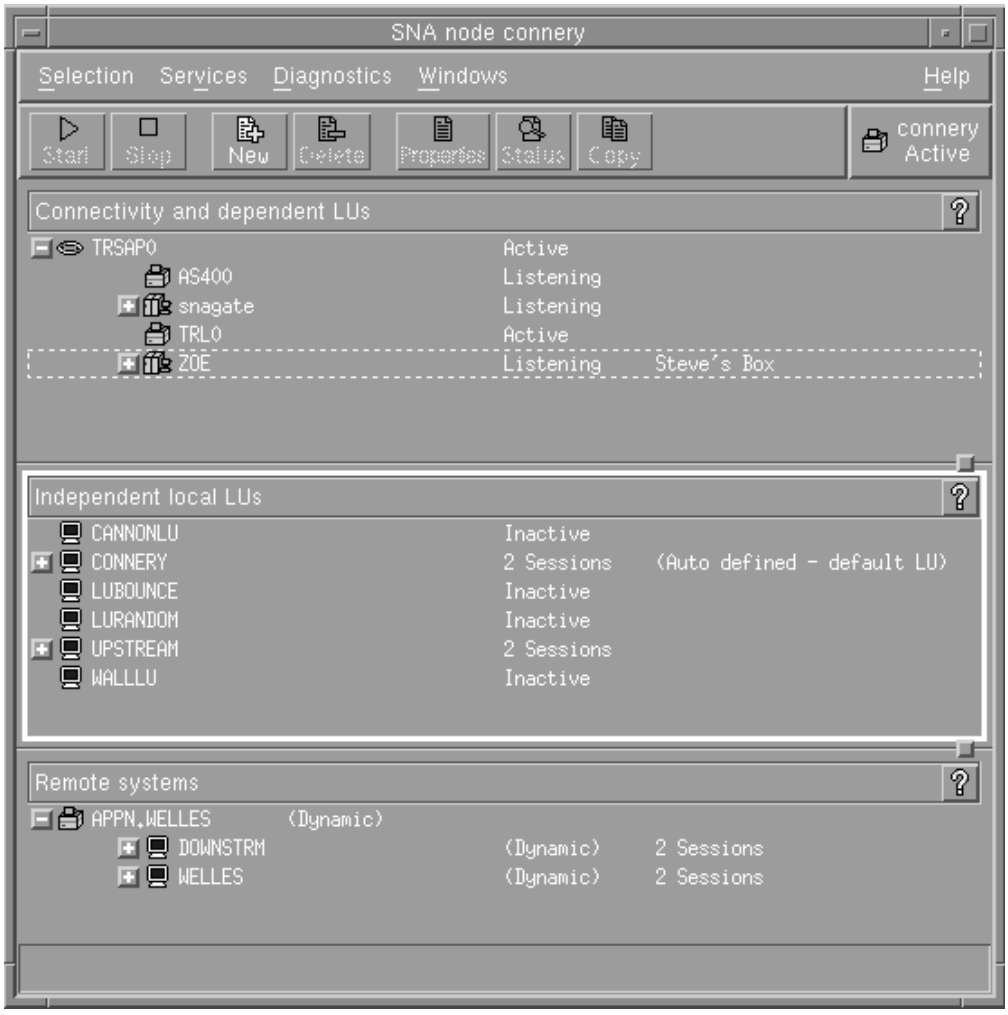

Figure 4. Fenêtre Nœud

À partir de la fenêtre Nœud, vous pouvez configurer et gérer toutes les ressources et tous les composants du nœud CS/AIX.

- Ports
- Postes de liaison
- LU de type 0 à 3 et LU dépendantes de type 6.2
- PU internes du DLUR
- LU locales indépendantes
- Nœuds éloignés
- LU partenaires

Vous pouvez ajouter, supprimer, modifier et gérer toutes ces ressources à partir de la fenêtre Nœud. La disposition des ressources à l'intérieur de la fenêtre illustre les liens entre celles-ci et vous permet de vérifier lesquelles sont affichées.

Les ports, les LU locales et les nœuds éloignés sont toujours affichés. Dans la fenêtre Nœud, chaque poste de liaison apparaît au-dessous du port parent et chaque LU dépendante, au-dessous du poste de liaison parent. Les LU partenaires apparaissent également au-dessous des LU locales et des nœuds éloignés.

La fenêtre Nœud contient des sections distinctes pour les différents types de ressources du nœud :

- La case Nœud, située à l'angle supérieur droit de la fenêtre Nœud indique si le nœud est `Actif` ou `Inactif`.
- La sous-fenêtre supérieure de la fenêtre Nœud (c'est-à-dire la sous-fenêtre de connectivité) énumère les ressources de connectivité du nœud, y compris les ports, postes de liaison ou PU de chaque port, ainsi que les LU dépendantes d'un poste de liaison ou d'une PU déterminé(e)s. La fenêtre indique l'état en cours de chaque ressource.
- La sous-fenêtre centrale (LU locales indépendantes) énumère les LU indépendantes définies sur le nœud local. Cette fenêtre affiche également des informations relatives aux sessions utilisant une LU particulière, ainsi que tout enregistrement définissant l'emplacement d'une LU partenaire par le poste de liaison permettant d'y accéder.
- La sous-fenêtre inférieure (sous-fenêtre des systèmes éloignés) affiche des informations sur les nœuds éloignés et les LU partenaires. Elle contient également des informations de session pour chaque nœud éloigné ou LU partenaire.

Vous pouvez sélectionner n'importe laquelle de ces sous-fenêtres en cliquant dessus. Vous pouvez également sélectionner uniquement certaines ressources d'une sous-fenêtre en cliquant sur les lignes correspondantes. Pour visualiser ou modifier la configuration d'un élément, cliquez deux fois sur celui-ci. (Vous pouvez utiliser les boutons et menus de cette fenêtre pour accéder aux informations de configuration de ressources déterminées.)

Les ressources appartenant à chacun des éléments de la liste sont imbriquées dans les informations relatives à celui-ci. Par exemple, les postes de liaison sont groupés sous le port auquel ils appartiennent. Pour afficher les ressources d'un élément, cliquez sur le symbole **+** situé à côté de l'élément, et pour les masquer cliquez sur le symbole **–**.

Vous pouvez effectuer les opérations d'administration suivantes à partir de la fenêtre Nœud :

Démarrage ou arrêt d'une ressource
Sélectionnez la ressource et cliquez sur les boutons **Lancement** ou **Arrêt**. (Vous pouvez également sélectionner les éléments **Lancement** ou **Arrêt** à partir du menu **Sélection**.)

Ajout d'une ressource à un élément
Sélectionnez l'élément et cliquez sur le bouton **Nouveau** (ou sélectionnez **Nouveau** à partir du menu **Sélection**). Par exemple, pour ajouter un poste de liaison à un port, sélectionnez ce dernier puis cliquez sur le bouton **Nouveau**.

Suppression d'une ressource
Sélectionnez la ressource et cliquez sur le bouton **Suppression** (ou sélectionnez **Suppression** à partir du menu **Sélection**).

Visualisation ou modification de la configuration d'une ressource
Sélectionnez la ressource et cliquez sur le bouton **Propriétés** (ou sélectionnez **Propriétés** à partir du menu **Sélection**).

Affichage d'informations sur l'état d'une ressource
Sélectionnez la ressource et cliquez sur le bouton **État** (ou sélectionnez **État** à partir du menu **Sélection**).

Copie de la configuration d'une ressource
Sélectionnez la ressource et cliquez sur le bouton **Copie** (ou sélectionnez **Copie** à partir du menu **Sélection**).

De plus, vous pouvez sélectionner des opérations de configuration déterminées (niveau nœud) à partir du menu **Services**, gérer les tâches de consignation (domaine) et de suivi (nœud) à partir du menu **Diagnostics** ou encore visualiser ou modifier les ressources domaines en sélectionnant un des éléments du menu **Fenêtres**.

Éléments ressource

La disposition des ressources à l'intérieur d'une fenêtre illustre les liens entre celles-ci.

Si un élément est associé à un ou plusieurs éléments enfants, le symbole **+** ou **–** apparaît à ses côtés :

- Le symbole **+** indique que les éléments enfants sont masqués. Pour les afficher, vous pouvez cliquer sur le symbole d'expansion ou appuyer sur la touche **+** du clavier numérique.
- Le symbole **-** indique que les éléments enfants sont affichés. Pour les masquer, vous pouvez cliquer sur le symbole **-** ou appuyer sur la touche **–** du clavier numérique.
- L'absence de symbole indique qu'aucune ressource enfant n'est associée à l'élément.

Par exemple, un poste de liaison est associé à un port particulier. Dans la sous-fenêtre de connectivité de la fenêtre Nœud, le poste de liaison apparaît sous le port parent, de même que tous les autres postes de liaison associés à ce port. Le port apparaît toujours, mais vous pouvez afficher ou masquer la liste des postes de liaison associés. De même, les postes de liaison possédant une liste de LU associées peuvent être étendus de façon à afficher les LU ou réduits pour les masquer.

Une ressource parent doit toujours être configurée avant ses ressources enfants. De plus, la suppression d'une ressource parent entraîne la suppression de toutes ses ressources parents.

Boutons de la barre d'outils

Les fenêtres de ressource contiennent des boutons de barre d'outils destinés à faciliter l'exécution des fonctions les plus courantes. La figure 5 présente un exemple de barre d'outils pour CS/AIX.

Figure 5. Barre d'outils pour CS/AIX

Tous les boutons n'apparaissent pas dans la barre d'outils de chaque fenêtre de ressource. Si l'opération correspondant à un bouton n'est pas valide pour l'élément sélectionné (ou si une opération requiert la sélection d'un élément), le contour du bouton apparaît en grisé et la fonction ne peut être sélectionnée (les clics de souris sont sans effet). Les boutons suivants peuvent apparaître dans les fenêtres de ressource :

Lancement
Lance l'élément sélectionné.

Arrêt Arrête l'élément sélectionné.

Nouveau
Ajoute un élément de ressource.

Suppression
Supprime les ressources sélectionnées.

Propriétés
Ouvre la boîte de dialogue de l'élément sélectionné pour vous permettre de visualiser ou de modifier la configuration de celui-ci.

État Affiche l'état en cours de l'élément sélectionné.

Copie Copie l'élément sélectionné. Lorsque vous cliquez sur ce bouton, la boîte de dialogue qui apparaît permet de dupliquer la configuration de l'élément sélectionné. Complétez les zones de cette boîte de dialogue (en entrant le nom du nouvel élément) pour ajouter la nouvelle ressource.

De nombreuses ressources, telles que les ports et les postes de liaison, ne peuvent être modifiées lorsqu'elles sont actives. Vous pouvez néanmoins visualiser les paramètres d'une ressource active en sélectionnant celle-ci, puis en cliquant sur le bouton **Propriétés** pour ouvrir les boîtes de dialogue correspondantes. Cliquez sur le bouton **Fermeture** lorsque vous avez terminé.

Configuration des fonctions client-serveur

Cette section est utile uniquement si vous avez installé CS/AIX pour l'exécuter en environnement client-serveur (avec plusieurs nœuds CS/AIX sur le même réseau).

En environnement client-serveur, un serveur peut être marqué comme serveur de configuration.CS/AIX conserve la liste de ces serveurs de configuration. Le premier serveur répertorié est le serveur maître, tous les autres étant des serveurs de secours. Les serveurs sont répertoriés dans un ordre défini : le deuxième serveur (le premier serveur de secours) prend le relais du serveur maître si celui n'est plus disponible, le troisième serveur (deuxième serveur de secours) prend le relais si le serveur maître et le premier serveur de secours ne sont pas disponibles, etc.

Lorsque des nœuds du domaine sont actifs, le premier serveur de configuration disponible du domaine (le premier serveur qui peut être contacté et sur lequel est exécuté CS/AIX) devient le serveur maître. Si le serveur en cours n'est plus disponible (car il ne peut pas être contacté, par exemple à cause d'une panne de réseau, ou si le logiciel SNA est arrêté), le serveur de configuration suivant de la liste devient le serveur maître.

CS/AIX peut être exécuté sans serveur maître. Cela se produit si aucun serveur de la liste de serveurs de configuration ne peut être contacté. Si cela se produit, vous pouvez afficher et configurer les ressources de nœud uniquement si les serveurs peuvent être contactés.

Remarque : Vous ne pouvez pas indiquer directement quel nœud agit en tant que serveur maître, le serveur maître est sélectionné selon l'ordre d'ajout des nœuds à la liste de serveurs de configuration. Pour déplacer un serveur en haut de la liste, retirez tous les autres nœuds de la liste puis ajoutez-les à nouveau.

Dans la fenêtre Domaine du programme d'administration Motif, vous pouvez ajouter un serveur de configuration en sélectionnant **Création d'un serveur de configuration** dans le menu **Sélection**. Le serveur est ajouté à la fin de la liste, il devient donc le serveur maître uniquement si tous les autres serveurs de configuration sont indisponibles. Pour supprimer un serveur, sélectionnez **Suppression du serveur de configuration** dans le menu **Sélection**.

Remarque : Vous ne pouvez pas supprimer un serveur s'il est le seul serveur de la liste sur lequel est exécuté le logiciel CS/AIX, car aucun autre serveur ne pourrait remplacer le serveur maître. Au moins un serveur maître est nécessaire dans une configuration client-serveur.

Pour plus d'informations sur la configuration et la gestion d'un système client-serveur CS/AIX, consultez le manuel *Communications Server for AIX Administration Guide*. Ce manuel fournit également des informations sur la configuration client-serveur avancée. Il indique notamment comment déplacer des clients et des serveurs vers différents domaines CS/AIX et comment configurer le fonctionnement des clients.

Configuration du nœud

La première étape de la configuration de CS/AIX sur un système consiste à configurer le nœud local. La configuration du nœud fournit en effet les informations de base nécessaires au nœud pour communiquer sur un réseau SNA. Vous devez configurer le nœud avant de définir la connectivité ou les autres ressources du nœud.

Si le nœud est déjà configuré, vous pouvez modifier la configuration à l'aide des procédures décrites dans la présente section ; vous devez cependant arrêter le nœud au préalable.

Avant de configurer le nœud, décidez si vous voulez configurer le nœud en tant que nœud APPN ou non APPN. Cette décision dépend des capacités des autres nœuds SNA avec lesquels vous communiquez.

La figure 6 montre un exemple de nœud CS/AIX communiquant directement avec un ordinateur hôte.

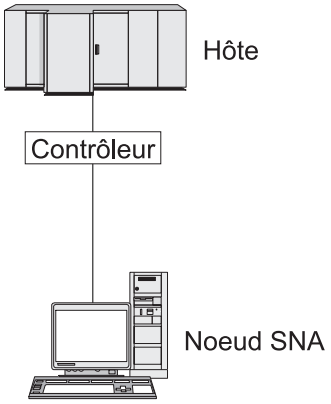

Figure 6. Nœud CS/AIX communiquant directement avec un ordinateur hôte

Si l'ordinateur hôte ne prend pas en charge APPN, configurez le nœud CS/AIX en tant que nœud LEN. Si l'hôte prend en charge APPN, vous pouvez configurer le

nœud CS/AIX soit en tant que nœud de réseau APPN soit en tant que nœud d'extrémité APPN (si CS/AIX utilise uniquement SNA pour communiquer avec l'hôte, vous pouvez configurer le nœud CS/AIX en tant que nœud d'extrémité ou nœud de réseau de type branche).

La figure 7 représente plusieurs nœuds CS/AIX dans un réseau APPN.

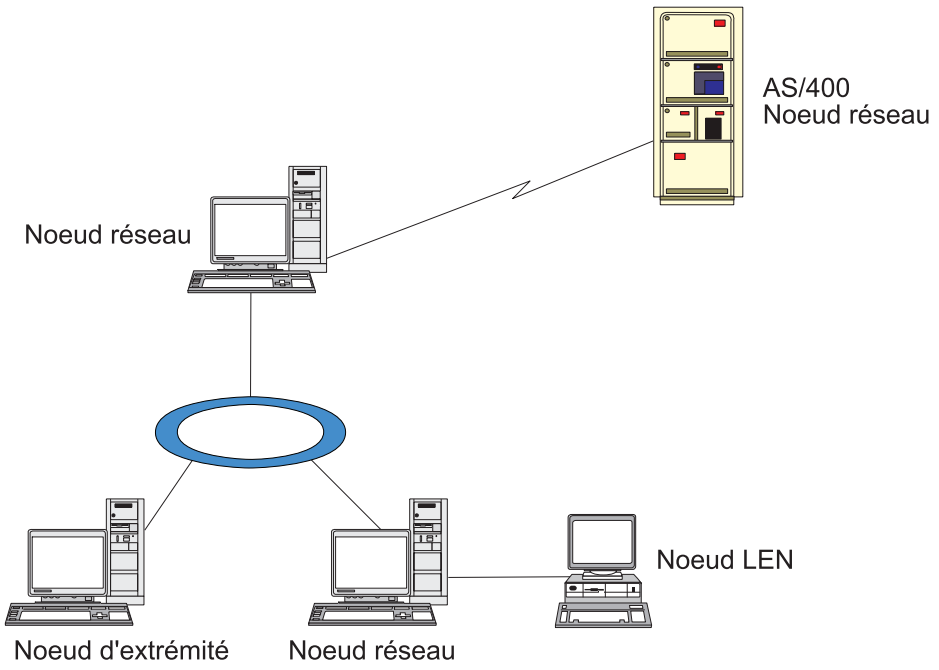

Figure 7. Nœuds CS/AIX dans un réseau APPN

Lorsque le nœud local fait partie d'un réseau APPN, vous devez le configurer en tant que nœud de réseau APPN, s'il doit assurer des services de routage APPN vers d'autres nœuds. Si d'autres nœuds assurent le routage, configurez le nœud local en tant que nœud d'extrémité APPN. Si le nœud local communique uniquement avec un nœud d'extrémité auquel il est directement connecté (qui peut être de n'importe quel type), configurez-le en tant que nœud LEN.

Avant de commencer à configurer le nœud, rassemblez les informations suivantes :

- Type de support APPN (nœud de réseau, nœud de réseau de type branche, nœud d'extrémité ou nœud LEN).
- Nom du point de contrôle (et alias, si différent). Entendez-vous avec votre gestionnaire de réseau pour définir ce nom.
- ID nœud par défaut (vous pouvez remplacer cette valeur par défaut lors de la configuration d'une liaison particulière)

Pour configurer le nœud, effectuez les étapes suivantes à partir de la fenêtre Nœud :

1. Sélectionnez **Configuration des paramètres du nœud** dans le menu **Services** ou bien double-cliquez sur la case Noeud en haut à droite de la fenêtre Noeud. CS/AIX affiche la boîte de dialogue Paramètres du nœud.
2. Indiquez un niveau de support APPN, le nom du point de contrôle et (si nécessaire) l'ID de nœud par défaut.

3. Cliquez sur **OK** pour définir le nœud. Lorsque vous définissez le nœud, CS/AIX détermine automatiquement une LU par défaut ayant le même nom que le point de contrôle.

   Pour sortir sans sauvegarder les valeurs que vous avez entrées, cliquez sur **Annulation**.

Configuration de la connectivité

Pour qu'un nœud CS/AIX puisse communiquer avec d'autres nœuds, vous devez configurer le nœud de connectivité avec au moins un nœud adjacent. Un lien de connexion peut être configuré de façon à prendre en charge le trafic dépendant, le trafic indépendant ou les deux.

Vous pouvez installer des cartes pour un ou plusieurs protocoles de liaison. La plupart des informations nécessaires à la configuration de la connectivité dépendent du protocole de liaison utilisé. Pour consulter la liste des protocoles de liaison pris en charge par CS/AIX, reportez-vous à la section «Conditions requises pour l'installation», à la page 22.

Pour configurer un lien, vous devez définir un port et (dans la plupart des cas) un poste de liaison. Lorsque vous utilisez le programme d'administration Motif, un DLC (contrôle de liaison de données) est automatiquement configuré lors de la configuration du port. De plus, vous avez la possibilité de définir le port en tant qu'élément d'un réseau de connexion.

Les liens à configurer dépendent du type d'opération que vous effectuez et du type de réseau (APPN ou non). Les informations requises varient selon le protocole de liaison utilisé et selon le type de trafic (dépendant, indépendant ou les deux).

À titre d'exemple, cette section explique comment configurer les types de liens suivants :

- Lien prenant en charge un trafic dépendant avec un système hôte à l'aide d'une ligne SDLC.
- Lien prenant en charge à la fois les trafic dépendant et indépendant sur un réseau APPN, à l'aide du protocole de liaison Ethernet. Cet exemple décrit également un réseau de connexion sur le port Ethernet.
- Lien Enterprise Extender à un réseau APPN (il est à noter que les liens Enterprise Extender ne prennent en charge que le trafic indépendant).

Pour les autres protocoles de liaison, consultez le manuel *Communications Server for AIX Administration Guide* ou l'aide en ligne du programme d'administration Motif.

Configuration d'un lien SDLC pour un trafic dépendant

Pour un port SDLC (contrôle de liaison de données synchrone), vous devez disposer des informations suivantes :

- Nom du port SNA (il est généralement possible d'utiliser la valeur par défaut). Vous devez également indiquer le numéro du périphérique SDLC.
- Le port doit-il être activé automatiquement au démarrage du nœud ?
- Type de ligne utilisée (commutée en sortie, commutée en entrée ou non commutée).
- Rôle du lien (principal, secondaire, négociable, principal multipoint ou secondaire multi-PU).

- Adresse d'appel (uniquement sur une ligne commutée en entrée sur un port non principal). Pour d'autres types de ports, configurez l'adresse d'appel sur le poste de liaison.

  Pour les lignes commutées en entrée et les lignes non commutées, vous devez également disposer d'informations relatives au codage (NRZ ou NRZI) et au duplex (semi-duplex ou non). Pour les autres types de ports, configurez les paramètres de codage et de duplexage sur le poste de liaison.
- Type de lien physique (pour identifier le type de modem).
- Chaîne de numérotation (nécessaire uniquement pour une ligne commutée en entrée). Pour une ligne commutée en sortie, configurez la chaîne de numérotation sur le poste de liaison.

Pour un poste de liaison SDLC, vous devez disposer des informations supplémentaires suivantes :

- Méthode d'activation (par l'administrateur, au démarrage du nœud ou à la demande).
- Type de trafic pris en charge (dans cet exemple, dépendant uniquement).
- Rôle du nœud éloigné (hôte, dans cet exemple).

Pour configurer le lien SDLC, effectuez les étapes suivantes à partir de la fenêtre Nœud :

1. Configuration du port :
   a. Sélectionnez la sous-fenêtre de connectivité.
   b. Sélectionnez **Nouveau port** à partir du sous-menu **Connectivité** du menu **Services** (ou cliquez sur **Nouveau** dans la barre des boutons).
   c. Dans la boîte de dialogue qui apparaît, sélectionnez le type de protocole approprié à partir du menu d'options, puis définissez le port.

      Lorsque vous cliquez sur **OK**, CS/AIX affiche la boîte de dialogue Port SDLC.
   d. Entrez les valeurs appropriées dans les diverses zones de la boîte de dialogue.
   e. Cliquez sur **OK** pour définir le port.

      Le port apparaît dans la sous-fenêtre de connectivité de la fenêtre Nœud.
2. Définition d'un poste de liaison sur le port :
   a. Veillez à sélectionner le port auquel vous ajoutez le poste de liaison dans la sous-fenêtre de connectivité.
   b. Sélectionnez **Nouveau poste de liaison** à partir du sous-menu **Connectivité** du menu **Services** (ou cliquez sur **Nouveau** dans la barre des boutons).
   c. Cliquez sur **OK**.

      CS/AIX affiche la boîte de dialogue Poste de liaison SDLC.
   d. Entrez les valeurs appropriées dans les diverses zones de la boîte de dialogue.
   e. Cliquez sur **OK** pour définir le poste de liaison.

      Celui-ci apparaît sous le port auquel il appartient dans la sous-fenêtre de connectivité de la fenêtre Nœud.

Configuration d'une liaison Ethernet pour les trafics dépendants et indépendants

Cet exemple indique comment configurer une liaison Ethernet prenant en charge à la fois les trafics dépendants et indépendants sur un réseau APPN. Il décrit également un réseau de connexion sur port Ethernet.

Pour un port Ethernet, vous devez disposer des informations suivantes :

- Nom du port SNA (il est généralement possible d'utiliser la valeur par défaut). Si vous disposez de plusieurs cartes de réseau Ethernet, vous devez également indiquer le numéro de la carte Ethernet. Vous devez aussi déterminer le numéro du SAP (point d'accès au service) local (en général `04`).
- Le port doit-il être activé automatiquement au démarrage du nœud ?
- Nom du réseau de connexion (doit être identique pour tous les ports d'un même réseau de connexion).

Pour un poste de liaison Ethernet, vous devez disposer des informations supplémentaires suivantes :

- Méthode d'activation (par l'administrateur, au démarrage du nœud ou à la demande).
- Type de trafic pris en charge (dans cet exemple, à la fois dépendant et indépendant).
- Nom du point de contrôle du nœud éloigné (nécessaire uniquement pour les nœuds LEN).
- Type de nœud éloigné (de réseau, d'extrémité ou localisation).
- Rôle du nœud éloigné (dans cet exemple, passerelle SNA ou émulation DLUR en aval).
- Pour configurer un poste de liaison sélectif, vous devez indiquer l'adresse MAC (contrôle d'accès au support) et le numéro de SAP (généralement `04`) du poste éloigné. Si vous ne précisez pas l'adresse et que vous définissez la zone *Activation* à `Par l'administrateur`, le poste de liaison est de type non sélectif en mode écoute.

Pour configurer le lien Ethernet, suivez les étapes ci-après à partir de la fenêtre Nœud :

1. Configuration du port :
   a. Sélectionnez la sous-fenêtre de connectivité.
   b. Sélectionnez **Nouveau port** à partir du sous-menu **Connectivité** du menu **Services** (ou cliquez sur **Nouveau** dans la barre des boutons).
   c. Dans la boîte de dialogue qui apparaît, sélectionnez le type de protocole approprié à partir du menu d'options, puis définissez le port.

      Lorsque vous cliquez sur **OK**, CS/AIX affiche la boîte de dialogue Ethernet SAP.
   d. Entrez les valeurs appropriées dans les diverses zones de la boîte de dialogue.
   e. Cliquez sur **OK** pour définir le port.

      Le port apparaît dans la sous-fenêtre de connectivité de la fenêtre Nœud.
2. Définition d'un poste de liaison sur le port :
   a. Veillez à sélectionner le port auquel vous ajoutez le poste de liaison dans la sous-fenêtre de connectivité.

b. Sélectionnez **Nouveau poste de liaison** à partir du sous-menu **Connectivité** du menu **Services** (ou cliquez sur **Nouveau** dans la barre des boutons).
c. Cliquez sur **OK**.

   CS/AIX affiche la boîte de dialogue Poste de liaison Ethernet.
d. Entrez les valeurs appropriées dans les diverses zones de la boîte de dialogue.
e. Cliquez sur **OK** pour définir le poste de liaison.

   Celui-ci apparaît sous le port auquel il appartient dans la sous-fenêtre de connectivité de la fenêtre Nœud.

Configuration d'une liaison Enterprise Extender

Cet exemple indique comment configurer une liaison Enterprise Extender sur un réseau APPN. Il est à noter que les liaisons Enterprise Extender ne prennent en charge que le trafic LU indépendant.

Pour un port Enterprise Extender, vous devez disposer des informations suivantes :

- Nom du port SNA (il est généralement possible d'utiliser la valeur par défaut). Si vous disposez de plusieurs cartes de réseau exécutant IP, indiquez également le nom de l'interface IP que vous souhaitez utiliser (par exemple, `eth0`).
- Le port doit-il être activé automatiquement au démarrage du nœud ?

Pour un poste de liaison Enterprise Extender, vous devez disposer des informations supplémentaires suivantes :

- Méthode d'activation (par l'administrateur, au démarrage du nœud ou à la demande).
- Type de nœud éloigné (de réseau, d'extrémité ou localisation).
- Pour configurer un poste de liaison sélectif, vous devez indiquer le nom d'hôte IP ou l'adresse IP du poste éloigné. Si vous ne précisez pas ces informations et que vous définissez la zone *Activation* à `Par l'administrateur`, le poste de liaison est de type non sélectif en mode écoute.

Pour configurer le lien Enterprise Extender, effectuez les étapes suivantes à partir de la fenêtre Nœud :

1. Configuration du port :
   a. Sélectionnez la sous-fenêtre de connectivité.
   b. Sélectionnez **Nouveau port** à partir du sous-menu **Connectivité** du menu **Services** (ou cliquez sur **Nouveau** dans la barre des boutons).
   c. Dans la boîte de dialogue qui apparaît, sélectionnez le type de protocole approprié à partir du menu d'options, puis définissez le port.

      Lorsque vous cliquez sur **OK**, CS/AIX affiche la boîte de dialogue Port IP.
   d. Entrez les valeurs appropriées dans les diverses zones de la boîte de dialogue.
   e. Cliquez sur **OK** pour définir le port.

      Le port apparaît dans la sous-fenêtre de connectivité de la fenêtre Nœud.
2. Définition d'un poste de liaison sur le port :
   a. Veillez à sélectionner le port auquel vous ajoutez le poste de liaison dans la sous-fenêtre de connectivité.
   b. Sélectionnez **Nouveau poste de liaison** à partir du sous-menu **Connectivité** du menu **Services** (ou cliquez sur **Nouveau** dans la barre des boutons).

c. Cliquez sur **OK**.

   CS/AIX affiche la boîte de dialogue Poste de liaison IP.

d. Entrez les valeurs appropriées dans les diverses zones de la boîte de dialogue.

e. Cliquez sur **OK** pour définir le poste de liaison.

   Celui-ci apparaît sous le port auquel il appartient dans la sous-fenêtre de connectivité de la fenêtre Nœud.

Configuration des LU de type 0 à 3

Pour prendre en charge les applications utilisateur qui utilisent des LU de type 0 à 3, vous devez configurer des LU dépendantes. Vous devez au préalable définir la configuration suivante :

- Configurez le nœud selon la procédure décrite à la section «Configuration du nœud», à la page 92.
- Configurez un lien supportant le trafic de LU dépendant, comme indiqué à la section «Configuration de la connectivité», à la page 94.

  Il est inutile de configurer un lien direct vers l'hôte si vous utilisez une liaison en amont vers un autre nœud via la passerelle SNA ou si vous utilisez DLUR. Pour plus d'informations, reportez-vous aux sections «Configuration d'une passerelle SNA», à la page 109 et «Configuration d'un demandeur de LU dépendante (DLUR)», à la page 112.

Vous devez configurer des LU dépendantes de types 0 à 3 pour prendre en charge la communication avec un système hôte. Vous pouvez utiliser les informations contenues dans cette section pour définir une LU prenant en charge LUA, DLUR ou la concentration de PU. Il est possible de définir une série de LU, de façon à configurer plusieurs LU de même type en une seule opération.

Vous pouvez également définir un groupe de LU à utiliser selon les besoins, soit en attribuant une LU à un groupe lorsque vous définissez celle-ci, soit en attribuant à un groupe des LU préalablement définies.

Définition de LU de type 0 à 3

Avant de configurer la LU 3270, rassemblez les informations suivantes :

- Nom de la LU (identificateur local qui ne doit pas nécessairement correspondre à la configuration hôte)
- Numéro de la LU (ou numéro de chaque LU d'une série)
- Type de LU (modèle d'affichage 3270 ou imprimante 3270)
- Nom du groupe (si vous ajoutez la LU à un groupe)

Pour configurer une LU de type 0 à 3 pour poste de liaison précédemment défini, effectuez les étapes suivantes à partir de la fenêtre Nœud :

1. Sélectionnez le poste de liaison vers l'hôte dans la sous-fenêtre de connectivité.
2. Cliquez sur **Nouveau**.
3. Sélectionnez le type de LU (nouvelle LU d'écran 3270 ou nouvelle LU d'imprimante 3270) dans la boîte de dialogue qui apparaît.

   Cliquez ensuite sur **OK**. CS/AIX affiche alors la boîte de dialogue LU de type 0 à 3.
4. Entrez les valeurs appropriées dans les diverses zones de la boîte de dialogue.
5. Cliquez sur **OK** pour définir la LU.

Celle-ci apparaît dans la sous-fenêtre de connectivité de la fenêtre Nœud, sous le poste de liaison vers l'hôte.

Définition d'un groupe de LU

Avec les LU de type 0 à 3, vous pouvez définir des groupes de LU pour simplifier la configuration utilisateur et la procédure d'établissement de sessions hôte. Vous pouvez, par exemple, définir plusieurs LU dans un même groupe de LU, puis configurer plusieurs utilisateurs utilisant ce groupe de LU. Ceci facilite la configuration des sessions utilisateur et permet à toute session d'utiliser n'importe quelle LU du groupe.

Remarque : Vous pouvez attribuer une session utilisateur à une LU particulière ou à un groupe de LU.

- Si vous attribuez la session utilisateur à une LU particulière appartenant à un groupe, la session utilise cette LU si elle est disponible. Sinon elle utilise n'importe quelle LU disponible du groupe, comme si vous l'aviez attribuée au groupe de LU au lieu de l'attribuer à une LU particulière.
- Si vous souhaitez que l'utilisateur utilise uniquement une LU particulière, afin que la session utilisateur ne puisse pas être établie si la LU est déjà utilisée, veillez à ce que la LU n'appartienne à aucun groupe.

Vous pouvez visualiser les groupes de LU du nœud CS/AIX local à l'aide de la fenêtre Groupes de LU. Cette fenêtre énumère les groupes de LU configurés sur le système local et vous permet de sélectionner les LU que vous voulez ajouter à un groupe.

Vous pouvez ajouter les types de LU suivants à un groupe (ne placez pas des LU de différents types dans un même groupe) :

- LU d'écran 3270
- LU sans restriction

Avant d'ajouter des LU à un groupe, vous devez définir celles-ci sur le nœud local.

Pour configurer un groupe de LU, effectuez les étapes ci-après à partir de la fenêtre Nœud :

1. Sélectionnez **Groupes de LU** à partir du menu **Fenêtres**.

   CS/AIX affiche alors la fenêtre Groupes de LU.
2. Cliquez sur **Nouveau**.

   CS/AIX affiche la boîte de dialogue Configuration d'un groupe de LU.

   La zone de droite énumère les LU qui ne sont attribuées à aucun groupe. Chacune de ces LU peut être ajoutée au nouveau groupe.
3. Sélectionnez la ou les LU que vous voulez ajouter, puis cliquez sur **Nouveau** pour déplacer la sélection vers la zone de gauche.

   Pour supprimer une LU de la zone de gauche, sélectionnez-la et cliquez sur **Suppression**.
4. Cliquez sur **OK** pour définir le groupe de LU.

   Toutes les LU apparaissant dans la zone de gauche sont ajoutées au groupe.

   Celui-ci apparaît alors dans la fenêtre Groupes de LU.

Configuration de sessions de communication APPC

Vous devez configurer APPC avant de pouvoir utiliser les applications APPC et CPI-C. Une application APPC utilise les ressources LU 6.2 du nœud pour communiquer avec une autre application APPC ou CPI-C (Communications CPI) sur un ordinateur hôte ou homologue, par le biais d'un mode déterminé.

Avant de configurer les communications APPC, vous devez effectuer les opérations suivantes :

1. Configurez le nœud selon la procédure décrite à la section «Configuration du nœud», à la page 92.
2. Configurez la connectivité selon la procédure décrite à la section «Configuration de la connectivité», à la page 94.

Les étapes suivantes de la configuration varient selon le type de trafic pris en charge (dépendant, indépendant ou les deux) :

Communications APPC indépendantes
Les communications APPC indépendantes utilisent des LU indépendantes. Chaque session LU-LU implique une LU locale et une LU partenaire.

Pour la LU locale, vous pouvez utiliser la LU prédéfinie par défaut, associée au point de contrôle du nœud, ou configurer de nouvelles LU locales.

Il n'est pas nécessaire de configurer la LU partenaire, si le nœud CS/AIX est un nœud d'extrémité ou de réseau APPN, puisque APPN peut localiser les LU partenaires dynamiquement. En revanche, si ces conditions ne sont pas remplies, vous devez configurer la LU partenaire. Dans ce cas, vous devez configurer le nœud éloigné où se trouve la LU partenaire, puis définir celle-ci sur le nœud éloigné.

Communications APPC dépendantes
Si le nœud éloigné est un hôte ne prenant pas en charge les LU 6.2 indépendantes, définissez une configuration pour trafic dépendant. Pour les communications APPC dépendantes, vous devez configurer une LU locale.

Pour des applications utilisant CPI-C, il peut s'avérer nécessaire de définir des configurations CPI-C supplémentaires après avoir configuré APPC (reportez-vous à la section «Configuration de communications CPI», à la page 106). Une application CPI-C utilise les ressources LU 6.2 et le mode du nœud pour communiquer avec une autre application APPC ou CPI-C sur un ordinateur hôte ou homologue. Vous devez définir les mêmes ressources pour une application CPI-C que pour une application APPC. De plus, si le TP de l'ordinateur CS/AIX est le TP appelant ou TP source (c'est-à-dire le TP qui lance la conversation), il peut être nécessaire de définir une ou plusieurs informations complémentaires, comme indiqué à la section «Configuration de communications CPI», à la page 106. Ces informations fournissent des détails sur le TP partenaire, sur les LU et le mode utilisés pour y accéder, ainsi que toute information de sécurité requise.

La présente section explique comment configurer un réseau APPN simple (utilisant une LU 6.2 indépendante) comprenant un nœud de réseau, un nœud d'extrémité et un nœud LEN, comme indiqué à la section «Configuration d'un réseau APPN simple», à la page 101. (Ce scénario explique également comment obtenir des informations d'état sur les sessions CP-CP entre deux nœuds.)

Cette rubrique explique également comment configurer une communication APPC dépendante, comme indiqué à la section «Configuration de communications APPC dépendantes», à la page 105.

Les deux scénarios supposent que les sessions APPC utilisent un mode et une classe de service (COS) standard.

Pour plus d'informations sur la configuration d'informations APPC complémentaires, telles que les modes, la sécurité et les TP pouvant être appelés (cible), voir le manuel *Communications Server for AIX Administration Guide*.

Configuration d'un réseau APPN simple

Le réseau APPN le plus simple que vous puissiez configurer ne comprend que deux nœuds : un nœud de réseau APPN et un nœud d'extrémité APPN. Le nœud de réseau gère le routage de session pour le nœud d'extrémité.

Configuration d'un nœud de réseau

Ce scénario suppose que vous utilisez la LU de point de contrôle et un mode standard, ainsi qu'une liaison de type réseau local (anneau à jeton ou Ethernet). Si tel est le cas, vous pouvez configurer le nœud de réseau en exécutant simplement les opérations de configuration suivantes :

1. Configurez le nœud selon la procédure décrite à la section «Configuration du nœud», à la page 92. Dans la zone *APPN support*, sélectionnez la valeur `Nœud de réseau`. Notez le nom du point de contrôle.
2. Configurez la connectivité selon la procédure décrite à la section «Configuration de la connectivité», à la page 94. Configurez la liaison pour la prise en charge du trafic indépendant.

Pour contacter ce nœud de réseau à partir d'un nœud d'extrémité adjacent, vous devez connaître l'adresse MAC et le numéro de SAP du port du nœud de réseau. Vous pouvez obtenir l'adresse MAC d'un nœud à l'aide de la procédure suivante :

1. Sélectionnez le port à partir de la fenêtre Nœud.
2. Cliquez sur **Lancement** pour démarrer le port.
3. Cliquez sur **État** pour obtenir des informations d'état sur le port. La boîte de dialogue État du port indique l'adresse MAC et le numéro de SAP.
4. Notez ces valeurs afin de les entrer dans les zones correspondantes de la boîte de dialogue de configuration du poste de liaison du nœud d'extrémité.

Configuration du nœud d'extrémité

Ce scénario suppose que vous utilisez la LU de point de contrôle et un mode standard, ainsi qu'une liaison de type réseau local (anneau à jeton ou Ethernet). Si tel est le cas, vous pouvez configurer le nœud de réseau en exécutant simplement les opérations de configuration suivantes :

1. Configurez le nœud selon la procédure décrite à la section «Configuration du nœud», à la page 92. Dans la zone *APPN support*, sélectionnez la valeur `Nœud d'extrémité`.
2. Configurez la connectivité selon la procédure décrite à la section «Configuration de la connectivité», à la page 94. Configurez la liaison pour la prise en charge du trafic indépendant et indiquez les informations suivantes pour le poste de liaison :
   - Entrez le nom du nœud de réseau (reportez-vous à la section «Configuration d'un nœud de réseau») dans la zone *Nœud éloigné*.

- Entrez l'adresse MAC et le numéro de SAP du port, dans la sous-fenêtre Informations contact de la boîte de dialogue de configuration du poste de liaison.

Sur un réseau APPN, un seul et unique poste de liaison vers un nœud de réseau adjacent permet de communiquer avec n'importe quel nœud éloigné du réseau. Il n'est donc pas nécessaire de configurer un poste de liaison distinct pour chaque nœud éloigné.

Vérification de la connectivité entre deux nœuds

Ce scénario suppose que vous avez configuré un nœud de réseau et un nœud d'extrémité, comme indiqué respectivement aux sections «Configuration d'un nœud de réseau», à la page 101 et «Configuration du nœud d'extrémité», à la page 101. Vous pouvez effectuer la procédure suivante à partir du nœud d'extrémité :

1. Dans la fenêtre Nœud, sélectionnez le poste de liaison établissant la connexion vers le nœud de réseau adjacent.
2. Cliquez sur **Lancement** pour lancer le poste de liaison.

   Les sessions CP-CP entre les deux nœuds sont établies automatiquement au démarrage du poste de liaison. Ces sessions apparaissent dans la sous-fenêtre LU locales indépendantes de la fenêtre Nœud.
3. Pour obtenir des informations d'état sur une session, sélectionnez celle-ci dans la fenêtre Nœud et cliquez sur le bouton **État**.

Configuration d'une LU APPC indépendante

Les applications utilisent souvent la LU de point de contrôle du nœud qui est automatiquement définie lors de la configuration du nœud. Il s'agit de la LU par défaut : si aucune LU particulière n'est définie pour votre application, elle peut utiliser celle-ci. Si tel est le cas, il n'est pas nécessaire de définir une LU locale. Consultez la documentation de votre application APPC ou contactez le développeur.

Pour configurer une LU 6.2 indépendante, vous devez disposer des informations suivantes :

- Nom de la LU locale ;
- Alias de la LU locale (si vous utilisez un alias pour un TP pris en charge par cette LU) ;

Pour configurer une LU locale indépendante, effectuez les étapes suivantes à partir de la fenêtre Nœud :

1. Sélectionnez la sous-fenêtre LU locales indépendantes.
2. Sélectionnez **Nouvelle LU locale indépendante** à partir du sous-menu **APPC** du menu **Services** (ou cliquez sur **Nouveau**).

   CS/AIX affiche alors la boîte de dialogue LU locale.
3. Entrez les valeurs appropriées dans les diverses zones de la boîte de dialogue.
4. Cliquez sur **OK** pour définir la LU locale. La LU indépendante apparaît dans la sous-fenêtre LU locales indépendantes de la fenêtre Nœud.

Configuration des LU partenaires pour un nœud LEN

Vous devez définir un nœud éloigné (ainsi que les LU partenaires du nœud) dans les cas suivants :

- Si le nœud local est un nœud LEN, vous devez définir tous les nœuds éloignés et toute LU partenaire du nœud éloigné avec lequel il communique à l'aide d'APPC. Un nœud LEN ne peut localiser les LU partenaires si le nœud éloigné n'est pas défini.

- Si le nœud local ne fait pas partie d'un réseau APPN (si vous disposez, par exemple, de deux nœuds d'extrémité directement connectés, sans serveur de nœud de réseau), les LU ne peuvent pas être localisées dynamiquement. Dans ce cas, vous devez configurer chaque LU partenaire.
- Si le nœud éloigné est un nœud LEN et que le nœud local est un nœud de réseau agissant en tant que serveur de nœud de réseau du nœud LEN, vous devez définir ce dernier (et les LU partenaires correspondantes) en tant que nœud éloigné du serveur de nœud de réseau. Cette définition permet aux nœuds du reste du réseau APPN de localiser les LU sur le nœud LEN.
- Si Ie nœud éloigné est situé sur un réseau APPN distinct, vous devez définir le nœud éloigné, car il ne peut être localisé dynamiquement.

Ne définissez pas de LU partenaires si les nœuds locaux et éloignés appartiennent au même réseau APPN.

Lorsque vous ajoutez une définition de nœud éloigné, une LU partenaire du même nom que celui-ci est automatiquement ajouté et constitue la LU de point de contrôle du nœud éloigné. Si votre application utilise cette LU partenaire, il n'est pas nécessaire d'ajouter une autre LU partenaire. Vous pouvez en revanche ajouter un alias de LU pour la LU partenaire. Pour ce faire, cliquez deux fois sur la LU partenaire et entrez l'alias dans la boîte de dialogue Configuration d'une LU partenaire.

Si votre application utilise un alias de LU pour désigner la LU partenaire, il est recommandé d'ajouter une définition d'alias de LU partenaire.

Si le nœud local ou éloigné est un nœud LEN, vous devez définir la LU partenaire en tant qu'enfant du nœud éloigné, car un nœud LEN ne peut pas participer à la localisation dynamique des LU. Si votre application utilise les LU de point de contrôle du nœud éloigné en tant que LU partenaire, la LU de point de contrôle est définie automatiquement lors de la définition du nœud éloigné.

Vous pouvez utiliser le programme d'administration Motif pour ajouter un alias de LU partenaire (reportez-vous à la section «Définition d'un alias de LU partenaire», à la page 104), une définition de LU partenaire sur un nœud éloigné déterminé (section «Définition d'une LU partenaire sur un nœud éloigné», à la page 104) ou encore définir plusieurs LU partenaires à l'aide de caractères génériques (section «Définition de plusieurs LU partenaires à l'aide de caractères génériques», à la page 104).

Définition d'un nœud éloigné : Avant de configurer un nœud, vous devez disposer des informations suivantes :

- Nom complet de réseau SNA du nœud.

Pour configurer un nœud éloigné, suivez les étapes ci -après à partir de la fenêtre Nœud :

1. Sélectionnez la sous-fenêtre des systèmes éloignés.
2. Select **Nouveau nœud éloigné** dans le sous-menu **APPC** du menu **Services** (ou cliquez sur **Nouveau** dans la barre des boutons, puis sélectionnez **Définition d'un nœud éloigné**).

   CS/AIX affiche la boîte de dialogue Configuration d'un nœud éloigné.
3. Entrez les valeurs appropriées dans les diverses zones de la boîte de dialogue.
4. Cliquez sur **OK** pour définir le nœud éloigné. Le nœud éloigné apparaît dans la sous-fenêtre des systèmes éloignés de la fenêtre Nœud.

Lorsque vous définissez un système éloigné, CS/AIX définit automatiquement la LU de point de contrôle du nœud éloigné en tant que LU partenaire du nœud local.

Définition d'un alias de LU partenaire : Pour définir un alias de LU partenaire, vous devez disposer des informations suivantes :

- Nom complet de la LU partenaire (nom du réseau SNA et de la LU)
- Alias de la LU partenaire utilisée par un TP local

Pour ajouter un alias de LU partenaire, suivez les étapes ci-après à partir de la fenêtre Nœud :

1. Sélectionnez la sous-fenêtre des systèmes éloignés.
2. Sélectionnez **APPC**, **Nouvelles LU partenaires** et **Alias de la LU partenaire** à partir du menu **Services** (ou cliquez sur **Nouveau** dans la barre des boutons et sélectionnez **Définition d'un alias de LU partenaire**).

   CS/AIX affiche la boîte de dialogue Configuration d'un alias de LU partenaire.
3. Entrez le nom et l'alias de la LU partenaire.
4. Cliquez sur **OK** pour définir l'alias de la LU partenaire. Celle-ci apparaît alors dans la sous-fenêtre des systèmes éloignés de la fenêtre Nœud (en tant qu'élément de la définition du réseau).

Définition d'une LU partenaire sur un nœud éloigné : Pour définir une LU partenaire sur un nœud éloigné déterminé, vous devez disposer des informations suivantes :

- Nom complet de la LU partenaire ;
- Alias de la LU partenaire (si un TP local utilise un alias) ;
- Nom complet du nœud contenant les informations de répertoire relatives à la LU partenaire ;
- Si la LU partenaire se trouve sur un réseau TCP/IP, la méthode de routage préférée (APPN ou AnyNet).

Pour ajouter une définition de LU partenaire pour un nœud éloigné déterminé, suivez les étapes ci-après à partir de la fenêtre Nœud :

1. Sélectionnez le nœud éloigné.
2. Sélectionnez **APPC**, **Nouvelles LU partenaires** et **LU partenaire sur nœud éloigné** à partir du menu **Services** (ou cliquez sur **Nouveau** dans la barre des boutons, puis sélectionnez **Définition de la LU partenaire sur le nœud éloigné**).

   CS/AIX affiche la boîte de dialogue Configuration d'une LU partenaire.
3. Entrez les valeurs appropriées dans les diverses zones de la boîte de dialogue.
4. Cliquez sur **OK** pour définir la LU partenaire. L'alias de la LU partenaire apparaît dans la sous-fenêtre des systèmes éloignés de la fenêtre Nœud, au-dessous du système éloigné auquel il appartient.

Définition de plusieurs LU partenaires à l'aide de caractères génériques : Vous pouvez utiliser des caractères génériques pour configurer l'emplacement d'un ensemble de LU partenaires situées sur un même nœud éloigné et dont les noms commencent par des caractères identiques. L'utilisation de caractères génériques permet de ne pas configurer chaque LU partenaire individuellement.

Lorsque vous définissez des LU partenaires à l'aide de caractères génériques, vous devez fournir les informations suivantes :

- Nom tronqué de la LU partenaire. Le nom tronqué de la LU partenaire est composé de deux types de chaînes EBCDIC de type A, de 1 à 8 caractères chacune, correspondant aux noms complets de LU du groupe de LU partenaires.

  La première chaîne peut être un nom de réseau SNA complet identique au nom de réseau des LU partenaires ou un préfixe constitué d'un caractère générique correspondant au début du nom du réseau. Si vous entrez un préfixe sous forme de caractère générique pour le nom du réseau, laissez la seconde chaîne vide.

  Si vous indiquez un nom de réseau SNA complet pour la première chaîne, vous pouvez entrer une valeur pour la seconde chaîne. (Vous ne pouvez pas saisir la seconde chaîne si vous ne fournissez pas un nom de réseau SNA valide pour la première chaîne.) La seconde chaîne est traitée sous la forme d'un préfixe en caractères génériques qui doit correspondre au début de la deuxième partie du nom complet des LU partenaires.
- Nom du nœud où se situent les LU partenaires.

Pour ajouter plusieurs LU partenaires, suivez les étapes ci -après à partir de la fenêtre Nœud :

1. Sélectionnez le nœud éloigné pour lequel vous voulez définir des LU partenaires.
2. À partir du menu **Services**, sélectionnez **APPC**, **Nouvelles LU partenaires** et **LU partenaire en caractères génériques sur nœud éloigné** (ou cliquez sur **Nouveau** dans la barre des boutons, puis sélectionnez l'option de définition des LU partenaires en caractères génériques sur nœud éloigné).

   CS/AIX affiche la boîte de dialogue Configuration d'une LU partenaire en caractères génériques.
3. Entrez les valeurs appropriées dans les diverses zones de la boîte de dialogue.
4. Cliquez sur **OK** pour définir les LU partenaires. Celles-ci apparaissent alors dans la sous-fenêtre des systèmes éloignés de la fenêtre Nœud, au-dessous du nœud éloigné auquel elles appartiennent.

Configuration de communications APPC dépendantes

Pour configurer une LU 6.2 dépendante, vous devez disposer des informations suivantes :

- Nom de la LU locale ;
- Alias de la LU locale (si vous utilisez un alias pour un TP pris en charge par cette LU) ;
- Nom du poste de liaison qui assure la connexion vers le système hôte ;
- Numéro de LU ;
- La LU doit-elle être affectée au groupe par défaut de la LU 6.2 dépendante ?

Les LU dépendantes de type 6.2 destinées à être utilisées avec des applications APPC ou CPI-C peuvent être définies en tant que membres du groupe par défaut. Une application pour laquelle aucune LU locale n'est définie est associée à une des LU du groupe de LU par défaut.

Pour configurer une LU locale dépendante, suivez les étapes ci-après à partir de la fenêtre Nœud :

1. Sélectionnez un poste de liaison dans la sous-fenêtre de connectivité.

2. Sélectionnez **Nouvelle LU locale dépendante** à partir du sous-menu **APPC** du menu **Services** (ou cliquez sur **Nouveau** dans la barre des boutons, puis sélectionnez **Nouvelle LU locale dépendante**).

   CS/AIX affiche alors la boîte de dialogue LU locale.
3. Entrez les valeurs appropriées dans les diverses zones de la boîte de dialogue.
4. Cliquez sur **OK** pour définir la LU locale. Celle-ci apparaît dans la sous-fenêtre de connectivité, sous le poste de liaison auquel elle appartient.

Configuration de communications CPI

Si votre système prend en charge une application CPI-C utilisant les noms de destination symboliques, vous devez définir les informations annexes relatives à la communication CPI. Ces informations associent le nom de destination symbolique à des informations relatives au TP partenaire, à la LU partenaire, au mode et à la sécurité.

Pour déterminer le nom de destination symbolique pour la communication CPI, consultez le développeur de votre application (ou dans le cas d'un programme tiers, consultez la documentation produit).

Avant de configurer les informations annexes relatives à la communication CPI, vous devez disposer des informations suivantes :

- Nom de destination symbolique utilisé par le TP ;
- Nom du TP partenaire ;
- Nom ou alias de la LU partenaire ;
- Nom du mode.

Pour configurer les informations annexes relatives à la communication CPI, suivez les étapes ci-après à partir de la fenêtre Nœud :

1. Sélectionnez **CPI-C** dans le sous-menu **APPC** du menu **Services**.

   CS/AIX affiche alors la fenêtre Noms de destination CPI-C.
2. Cliquez sur **Nouveau**.

   CS/AIX affiche la boîte de dialogue Configuration d'une destination CPI-C.
3. Entrez les valeurs appropriées dans les diverses zones de la boîte de dialogue.
4. Cliquez sur **OK** pour définir les informations annexes relatives à la communication CPI.

Configuration des LUA

Pour les nouvelles applications fonctionnant avec des LU de type 0 à 3, utilisez l'API LUA. Cette API peut être utilisée pour des applications qui utilisent des LU de type 0 à 3 pour communiquer avec un ordinateur hôte. (Pour plus d'informations, sur l'API LUA, voir le manuel *Communications Server for AIX LUA Programmer's Guide*.)

Avant de configurer une LUA, effectuez les opérations de configuration suivantes :

1. Configurez le nœud selon la procédure décrite à la section «Configuration du nœud», à la page 92.
2. Configurez la connectivité pour le trafic dépendant, selon la procédure décrite à la section «Configuration de la connectivité», à la page 94. (Si vous utilisez une passerelle SNA ou un DLUR en amont, configurez le lien vers le nœud en amont au lieu de le configurer directement vers l'hôte.)

Pour configurer une LUA, vous devez disposer des informations suivantes :

- Nom de la LU ou du groupe de LU ;
- Numéro de chaque LU ; le numéro de LU doit correspondre à celui configuré sur l'hôte.

Pour configurer une LUA, définissez la LU en suivant la procédure ci-après :

1. Sélectionnez le poste de liaison vers l'hôte dans la sous-fenêtre de connectivité de la fenêtre Nœud.
2. Cliquez sur **Nouveau**.
3. Dans la boîte de dialogue qui apparaît, sélectionnez **Nouvelle LU pour LUA**.
4. Entrez les valeurs appropriées dans les diverses zones de la boîte de dialogue. Définissez une LU de type `Sans restriction`.
5. Cliquez sur **OK**. La LU apparaît dans la sous-fenêtre de connectivité de la fenêtre Nœud, au-dessous du poste de liaison vers l'hôte.
6. Si vous prévoyez d'utiliser des groupes de LU, définissez-les selon la procédure décrite à la section «Définition d'un groupe de LU», à la page 99.

Configuration d'une LU 0

La LU principale d'une LU 0 prend en charge la communication avec les LU situées sur les nœuds secondaires (tels que les contrôleurs de magasin). Ce type de LU peut prendre en charge à la fois les sessions de LU 0 principales avec le contrôleur situé en aval et les sessions en mode émulation entre l'hôte et la LU secondaire. La LU 0 principale requiert une ligne SDLC principale utilisant les protocoles EIA-232D ou EIA-422A.

La LU 0 secondaire prend en charge la communication avec l'hôte. Elle fonctionne comme une application SNA générique utilisant le pilote de périphérique générique SNA de CS/AIX.

Remarque : Pour les nouvelles applications LU 0 secondaires, utilisez l'API LUA au lieu de l'API LU 0. Pour plus d'informations sur la configuration des LUA, reportez-vous à la section «Configuration des LUA», à la page 106.

Configuration d'une LU 0 principale

Avant de configurer une LU 0 principale, vous devez effectuer les opérations de configuration suivantes :

1. Configurez le nœud selon la procédure décrite à la section «Configuration du nœud», à la page 92.

Avant de configurer la LU 0 principale, vous devez rassembler les informations suivantes :

- Protocole SDLC utilisé pour la ligne principale (EIA-232D ou EIA-422A) ;
- Adresse du poste local de la ligne principale ;
- Adresse du poste éloigné de la ligne principale ;
- Une requête INIT-SELF provenant d'un poste en aval peut-elle lancer l'application de la LU principale sur le nœud local ?
- Nom de l'application de la LU 0 principale située sur le nœud local (si les requêtes INIT-SELF sont acceptées) ;
- Adresses de la LU principale sur le nœud local.

Pour configurer la LU 0 principale, suivez la procédure ci-après :

1. Configurez une ligne principale LU 0 :
   a. Sélectionnez **Nouvelle ligne principale LU 0** à partir du menu **Services** de la fenêtre Nœud.

      CS/AIX affiche alors la boîte de dialogue Configuration d'une ligne principale LU 0.
   b. Entrez les valeurs appropriées dans les diverses zones de cette boîte de dialogue.
   c. Cliquez sur **OK** pour définir la ligne principale LU 0.

   Configurez une LU principale pour la LU 0 :
   a. Sélectionnez **Nouvelle LU principale LU 0** à partir du menu **Services** de la fenêtre Nœud.

      CS/AIX affiche alors la boîte de dialogue Configuration d'une LU principale LU 0.
   b. Entrez les valeurs appropriées dans les diverses zones de la boîte de dialogue.
   c. Cliquez sur **OK** pour définir la LU principale LU 0.
2. Lancez le serveur LU 0 utilisé pour la ligne principale vers le poste en aval. Pour ce faire, entrez la commande suivante sur la ligne de commande AIX (où *Nom_ligne* est la ligne principale) :

   lu0 -p *Nom_ligne* **-b -t &**

Configuration d'une LU 0 secondaire

Avant de configurer une LU 0 secondaire, vous devez effectuer les opérations de configuration suivantes :

1. Configurez le nœud selon la procédure décrite à la section «Configuration du nœud», à la page 92. Si aucun autre hôte n'utilise le support PU fourni par le point de contrôle du nœud, vous pouvez entrer l'ID du nœud local dans la boîte de dialogue Paramètres du nœud.
2. Configurez la connectivité selon la procédure décrite à la section «Configuration de la connectivité», à la page 94. En revanche, si un autre système hôte utilise le support PU fourni par le point de contrôle du nœud, entrez l'ID du nœud local dans la boîte de dialogue Configuration des postes de liaison. Indiquez également l'adresse de liaison éloignée de la PU hôte.

Avant de configurer la LU 0 secondaire, vous devez rassembler les informations suivantes :

- Adresse de LU locale pour la LU secondaire utilisée pour communiquer avec l'hôte.
- Nom de la LU de session pour la configuration.
- Si vous voulez limiter la LU aux communications avec un SSCP déterminé, vous devez connaître l'ID du SSCP.
- La LU peut-elle envoyer une requête INIT-SELF à l'hôte ?
- Nom de l'application hôte ou du programme de service (si la LU peut envoyer des requêtes INIT-SELF).
- Entrée de table en mode journal (si la LU peut envoyer une requête INIT-SELF).
- Si la LU prend en charge l'émulation vers une LU principale, vous devez connaître le nom du profil de configuration de la LU principale (uniquement si la LU n'envoie pas de requête INIT-SELF).

Pour configurer la LU secondaire d'une LU 0, utilisez la procédure suivante, à partir de la fenêtre Nœud :

1. Sélectionnez le poste de liaison vers l'hôte dans la sous-fenêtre de connectivité de la fenêtre Nœud.
2. Cliquez sur **Nouveau**.
3. Dans la boîte de dialogue qui apparaît, sélectionnez **Nouvelle LU pour LUA** et cliquez sur **OK**.

   CS/AIX affiche alors la boîte de dialogue LU de type 0 à 3.
4. Entrez les valeurs appropriées dans les diverses zones de la boîte de dialogue. Définissez une LU de type `Sans restriction`.
5. Cliquez sur **Param. avancés**.

   CS/AIX affiche la boîte de dialogue Paramètres avancés d'une LU de type 0 à 3.
6. Dans la zone *Utilisation de la LU*, sélectionnez `LU0 secondaire`. La boîte de dialogue Motif est agrandie de manière à pouvoir contenir les zones correspondant à la LU 0 secondaire.
7. Entrez les valeurs appropriées dans les diverses zones de la boîte de dialogue.
8. Cliquez sur **OK** pour définir la LU.

   Celle-ci apparaît dans la sous-fenêtre de connectivité de la fenêtre Nœud, sous le poste de liaison vers l'hôte.
9. Pour lancer le serveur LU 0 utilisé pour la liaison vers l'hôte, entrez la commande suivante sur la ligne de commande AIX, en indiquant le nom du poste de liaison vers l'hôte :

   lu0
   -s *NomLiaison* **-b -t &**
10. Pour lancer l'application LU 0, indiquez le nom de la LU secondaire LU 0 en tant que paramètre.

Configuration d'une passerelle SNA

CS/AIX assure un accès direct à l'ordinateur hôte et permet en outre de bénéficier des fonctions de passerelle SNA. Ces fonctions permettent aux ordinateurs d'accéder à un système hôte à l'aide d'un nœud CS/AIX, sans nécessiter chacun une connexion distincte.

La fonction passerelle SNA est représentée à la figure 8, à la page 110.

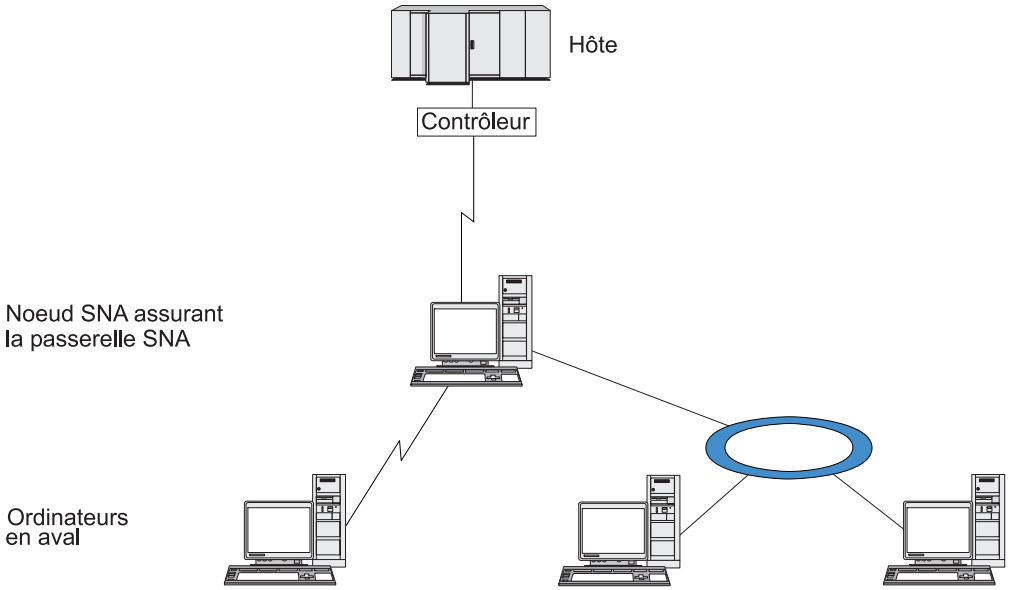

Figure 8. Passerelle SNA

L'ordinateur en aval doit être doté d'une PU SNA de type 2.0 ou 2.1 pour prendre en charge les LU dépendantes. Par exemple, l'ordinateur en aval peut être un autre ordinateur CS/AIX ou un PC exécutant Communications Server pour Windows NT.

Si le nœud CS/AIX local utilise la fonction passerelle SNA, toutes les données transmises entre les ordinateurs hôte et en aval sont acheminées à l'aide du nœud local. Ceci permet à un ordinateur en aval de partager une connexion hôte avec CS/AIX ou avec d'autres ordinateurs en aval, sans avoir recours à une liaison directe. Vous pouvez, par exemple, configurer plusieurs ordinateurs en aval connectés à CS/AIX à travers un réseau en anneau à jeton, afin qu'ils puissent tous accéder à la même ligne longue distance non commutée, de CS/AIX vers l'hôte.

Le recours à une passerelle SNA simplifie également la configuration au niveau de l'hôte en supprimant la nécessité de définir les ordinateurs en aval et les liaisons de communication correspondantes. La configuration de l'hôte ne doit comprendre que l'ordinateur CS/AIX et la liaison de communication hôte correspondante. Les LU des ordinateurs en aval sont configurées en tant que ressources de l'ordinateur CS/AIX. L'ordinateur hôte ne reçoit pas d'informations indiquant qu'une passerelle SNA est en cours d'utilisation.

Avant de configurer la passerelle SNA, vous devez effectuer les opérations de configuration suivantes :

- Définissez le nœud local selon la procédure décrite à la section «Configuration du nœud», à la page 92.
- Configurez un port et un poste de liaison pour le trafic dépendant entre le nœud local et l'hôte, selon la procédure décrite à la section «Configuration de la connectivité», à la page 94. Configurez également des ports et des postes de liaison pour le trafic dépendant entre le nœud local et les nœuds en aval. Pour prendre en charge des LU en aval non définies préalablement, vous pouvez définir un modèle sur le port, afin de supporter les PU implicites et les LU en aval (reportez-vous à la section «Prise en charge de LU en aval implicites», à la page 111).

- Définissez les LU du nœud local qui sont utilisées pour la communication avec l'hôte (LU en amont). Définissez les LU en amont en tant que LU de type 0 à 3 avec une LU de type `sans restriction` (`inconnu`). (Les LU situées au niveau des nœuds en aval peuvent être de tout type.)
- Si vous prévoyez d'utiliser des groupes de LU, définissez-les selon la procédure décrite à la section «Définition d'un groupe de LU», à la page 99.

Prise en charge de LU en aval implicites

Pour prendre en charge des LU en aval non prédéfinies pour CS/AIX, vous pouvez définir un modèle sur le port pour les PU et LU en aval implicites (pour plus de détails sur la configuration de base du port, reportez-vous à la section «Configuration de la connectivité», à la page 94). Ces modèles permettent de prendre en charge les LU en aval. Ainsi, il n'est pas nécessaire de configurer une LU sur le nœud local pour supporter chaque LU située sur un nœud en aval.

Avant de configurer une LU en aval pour une passerelle SNA, vous devez disposer des informations suivantes :

- Série de numéros de LU prenant en charge les LU en aval
- Nom de la LU hôte

Pour définir un modèle de LU en aval implicites, suivez les étapes ci-après :

1. Si le port est déjà configuré, cliquez deux fois sur la définition de port dans la sous-fenêtre de connectivité. CS/AIX affiche alors la boîte de dialogue de configuration du port.

   Si vous n'avez pas encore configuré le port, faites-le maintenant :

   a. Sélectionnez la sous-fenêtre de connectivité dans la fenêtre Nœud.
   b. Cliquez sur **Nouveau**.
   c. Dans la boîte de dialogue qui apparaît, sélectionnez l'option de définition de port, puis choisissez un type de protocole de liaison.

      CS/AIX affiche alors la boîte de dialogue de configuration du port.
   d. Entrez les paramètres de port de base, selon la procédure indiquée à la section «Configuration de la connectivité», à la page 94.
2. Cliquez sur le bouton **Param. avancés**, dans la partie inférieure de la boîte de dialogue.

   CS/AIX affiche alors la boîte de dialogue de Paramètres du port. La sous-fenêtre inférieure contient les paramètres affectant les modèles de LU en aval.
3. Sélectionnez l'option *Configuration des LU en aval pour un accès aux PU implicites*.
4. Cliquez sur **OK**.

   CS/AIX affiche alors la boîte de dialogue Configuration d'un modèle de LU en aval.
5. Entrez les valeurs appropriées dans les diverses zones de la boîte de dialogue.
6. Cliquez sur **OK** pour définir le modèle de LU en aval implicite.

Définition de LU en aval

Avant de configurer une LU en aval pour une passerelle SNA, vous devez disposer des informations suivantes :

- Nom de chaque LU en aval (identificateur local qui ne doit pas nécessairement correspondre à la configuration du système en aval)
- Numéro de chaque LU en aval

- Poste de liaison vers le nœud en aval
- Nom de la LU en amont (pour la LU hôte)

Avant de configurer une LU en aval pour une passerelle SNA, suivez les étapes ci-après :

1. Sélectionnez le poste de liaison vers le nœud en aval dans la sous-fenêtre de connectivité de la fenêtre Nœud.
2. Cliquez sur **Nouveau**.
3. Sélectionnez **Nouvelle LU en aval** et cliquez sur **OK**.

   CS/AIX affiche alors la boîte de dialogue LU en aval.
4. Entrez les valeurs appropriées dans les diverses zones de la boîte de dialogue.
5. Cliquez sur **OK** pour définir la LU en aval.

   La définition de LU apparaît alors dans la sous-fenêtre de connectivité, au-dessous du poste de liaison vers le nœud en aval.

Configuration d'un demandeur de LU dépendante (DLUR)

CS/AIX assure un accès direct à un ordinateur hôte et permet en outre de bénéficier de la fonction DLUR (demandeur de LU dépendante). Cette fonction permet aux sessions de LU dépendantes de desservir plusieurs nœuds sur un réseau APPN, sans nécessiter de connexion directe vers l'hôte.

En principe, une session LU dépendante requiert un lien de communication direct vers l'ordinateur hôte. Si de nombreux nœuds (y compris un nœud hôte) sont connectés ensemble sur un réseau APPN, certains d'entre eux peuvent ne pas être connectés directement à l'hôte. Dans ce cas, ils disposent d'une connexion indirecte à travers un autre nœud. Il est impossible d'établir des sessions LU dépendantes vers l'hôte à partir des LU situées sur des nœuds ne bénéficiant pas d'une connexion directe.

La fonction DLUR (Demandeur de LU dépendante) est un utilitaire APPN conçu pour parer à cette restriction.

Le DLUR d'un nœud APPN (tel qu'un nœud CS/AIX) fonctionne en association avec un serveur de LU dépendante (DLUS) au niveau du système hôte. Il permet d'acheminer des sessions à partir de LU dépendantes (sur le nœud du DLUR à travers le réseau APPN) vers le système hôte du DLUS. Le chemin vers l'hôte peut desservir plusieurs nœuds et bénéficier des fonctions de gestion de réseau APPN, de localisation automatique des ressources et de calcul de route. Le DLUR doit être disponible sur le nœud où résident les LU, tandis que le DLUS doit être disponible sur le nœud hôte. En revanche, le DLUR n'est requis sur aucun nœud intermédiaire du chemin de la session en cours.

Si le nœud du DLUR CS/AIX est un nœud de réseau ou un nœud de réseau de type branche, il peut également fournir des fonctions d'émulation DLUR pour les LU dépendantes situées sur des ordinateurs en aval connectés au nœud CS/AIX. Ces LU peuvent utiliser le DLUR du nœud CS/AIX pour accéder au système hôte à travers le réseau, comme le feraient des LU situées sur le nœud. Les systèmes en aval n'exécutent pas DLUR et n'ont pas besoin de savoir que DLUR est en cours d'utilisation.

La figure 9, à la page 113 présente un serveur CS/AIX configuré sous la forme d'un nœud de réseau APPN, mettant en œuvre une émulation DLUR prenant en

charge les sessions entre les différentes LU du système hôte (nœud en amont)et les LU situées sur les nœuds du réseau APPN (nœuds en aval).).

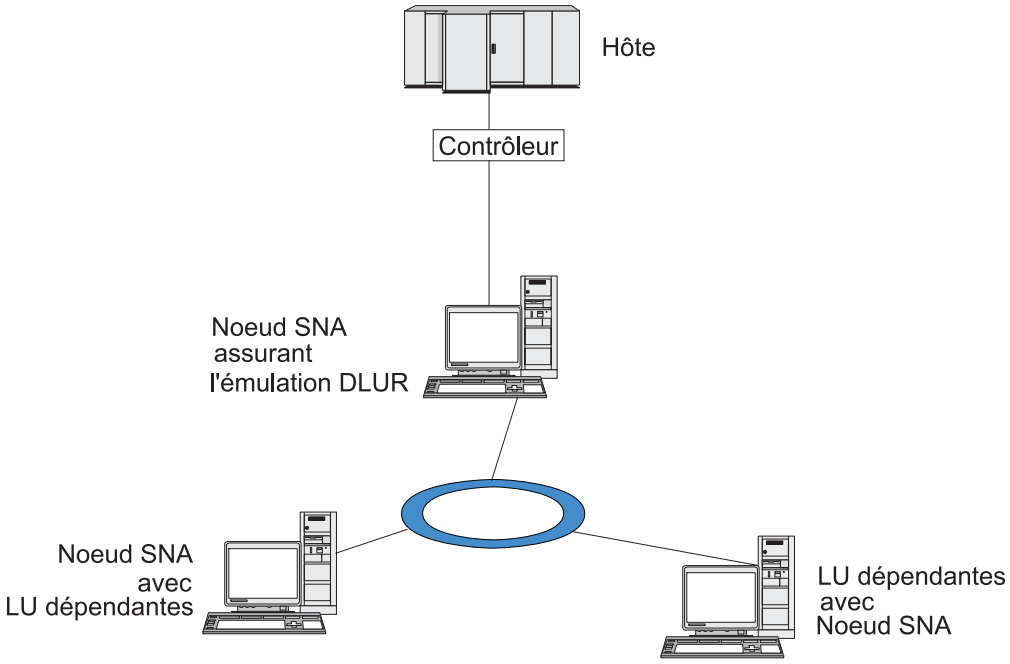

Figure 9. Nœud CS/AIX fournissant une émulation DLUR

Remarque :

1. Il est impossible de configurer un DLUR sur un nœud LEN.
2. Il est possible de configurer une émulation DLUR uniquement sur un nœud de réseau ou un nœud de réseau de type branche.
3. Si vous utilisez Branch Extender, vous ne pouvez pas configurer l'émulation DLUR sur un nœud d'extrémité de la branche (ayant comme serveur de nœud de réseau un nœud de réseau de type branche). Cependant, vous pouvez prendre en charge des applications de LU dépendantes à partir de ce nœud en configurant une émulation DLUR sur le nœud de réseau de type branche (de sorte que le nœud d'extrémité de la branche n'exécute pas DLUR mais utilise l'émulation DLUR sur le nœud de réseau de type branche).

Les opérations nécessaires à la configuration d'un DLUR varient selon que les LU dépendantes sont situées sur le nœud local ou sur les nœuds en aval.

Configuration d'un support DLUR sur le nœud local

Pour effectuer cette opération, vous devez disposer des informations suivantes :

- ID de la PU située sur le nœud local
- Nom de la PU (identificateur local qui ne doit pas nécessairement correspondre à la configuration hôte)
- Nom du DLUS sur l'hôte (et nom du DLUS de secours, le cas échéant)
- Nom, numéro et type de LU de chaque LU en aval. Le numéro de LU doit correspondre au numéro configuré sur l'hôte.

Pour configurer un support DLUR sur le nœud local, vous devez effectuer les opérations de configuration suivantes :

1. Définissez le nœud local selon la procédure décrite à la section «Configuration du nœud», à la page 92. Si le support DLUR en accès transparent est configuré pour la prise en charge des nœuds en aval, définissez le nœud en tant que nœud de réseau APPN ou nœud réseau de type branche.
2. Configurez la connectivité vers un réseau APPN. La connectivité APPN requiert au moins un port et un poste de liaison pour le trafic indépendant entre le nœud local et le nœud de réseau APPN adjacent (reportez-vous à la section «Configuration de la connectivité», à la page 94).
3. Définissez une PU de DLUR sur le nœud local (la PU du DLUR prend en charge la connectivité vers l'hôte).

   Pour configurer une PU DLUR, suivez les étapes ci-après à partir de la fenêtre Nœud :

   a. Sélectionnez le menu **Services**, puis le sous-menu **Connectivité** et ensuite **Nouvelle PU du DLUR** (ou cliquez su **Nouveau** dans la barre des boutons, puis sélectionnez **PU du DLUR**).

      Lorsque vous cliquez sur **OK**, CS/AIX affiche la boîte de dialogue de configuration de la PU du DLUR.

   b. Entrez les valeurs appropriées dans les diverses zones de la boîte de dialogue.

   c. Cliquez sur **OK** pour définir une PU de DLUR.

      Celle-ci apparaît dans la sous-fenêtre de connectivité au-dessous de l'élément DLUR.
4. Pour configurer un DLUR de façon à assurer la prise en charge des LU sur le nœud local, ajoutez les LU au nœud local. Les LU doivent être configurées de façon à prendre en charge les LUA, comme décrit dans «Configuration des LUA», à la page 106. Selon les besoins des applications utilisateur prises en charge par les LU, vous devez également effectuer d'autres configurations.

Configuration d'un support d'émulation DLUR pour les nœuds en aval

Pour effectuer cette opération, vous devez disposer des informations suivantes :

- Nom de la PU en aval de chaque nœ en aval, ou nom de chaque PU du nœ en aval (identificateur local qui ne doit pas nécessairement correspondre à la configuration hôte)
- Nom des DLUS sur l'hôte.

Pour configurer un support d'émulation DLUR pour les nœuds en aval, vous devez effectuer les opérations de configuration suivantes :

1. Définissez le nœud local en tant que nœud de réseau APPN (reportez-vous à la section «Configuration du nœud», à la page 92).
2. Configurez la connectivité sur les nœuds en aval. Configurez également des ports et des postes de liaison pour le trafic dépendant entre le nœud local et chaque nœud en aval, selon la procédure décrite à la section «Configuration de la connectivité», à la page 94. (Il n'est pas nécessaire de définir une PU de DLUR pour prendre en charge la fonction émulation DLUR pour les nœuds en aval.)

3. Un nœud en aval peut prendre en charge plusieurs PU. Dans ce cas, chaque PU en aval est associée à un lien distinct. Vous devez donc configurer plusieurs liens entre le nœud DLUR CS/AIX et le nœud en aval et connaître le nom de la PU en aval de chaque lien.

Configuration d'un serveur TN

Les programmes d'émulation 3270 qui communiquent sur un réseau TCP/IP (et non un réseau SNA) sont désignés par le terme Programmes TN3270 (programmes d'émulation Telnet 3270).

Les programmes TN3270 peuvent également prendre en charge TN3270E (extensions standard de Telnet 3270). TN3270E est un protocole ouvert prenant en charge l'émulation 3270 (à la fois pour les terminaux et pour les imprimantes) à l'aide de Telnet. Il permet à un client Telnet de sélectionner un périphérique particulier (en indiquant le nom de la LU) et fournit un support amélioré pour diverses fonctions, y compris la gestion des touches ATTN et SYSREQ et de la réponse SNA.

Remarque : Dans le présent manuel, le terme TN3270 est utilisé pour des informations s'appliquant à la fois aux protocoles TN3270, TN3287 et TN3270E.

Le serveur TN de CS/AIX permet aux utilisateurs de TN3270 installés sur d'autres postes de travail d'accéder aux ordinateurs hôte 3270. Il permet également aux utilisateurs de TN3270 de partager une connexion hôte avec CS/AIX ou avec d'autres utilisateurs de TN3270, sans avoir recours à une liaison directe. Enfin, grâce au serveur TN, les utilisateurs de TN3270 peuvent accéder à des systèmes hôte n'exécutant pas TCP/IP.

La figure 10, à la page 116 représente un nœud CS/AIX prenant en charge un serveur TN pour des clients TN3270. Le nœud du serveur TN et les clients communiquent par le biais du réseau TCP/IP.

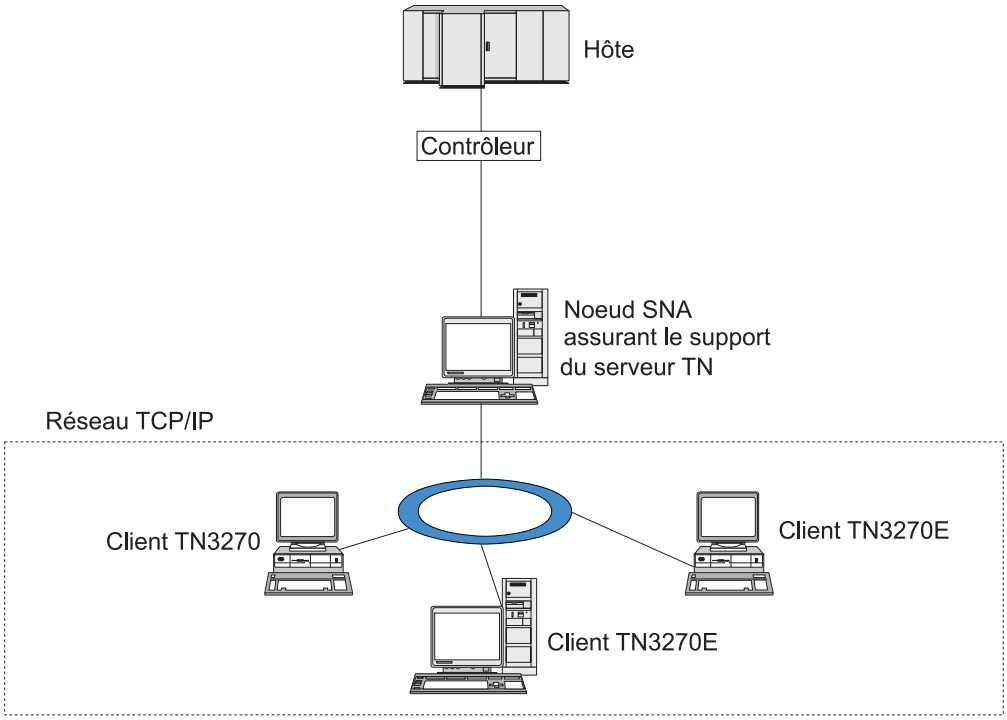

Figure 10. Nœud CS/AIX configuré pour un serveur TN

Le serveur TN CS/AIX permet d'associer un utilisateur TN3270 et une LU 3270 CS/AIX. Toutes les données provenant de l'utilisateur TN3270 sont acheminées vers la LU. Cela signifie que la configuration de l'hôte et de l'utilisateur TN3270 est la même que s'ils étaient connectés directement ; aucun des deux éléments n'a besoin d'être informé du fait que les données sont acheminées par le serveur TN.

Le serveur TN CS/AIX prend en charge tous les programmes d'émulation client TN3270 qui mettent correctement en œuvre les protocoles définis dans les documents RFC 1123, 1576, 1646, 1647 et 2355 de l'IETF.

Lorsqu'un programme TN3270 communique avec le serveur TN, CS/AIX identifie ce programme à l'aide de l'adresse TCP/IP de l'ordinateur sur lequel il est exécuté. CS/AIX ne peut pas distinguer deux programmes TN3270 utilisés par des utilisateurs distincts sur un même ordinateur. Dans la documentation CS/AIX, le terme serveur TN désigne l'ordinateur sur lequel un programme TN3270 est exécuté et ne fait pas référence à un utilisateur particulier de ce programme.

La figure 11, à la page 117 illustre les relations entre l'hôte et le serveur TN et la configuration du serveur TN.

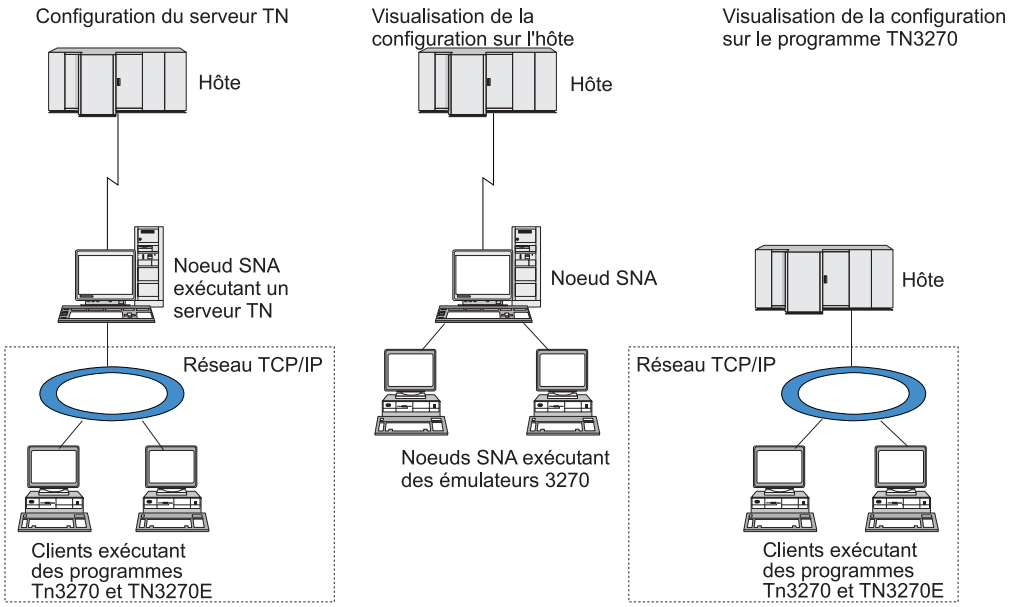

Figure 11. Serveur TN

Chaque utilisateur de serveur TN qui se connecte à CS/AIX à l'aide du composant Serveur TN3270 est généralement configuré pour accéder à une seule LU 3270 et ne peut donc établir qu'une session hôte à la fois. Cependant, vous pouvez également configurer un utilisateur de serveur TN pour qu'il accède au groupe de LU 3270 au lieu de disposer d'une seule LU 3270 par utilisateur. Ceci permet aux utilisateurs d'accéder à autant de sessions qu'il y a de LU disponibles dans le groupe.

Pour configurer l'accès au serveur TN, vous devez effectuer les opérations suivantes :

- Définissez le nœud local selon la procédure décrite à la section «Configuration du nœud», à la page 92.
- Configurez un port et un poste de liaison pour le trafic dépendant entre le nœud local et l'hôte, selon la procédure décrite à la section «Configuration de la connectivité», à la page 94.

Pour configurer l'accès au serveur TN, effectuez les tâches de configuration suivantes :

- Définissez les LU 3270 du nœud local qui sont utilisées pour la communication avec l'hôte. Pour ajouter des LU, reportez-vous à la section «Définition de LU 3270».
- Si vous prévoyez d'utiliser des groupes de LU, définissez-les selon la procédure décrite à la section «Définition d'un groupe de LU», à la page 118.

Définition de LU 3270

Avant de configurer la LU 3270, rassemblez les informations suivantes :

- Nom de la LU (identificateur local qui ne doit pas nécessairement correspondre à la configuration hôte)
- Numéro de la LU (ou numéro de chaque LU d'une série)
- Type de LU (modèle d'affichage 3270 ou imprimante 3270)
- Nom du groupe (si vous ajoutez la LU à un groupe)

Pour configurer une LU de type 0 à 3 pour poste de liaison précédemment défini, effectuez les étapes suivantes à partir de la fenêtre Nœud :

1. Sélectionnez le poste de liaison vers l'hôte dans la sous-fenêtre de connectivité.
2. Cliquez sur **Nouveau**.
3. Sélectionnez le type de LU (nouvelle LU d'écran 3270 ou nouvelle LU d'imprimante 3270) dans la boîte de dialogue qui apparaît.

   Cliquez ensuite sur **OK**. CS/AIX affiche alors la boîte de dialogue LU de type 0 à 3.
4. Entrez les valeurs appropriées dans les diverses zones de la boîte de dialogue.
5. Cliquez sur **OK** pour définir la LU.

   Celle-ci apparaît dans la sous-fenêtre de connectivité de la fenêtre Nœud, sous le poste de liaison vers l'hôte.

Définition d'un groupe de LU

Avec 3270, vous pouvez définir des groupes de LU pour simplifier la configuration utilisateur et la procédure d'établissement de sessions hôte. Vous pouvez, par exemple, définir plusieurs LU 3270 dans un seul groupe de LU, puis configurer plusieurs clients TN3270 avec ce groupe de LU. Ceci facilite la configuration des sessions 3270 et permet à tout client d'utiliser n'importe quelle LU du groupe.

Remarque : Vous pouvez attribuer un client TN3270 à une LU particulière ou à un groupe de LU.

- Si vous attribuez le client à une LU particulière appartenant à un groupe, le client utilise cette LU si elle est disponible. Sinon il utilise n'importe quelle LU disponible du groupe, comme si vous l'aviez attribué au groupe de LU au lieu de l'attribuer à une LU particulière.
- Si vous souhaitez que le client utilise uniquement une LU particulière, afin que la session client ne puisse pas être établie si la LU est déjà utilisée, veillez à ce que la LU n'appartienne à aucun groupe.

Vous pouvez visualiser les groupes de LU du nœud CS/AIX local à l'aide de la fenêtre Groupes de LU. Cette fenêtre énumère les groupes de LU configurés sur le système local et vous permet de sélectionner les LU que vous voulez ajouter à un groupe.

Vous pouvez ajouter les types de LU suivants à un groupe à utiliser sous 3270 (ne mélangez pas des LU de types différents au sein d'un même groupe) :

- LU d'écran 3270
- LU sans restriction

Avant d'ajouter des LU à un groupe, vous devez définir celles-ci sur le nœud local.

Pour configurer un groupe de LU, effectuez les étapes ci-après à partir de la fenêtre Nœud :

1. Sélectionnez **Groupes de LU** à partir du menu **Fenêtres**.

   CS/AIX affiche alors la fenêtre Groupes de LU.
2. Cliquez sur **Nouveau**.

   CS/AIX affiche la boîte de dialogue Configuration d'un groupe de LU.

La zone de droite énumère les LU qui ne sont attribuées à aucun groupe. Chacune de ces LU peut être ajoutée au nouveau groupe.

3. Sélectionnez la ou les LU que vous voulez ajouter, puis cliquez sur **Nouveau** pour déplacer la sélection vers la zone de gauche.

   Pour supprimer une LU de la zone de gauche, sélectionnez-la et cliquez sur **Suppression**.

4. Cliquez sur **OK** pour définir le groupe de LU.

   Toutes les LU apparaissant dans la zone de gauche sont ajoutées au groupe.

   Celui-ci apparaît alors dans la fenêtre Groupes de LU.

Configuration du serveur TN3270

Avant de configurer le serveur TN3270, vous devez disposer des informations suivantes :

- Le serveur supporte-t-il uniquement TN3270 ou reconnaît-il également TN3270E (qui prend en charge TN3270) ?
- Un client TN3270E peut-il interroger une LU déterminée ?
- Noms des LU écran et imprimante (ou nom du groupe de LU) pour chaque client. (Les noms de LU d'imprimante sont requis uniquement si votre système prend en charge TN3270E.)
- Nom ou adresse TCP/IP du client (si seuls certains clients sont autorisés ou si vous voulez limiter les droits d'accès de certains clients à des LU déterminées).
- Numéro du port TCP/IP situé sur le nœud du serveur TN.
- Le chiffrement de données, l'authentification du client et l'authentification du serveur sont-ils requis (cette option n'est disponible que si le logiciel supplémentaire requis est installé) ?
- Le serveur TN3270 est-il utilisé dans un réseau SLP ?

Pour associer une LU d'écran à une LU d'imprimante, vous devez disposer du nom de ces LU. L'enregistrement des associations du serveur TN définit une association entre une LU d'imprimante et une LU d'écran permettant au protocole TN3270E de les connecter. Il n'est pas nécessaire de définir un enregistrement d'association si TN3270E n'est pas pris en charge ou si les LU d'imprimante ne sont pas prises en charge.

L'enregistrement des paramètres par défaut du serveur TN définit les paramètres utilisés sur toutes les sessions client TN3270. Vous pouvez définir un enregistrement des paramètres par défaut unique pour chaque serveur.

Pour configurer un serveur TN3270, suivez les étapes ci-après à partir de la fenêtre Nœud :

1. Définissez un enregistrement des accès au serveur TN :
   a. Sélectionnez **Serveur TN** à partir du menu **Services**.

      CS/AIX affiche alors la fenêtre Serveur TN. Elle énumère tous les enregistrements des accès au serveur TN dans la sous-fenêtre supérieure et tous les enregistrements des associations dans la sous-fenêtre inférieure.

   b. Sélectionnez la sous-fenêtre contenant les enregistrements des accès au serveur TN3270, puis cliquez sur **Nouveau**.

      CS/AIX affiche alors la boîte de dialogue Accès au serveur TN.

   c. Entrez les valeurs appropriées dans les diverses zones de la boîte de dialogue.

d. Cliquez sur **OK** pour définir l'enregistrement des accès au serveur TN. Cet enregistrement apparaît alors dans la fenêtre Serveur TN.

2. Définissez un enregistrement des associations du serveur TN :
   a. Sélectionnez la sous-fenêtre contenant les enregistrements des associations dans la fenêtre Serveur TN et cliquez sur **Nouveau**.

      CS/AIX affiche alors la boîte de dialogue des enregistrements des associations du serveur TN.
   b. Entrez les valeurs appropriées dans les diverses zones de la boîte de dialogue.
   c. Cliquez sur **OK** pour définir l'enregistrement des associations du serveur TN. Cet enregistrement apparaît alors dans la fenêtre Serveur TN.
3. Si vous avez besoin de forcer des réponses lors des sessions d'impression, précisez une méthode de mise au repos pour toutes les sessions TN3270, indiquez comment accéder au serveur LDAP externe qui détient une liste de révocation servant à vérifier l'autorisation des clients TN3270 ou utilisez TN3270 SLP (Service Location Protocol). Pour ce faire, utilisez la boîte de dialogue des paramètres avancés du serveur TN.

Pour plus d'informations sur la configuration de la prise en charge SSL pour le serveur TN, consultez les pages Web de support d'IBM Communications Server à l'adresse : http://www.ibm.com/software/network/commserver/support/.

Configuration du redirecteur TN

La fonction de redirection TN de CS/AIX assure des fonctions d'accès transparent TCP/IP aux clients TN3270, TN3270E, TN5250 et VT désignés collectivement par clients Telnet. L'utilisateur Telnet communique avec CS/AIX via une connexion TCP/IP ; CS/AIX communique ensuite avec l'hôte via une autre connexion TCP/IP. Cela permet d'utiliser le contrôle d'autorisation d'accès SSL (Secure Sockets Layer) uniquement lorsque cela est nécessaire, et non sur l'ensemble de la connexion entre l'utilisateur et l'hôte. Exemples :

- Si les postes client sont connectés à CS/AIX via un réseau local TCP/IP pour lequel aucune vérification n'est nécessaire et à un hôte éloigné qui nécessite SSL, vous pouvez utiliser SSL via la connexion TCP/IP entre CS/AIX et l'hôte. Cela signifie que la sécurité est vérifiée une fois pour tous les clients et que les clients individuels n'ont pas besoin de fournir des informations de sécurité.
- Si CS/AIX est installé sur le même site que l'hôte mais que les clients se connectent depuis des sites externes, vous pouvez utiliser SSL via les connexions client à CS/AIX sans avoir à installer le logiciel SSL sur l'hôte.

Configuration du redirecteur TN

Avant de configurer l'accès au Redirecteur TN, vous devez définir le nœud local selon la procédure décrite dans la section «Configuration du nœud», à la page 92. Les informations suivantes sont également nécessaires :

- Nom ou adresse TCP/IP du client si seuls certains clients sont autorisés.
- Numéro de port TCP/IP utilisé par le client pour se connecter au nœud de Redirecteur TN.
- Nom ou adresse TCP/IP de l'hôte.
- Numéro de port TCP/IP utilisé par le nœud de Redirecteur TN pour se connecter à l'hôte.

- Le chiffrement de données, l'authentification du client et l'authentification du serveur sont-ils requis entre le client et le nœud de Redirecteur TN (cette option n'est disponible que si le logiciel supplémentaire requis est installé) ?
- Le chiffrement de données SSL est-il requis entre le nœud de Redirecteur TN et l'hôte ?

L'enregistrement des paramètres par défaut du Redirecteur TN définit les paramètres utilisés sur toutes les sessions client du Redirecteur TN. Vous pouvez définir un enregistrement des paramètres par défaut unique pour chaque numéro de port TCP/IP client.

Pour configurer un Redirecteur TN, suivez les étapes ci-après à partir de la fenêtre Nœud pour définir un enregistrement d'accès au Redirecteur TN :

1. Sélectionnez **Serveur TN** à partir du menu **Services**.

   CS/AIX affiche alors la fenêtre Serveur TN. Celle-ci répertorie tous les enregistrements d'accès au serveur TN3270, les enregistrements d'association du serveur TN3270 et les enregistrements d'accès au Redirecteur TN.
2. Sélectionnez la sous-fenêtre contenant les enregistrements des accès au Redirecteur TN, puis cliquez sur **Nouveau**.

   CS/AIX affiche alors la boîte de dialogue Accès au Redirecteur TN.
3. Entrez les valeurs appropriées dans les diverses zones de la boîte de dialogue.
4. Cliquez sur **OK** pour définir l'enregistrement des accès au Redirecteur TN. Cet enregistrement apparaît alors dans la sous-fenêtre Redirecteur TN de la fenêtre Serveur TN.

Remarque : Le redirecteur TN peut être utilisé uniquement si le nœud SNA est actif, bien qu'il n'utilise aucune des ressources SNA du nœud.

Configuration d'AnyNet

CS/AIX comporte la fonction AnyNet APPC sur TCP/IP, laquelle prend en charge la conversion des protocoles et les communications entre des applications sur un réseau non natif. La fonction de nœud d'accès AnyNet APPC sur TCP/IP permet aux applications LU 6.2 (APPC) de communiquer sur un réseau TCP/IP, et la fonction de passerelle APPC sur TCP/IP permet aux applications APPC de communiquer sur un réseau en partie TCP/IP et en partie SNA. Pour plus d'informations sur APPC sur TCP/IP, voir le manuel *Communications Server for AIX AnyNet Guide to APPC over TCP/IP*.

La figure 12 représente un nœud d'accès APPC sur TCP/IP.

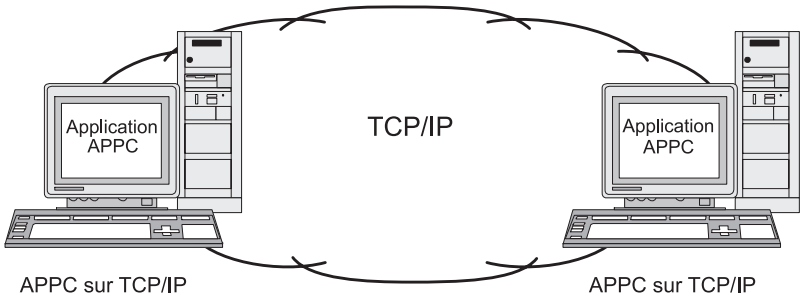

Figure 12. Nœud d'accès AnyNet APPC sur TCP/IP

La figure 13 représente une passerelle APPC sur TCP/IP.

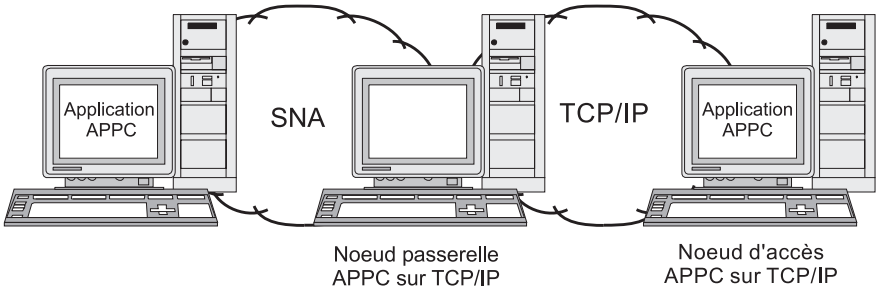

Figure 13. Passerelle AnyNet APPC sur TCP/IP

Configuration d'APPC sur TCP/IP

Avant de configurer APPC sur TCP/IP, vous devez effectuer les opérations de configuration suivantes :

1. Configurez le nœud selon la procédure décrite à la section «Configuration du nœud», à la page 92.

   Un nœud d'accès APPC sur TCP/IP peut être un nœud de réseau APPN, un nœud d'extrémité ou un nœud LEN. Dans le cas d'une passerelle APPC sur TCP/IP, le nœud local doit être un nœud de réseau.
2. Si vous configurez une passerelle APPC sur TCP/IP, configurez la connectivité vers le réseau SNA, selon la procédure décrite à la section «Configuration de la connectivité», à la page 94. (Cette étape est facultative pour les nœuds d'accès APPC sur TCP/IP.)

Avant de configurer APPC sur TCP/IP, vous devez rassembler les informations suivantes :

- Le système local est-il défini en tant que nœud d'accès APPC sur TCP/IP ou en tant que passerelle ? Si le système local est connecté à la fois à un réseau SNA et à un réseau TCP/IP, il peut être configuré en tant que passerelle permettant aux nœuds des deux réseaux de communiquer.
- Nom de domaine du réseau TCP/IP. Un nom de LU représenté sous la forme *NOM_RESEAU.NOM_LU* est converti en adresse TCP/IP sous la forme *NOM_LU.RESEAU.DOMAINE*. Le nom de domaine est configuré dans un fichier **/etc/hosts** ou sur une entrée DNS, sur le système local.
- Préférence de routage par défaut utilisée pour la recherche de LU (réseau SNA uniquement, réseau TCP/IP uniquement ou les deux).
- Si la préférence de routage par défaut n'inclut pas la recherche du réseau TCP/IP, vous devez disposer de la liste des LU à localiser à travers ce réseau. Les LU partenaires situées sur le réseau TCP/IP peuvent être les nœuds d'accès d'un réseau TCP/IP ou les LU d'un réseau SNA connecté au réseau TCP/IP par une passerelle APPC sur TCP/IP.
- Adresses Internet de chaque LU à localiser à travers le réseau TCP/IP. Cette information est configurée dans le fichier **/etc/hosts** ou sur le serveur DNS.

Pour configurer APPC sur TCP/IP, suivez la procédure ci-après :

1. Configurez les paramètres par défaut d'APPC sur TCP/IP :
   a. Sélectionnez l'option **AnyNet** du menu **Services** (fenêtre Nœud) et l'option **AnyNet** du sous-menu **AnyNet**.

      CS/AIX affiche la fenêtre AnyNet.

b. Sélectionnez l'option **Paramètres d'APPC sur TCP/IP** à partir du menu **Sélection**.

   CS/AIX affiche la boîte de dialogue Paramètres AnyNet APPC sur TCP/IP.

c. Entrez les valeurs appropriées dans les diverses zones de la boîte de dialogue.

d. Cliquez sur **OK**. La définition par défaut d'APPC sur TCP/IP apparaît dans la sous-fenêtre Sessions APPC sur TCP/IP de la fenêtre AnyNet.

2. Si vous n'avez pas défini de préférence de routage par défaut incluant le réseau TCP/IP, vous devez configurer chaque LU partenaire située sur le réseau TCP/IP :

   a. Sélectionnez la sous-fenêtre des systèmes éloignés de la fenêtre Nœud et cliquez sur **Nouveau**.

   b. Dans la boîte de dialogue qui apparaît, sélectionnez **LU partenaire sur nœud éloigné** et cliquez sur **OK**.

   c. Entrez le nom complet de la LU partenaire, et sélectionnez une option de routage AnyNet incluant le réseau TCP/IP.

   d. Cliquez sur **OK**. La définition de la LU partenaire apparaît dans la sous-fenêtre des systèmes éloignés de la fenêtre Nœud.

3. Configurez les adresses TCP/IP des LU partenaires. Vous pouvez ajouter une entrée du type ci-dessous au fichier **/etc/hosts** du système local ou au serveur DNS du réseau TCP/IP :

   adresse_notation_décimale_pointsLUNAME.NETWORKNAME.DOMAINNAME

   Pour une LU partenaire située sur un nœud d'accès APPC sur TCP/IP du réseau TCP/IP, utilisez l'adresse Internet du nœud. Pour une LU partenaire située sur un réseau SNA et connectée au réseau TCP/IP par une passerelle APPC sur TCP/IP, utilisez l'adresse Internet de la passerelle.

Désactivation de CS/AIX

La désactivation du logiciel CS/AIX arrête automatiquement le nœud CS/AIX et les éléments de connectivité correspondants. Elle met également fin à l'utilisation des ressources CS/AIX par tout autre traitement (programme d'émulation 3270, par exemple) sur ce serveur.

Avant d'arrêter les services individuels, il est recommandé d'attendre que tous les utilisateurs cessent de les utiliser. De même, ne désactivez pas le système tant qu'il existe une activité CS/AIX.

Si vous devez désactiver CS/AIX lorsque des utilisateurs sont actifs, prévenez-les de l'arrêt de CS/AIX et donnez-leur le temps de terminer leurs activités.

Si un programme d'émulation 3270 utilise les LU situées sur le nœud lors de la désactivation du logiciel, toutes les sessions d'émulation 3270 utilisant ces LU s'arrêtent. Le programme continue de fonctionner, mais les utilisateurs ne peuvent utiliser les sessions tant que le logiciel n'est pas réactivé. Les applications utilisant les API APPC, CSV, LUA, NOF ou MS sont averties par un code de retour `COMM_SUBSYSTEM_ABENDED` et les applications CP-CI, par un code de retour `CM_PRODUCT_SPECIFIC_ERROR`.

Désactivation de CS/AIX

Pour désactiver le logiciel CS/AIX, entrez la commande suivante à l'invite de commande AIX :

sna stop

Si la désactivation de CS/AIX est réussie, la commande **sna stop** renvoie un code de sortie `0`. Tout autre code de sortie indique qu'une erreur s'est produite et que CS/AIX n'a pas été désactivé. Pour plus d'informations sur les valeurs des codes de sortie, voir le manuel *Communications Server for AIX Diagnostics Guide*.

Chapitre 10. Sources d'informations pour CS/AIX et SNA

Ce chapitre recense les sources d'informations sur la technologie SNA et les différents produits et services proposés par IBM. Il décrit également les informations disponibles dans les forums du réseau.

Bibliothèque SNA

La bibliothèque SNA comprend des brochures marketing, des manuels, des guides de l'utilisateur et des tutoriels qui fournissent des informations de base ou approfondies sur les sujets suivants :

- La théorie SNA
- Les produits SNA
- La mise en œuvre des produits
- La configuration des systèmes et des réseaux
- Les programmes d'applications SNA et les API
- L'organisation, les performances et l'ajustement à l'échelle globale
- Le diagnostic des incidents
- La gestion de réseau
- La sécurité du réseau

Vous pouvez commander ces publications IBM auprès de votre interlocuteur IBM local ou en appelant directement IBM au 1-800-879-2755.

Vous trouverez une liste de publications plus centrées sur CS/AIX dans la bibliographie figurant à la fin de ce manuel.

Pour plus d'informations sur d'autres publications, contactez votre interlocuteur IBM.

Informations accessibles par le réseau

Afin de favoriser l'échange d'informations, IBM parraine des forums électroniques et des services de messagerie. De plus, IBM diffuse des pages d'accueil sur Internet et propose une documentation en ligne également accessible sur CompuServe et le Web.

Support produit sur IBMLink

Le forum IBMLink est géré via des réseaux IBM. Il est conçu pour aider les utilisateurs de produits sous licence IBM à résoudre les incidents techniques et autres problèmes liés au système et au réseau. IBM répond aux questions des clients et leur permet de participer à des groupes de discussion en ligne.

Pour plus d'informations sur IBMLink, consultez le site http://www.ibmlink.ibm.com.

Informations contenues dans les pages d'accueil IBM

Sur Internet, différentes pages d'accueil IBM permettent d'accéder aux forums. Pour une aide plus détaillées, la page d'accueil principale d'IBM permet d'accéder aux centres d'information Internet. Vous pouvez accéder à cette page en tapant http://www.ibm.com.

Vous pouvez accéder aux informations sur les logiciels de gestion de réseau d'IBM, notamment CS/AIX à l'adresse http://www.ibm.com/software/network. Des informations relatives à CS/AIX sont disponibles à l'adresse http://www.ibm.com/software/network/commserver.

Pour plus de détails sur le support de CS/AIX, tapez http://www.ibm.com/software/network/commserver/support.

Informations à télécharger

Vous pouvez télécharger les documents Redbook à partir du Web en tapant http://www.redbooks.ibm.com.

Vous pouvez également accéder à d'autres informations utiles (telles que le code de programmation) via APPC Online sur le réseau CompuServe (avec `GO APPC`).

Des informations sur les logiciels IBM sont disponibles à l'adresse http://www.ibm.com/software, qui donne accès aux pages sur CS/AIX et tous les serveurs logiciels IBM.

Logiciels fournis pour une période d'essai

Dans certains pays, IBM propose une version d'essai gratuite de logiciels SNA durant 60 jours, y compris la dernière version de CS/AIX. Pour plus d'informations sur les versions d'essai, contactez votre interlocuteur IBM local ou consultez la page Web sur CS/AIX à l'adresse http://www.ibm.com/software/network/commserver/downloads.

Lectures conseillées

Pour approfondir vos connaissances sur l'architecture SNA, les manuels suivants traitent de la théorie SNA et de l'utilisation de CS/AIX dans la pratique. Ces ouvrages peuvent servir non seulement aux novices désireux de s'initier à SNA, mais aussi aux spécialistes qui souhaitent approfondir leurs connaissances sur le sujet.

- *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)

Si d'autres sujets vous intéressent, consultez la bibliographie pour obtenir d'autres références, ou contactez votre interlocuteur IBM local.

Annexe. Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM EMEA Director of Licensing
IBM Europe Middle-East Africa
Tour Descartes
La Défense 5
2, avenue Gambetta
92066 - Paris-La Défense CEDEX
France

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations
IBM Canada Ltd.
3600 Steeles Avenue East
Markham, Ontario
L3R 9Z7
Canada

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues par écrit à l'adresse suivante :

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

LE PRESENT DOCUMENT EST LIVRE «EN L'ETAT».IBM DECLINE TOUTE RESPONSABILITE, EXPLICITE OU IMPLICITE, RELATIVE AUX INFORMATIONS QUI Y SONT CONTENUES, Y COMPRIS EN CE QUI CONCERNE LES GARANTIES DE VALEUR MARCHANDE OU D'ADAPTATION A VOS BESOINS. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Il est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut modifier sans préavis les programmes et les logiciels qu'il décrit.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils

contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

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

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux termes du Contrat sur les produits et services IBM, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

LICENCE SUR LES DROITS D'AUTEUR : Le présent logiciel contient des exemples de programmes d'application en langage source destinés à illustrer les techniques de programmation sur différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits ou aux interfaces de programmation IBM. Ces exemples

de programmes n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation IBM.

Toute copie totale ou partielle de ces programmes exemples et des oeuvres qui en sont dérivées doit comprendre une notice de copyright, libellée comme suit : © (nom de votre société) (année). Des segments de code sont dérivés des Programmes exemples d'IBM Corp. © Copyright IBM Corp. 2000, 2005. All rights reserved.

Marques

Les termes qui suivent sont des marques d'International Business Machines Corporation dans certains pays :

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

Les termes qui suivent sont des marques d'autres sociétés :

Java et toutes les marques incluant Java sont des marques de Sun Microsystems, Inc. dans certains pays.

UNIX est une marque dans certains pays, dont seule la société The Open Group peut concéder la licence.

Intel est une marque de Intel Corporation.

Linux est une marque de Linus Torvalds.

RedHat et RPM sont des marques de Red Hat, Inc.

SuSE Linux est une marque de SuSE Linux AG.

UnitedLinux est une marque de UnitedLinux LLC.

Microsoft, Windows, Windows NT, Windows 2003 et le logo Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

D'autres sociétés sont propriétaires des autres marques, noms de produits ou logos qui pourraient apparaître dans ce document.

Bibliographie

Les publications IBM suivantes fournissent des informations relatives aux rubriques figurant dans cette bibliothèque. Elles sont réparties dans les catégories suivantes :

- CS/AIX, Version 6.3
- IBM Communications Server pour AIX, Version 4 Release 2
- Redbooks
- AnyNet/2 et SNA
- Multiplexeur par blocs et adaptateur PCI de canal ESCON S/390
- Système d'exploitation AIX
- Architecture unifiée de réseau (SNA)
- Configuration des systèmes hôte
- z/OS Communications Server
- Multiprotocol Transport Networking
- Transmission Control Protocol/Internet Protocol (TCP/IP)
- X.25
- Communications évoluées de programme à programme (APPC)
- Programmation
- Autres sujets relatifs aux réseaux IBM

Les manuels des bibliothèques CS/AIX font l'objet d'une brève description. Pour les autres manuels, seuls le titre, le numéro de commande et, dans certains cas, le titre abrégé utilisé dans le présent ouvrage sont indiqués.

Publications CS/AIX Version 6.3

La bibliothèque CS/AIX comprend les manuels suivants. Des versions en ligne de ces documents sont également disponibles sur le CD-ROM. Pour connaître la procédure permettant d'accéder aux fichiers électroniques du CD-ROM, voir le manuel *IBM Communications Server pour AIX - Guide d'initiation*. Pour accéder à ces manuels électroniques sur votre système, un espace disque de 9 à 15 Mo est requis (en fonction des versions de langue installées).

- *IBM Communications Server for AIX Migration Guide* (SC31-8585)

  Cet ouvrage explique la procédure de migration de Communications Server pour AIX Version 4 Release 2 ou antérieure vers CS/AIX Version 6.
- *IBM Communications Server pour AIX - Guide d'initiation* (GC11-1439)

  Ce manuel consiste dans une présentation générale de CS/AIX. Il fournit notamment des informations sur les caractéristiques de réseau prises en charge par le produit, ainsi que sur son installation, sa configuration et son utilisation.
- *IBM Communications Server for AIX Administration Guide* (SC31-8586)

  Ce manuel présente les concepts de l'architecture SNA et contient des informations sur la configuration et l'utilisation de CS/AIX.
- *IBM Communications Server for AIX Administration Command Reference* (SC31-8587)

  Ce manuel contient des informations sur SNA et sur les commandes de CS/AIX.
- *IBM Communications Server for AIX CPI-C Programmer's Guide* (SC31-8591)

Destiné aux programmeurs en langage “C” ou Java expérimentés, ce manuel est consacré à la création de programmes de transaction SNA à l’aide de l’API CPI-C de CS/AIX.

- *IBM Communications Server for AIX APPC Programmer’s Guide* (SC31-8590)

  Ce manuel est consacré à la création de programmes d’applications à l’aide des communications évoluées de programme à programme (APPC).
- *IBM Communications Server for AIX LUA Programmer’s Guide* (SC31-8592)

  Ce manuel est consacré à la création d’applications à l’aide de l’API LUA.
- *IBM Communications Server for AIX CSV Programmer’s Guide* (SC31-8593)

  Ce manuel est consacré à la création de programmes d’applications à l’aide de l’API CSV (Common Service Verbs).
- *IBM Communications Server for AIX MS Programmer’s Guide* (SC31-8594)

  Ce manuel est consacré à la création d’applications à l’aide de l’API de gestion de services (MS).
- *IBM Communications Server for AIX NOF Programmer’s Guide* (SC31-8595)

  Ce manuel est consacré à la création d’applications à l’aide de l’API NOF (Node Operator Facility).
- *IBM Communications Server for AIX Diagnostics Guide* (SC31-8588)

  Ce manuel est consacré à la résolution des incidents sur le réseau.
- *IBM Communications Server for AIX AnyNet Guide to APPC over TCP/IP* (GC31-8598)

  Ce manuel décrit l’installation, la configuration et l’utilisation de la fonction AnyNet APPC sur TCP/IP de CS/AIX.
- *IBM Communications Server for AIX AnyNet Guide to Sockets over SNA* (GC31-8597)

  Ce manuel décrit l’installation, la configuration et l’utilisation de la fonction AnyNet Sockets sur SNA de CS/AIX.
- *IBM Communications Server for AIX APPC Application Suite User’s Guide* (SC31-8596)

  Ce manuel contient des informations sur les applications APPC utilisées avec CS/AIX.
- *IBM Communications Server pour AIX - Glossaire* (GC11-2370)

  Ce manuel fournit une liste exhaustive de termes et de définitions utilisés dans la bibliothèque d’IBM Communications Server pour AIX.

Publications IBM Communications Server pour AIX Version 4 Release 2

Le manuel suivant provient d’une édition précédente de Communications Server pour AIX et ne s’applique pas à la Version 6. Ce manuel contient des informations sur les fonctions qui sont encore prises en charge mais dont il n’est pas fait mention dans la Version 6.

- *IBM Communications Server pour AIX Transaction Program Reference.* (SC31-8212)

  Ce manuel contient des informations de la Version 4 Release 2 portant sur les API de transactions. Les applications permettant d’utiliser les API Version 4 Release 2 peuvent toujours être utilisées avec la Version 6.

IBM Redbooks

Le centre international de support technique d'IBM édite des publications appelées Redbooks. Similaires à la documentation sur les produits, les Redbooks traitent des aspects théoriques et pratiques de la technologie SNA. Toutefois, ils ne contiennent pas les mêmes informations que les produits de réseau.

Les manuels suivants contiennent des informations qui peuvent être utiles pour CS/AIX :

- *IBM Communications Server pour 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)

Vous pouvez télécharger les documents Redbook à partir du Web en tapant http://www.redbooks.ibm.com.

Publications relatives au multiplexeur par blocs et à l'adaptateur PCI de canal ESCON S/390

Les manuels suivants contiennent des informations sur le multiplexeur par blocs et l'adaptateur PCI de canal ESCON S/390 :

- AIX Version 4.1 Block Multiplexer Channel Adapter: User's Guide and Service Information (SC31-8196)
- AIX Version 4.1 Enterprise Systems Connection Adapter: User's Guide and Service Information (SC31-8196)
- AIX Version 4.3 S/390 ESCON Channel PCI: User's Guide and Service Information (SC23-4232)
- IBM Communications Server for AIX Channel Connectivity User's Guide (SC31-8219)

Publications relatives à AnyNet/2 Sockets et SNA

Les manuels suivants contiennent des informations sur AnyNet/2 Sockets et SNA

- AnyNet/2 Version 2.0: Guide to Sockets over SNA (GV40-0376)
- AnyNet/2 Version 2.0: Guide to SNA over TCP/IP (GV40-0375)
- AnyNet/2: Guide to Sockets over SNA Gateway Version 1.1 (GV40-0374)
- z/OS V1R2.0 Communications Server: AnyNet Sockets over SNA (SC31-8831)
- z/OS V1R2.0 Communications Server: AnyNet SNA over TCP/IP (SC31-8832)

Publications relatives au système d'exploitation AIX

Les manuels suivants contiennent des informations sur le système d'exploitation AIX :

- *AIX Version 5.3 System Management Guide: Operating System and Devices* (SC23-4910)
- *AIX Version 5.3 System Management Concepts: Operating System and Devices* (SC23-4908)
- *AIX Version 5.3 System Management Guide: Communications and Networks* (SC23-4909)
- *AIX Version 5.3 Performance Management Guide* (SC23-4905)

- *AIX Version 5.3 Performance Tools Guide and Reference* (SC23-4906)
- *Performance Toolbox Version 2 and 3 Guide and Reference* (SC23-2625)
- *AIXlink/X.25 Version 2.1 for AIX: Guide and Reference* (SC23-2520)

Publications SNA (Systems Network Architecture)

Les manuels suivants contiennent des informations sur les réseaux 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)

Publications sur la configuration des systèmes hôte

Les manuels suivants contiennent des informations sur la configuration des systèmes hôte :

- *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)

Publications relatives à z/OS Communications Server

Les manuels suivants contiennent des informations sur z/OS Communications Server :

- *z/OS V1R7 Communications Server: SNA Network Implementation Guide* (SC31-8777-05)
- *z/OS V1R7 Communications Server: SNA Diagnostics* (Vol 1 : GC31-6850-00, Vol 2 : GC31-6851-00)
- *z/OS V1R6 Communications Server: Resource Definition Reference* (SC31-8778-04)

Publications relatives aux réseaux MPTN (transport multiprotocole)

Les manuels suivants contiennent des informations sur les réseaux MPTN (réseaux de transport multiprotocole) :

- Multiprotocol Transport Networking: Formats (GC31-7074)
- Multiprotocol Transport Networking Architecture: Technical Overview (GC31-7073)

Publications TCP/IP

Les manuels suivants contiennent des informations sur le protocole TCP/IP (Transmission Control Protocol/Internet Protocol) :

- *z/OS V1R7 Communications Server: IP Configuration Guide* (SC31-8775-07)
- *z/OS V1R7 Communications Server: IP Configuration Reference* (SC31-8776-08)
- *z/VM V5R1 TCP/IP Planning and Customization* (SC24-6125-00)

Publications X.25

Les manuels suivants contiennent des informations sur le protocole de réseau 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)

Publications APPC

Les manuels suivants contiennent des informations sur les réseaux APPC (communications évoluées de programme à programme) :

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

Publications relatives à la programmation

Les manuels suivants contiennent des informations relatives à la programmation :

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

Autres publications IBM consacrées aux réseaux

Les manuels suivants traitent d'autres sujets liés à CS/AIX :

- *SDLC Concepts* (GA27-3093-04)
- *Local Area Network Concepts and Products: LAN Architecture* (SG24-4753-00)
- *Local Area Network Concepts and Products: LAN Adapters, Hubs and ATM* (SG24-4754-00)
- *Local Area Network Concepts and Products: Routers and Gateways* (SG24-4755-00)
- *Local Area Network Concepts and Products: LAN Operating Systems and Management* (SG24-4756-00)
- *IBM Network Control Program Resource Definition Guide* (SC30-3349)

Index

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W

Commentaires

Vous pouvez nous faire part de vos appréciations et de vos critiques sur ce document en envoyant vos commentaires à IBM, selon l'une des méthodes décrites ci-dessous. Si vous souhaitez recevoir une réponse, veuillez indiquer vos nom, adresse et numéro de téléphone.

N'hésitez pas à nous signaler des erreurs ou des omissions et à nous faire part de vos remarques sur la précision, la structure de ce document, les rubriques traitées ou celles qui mériteraient d'être développées. Vos commentaires doivent toutefois porter sur les informations contenues dans le présent document et sur la manière dont elles sont organisées. Pour obtenir d'autres publications, poser des questions ou envoyer vos commentaires sur les fonctions des produits et des systèmes IBM, veuillez prendre contact avec votre partenaire commercial IBM.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Pour envoyer vos commentaires, utilisez l'un des moyens suivants :

- par télécopie au numéro suivant : 1+919-254-4028
- par courrier électronique, à l'adresse suivante :
  - comsvrcf@us.ibm.com.
- par courrier postal, à l'adresse suivante :

```
International Business Machines Corporation
Attn: z/OS Communications Server Information Development
P.O. Box 12195, 3039 Cornwallis Road
Department AKCA, Building 501
Research Triangle Park, North Carolina 27709-2195
```

Veuillez mentionner les informations suivantes dans votre message :

- le titre et le numéro de référence du présent document
- le numéro de la page ou la rubrique à laquelle votre commentaire fait référence.

Numéro de programme : 5765-E51

GC11-1439-02