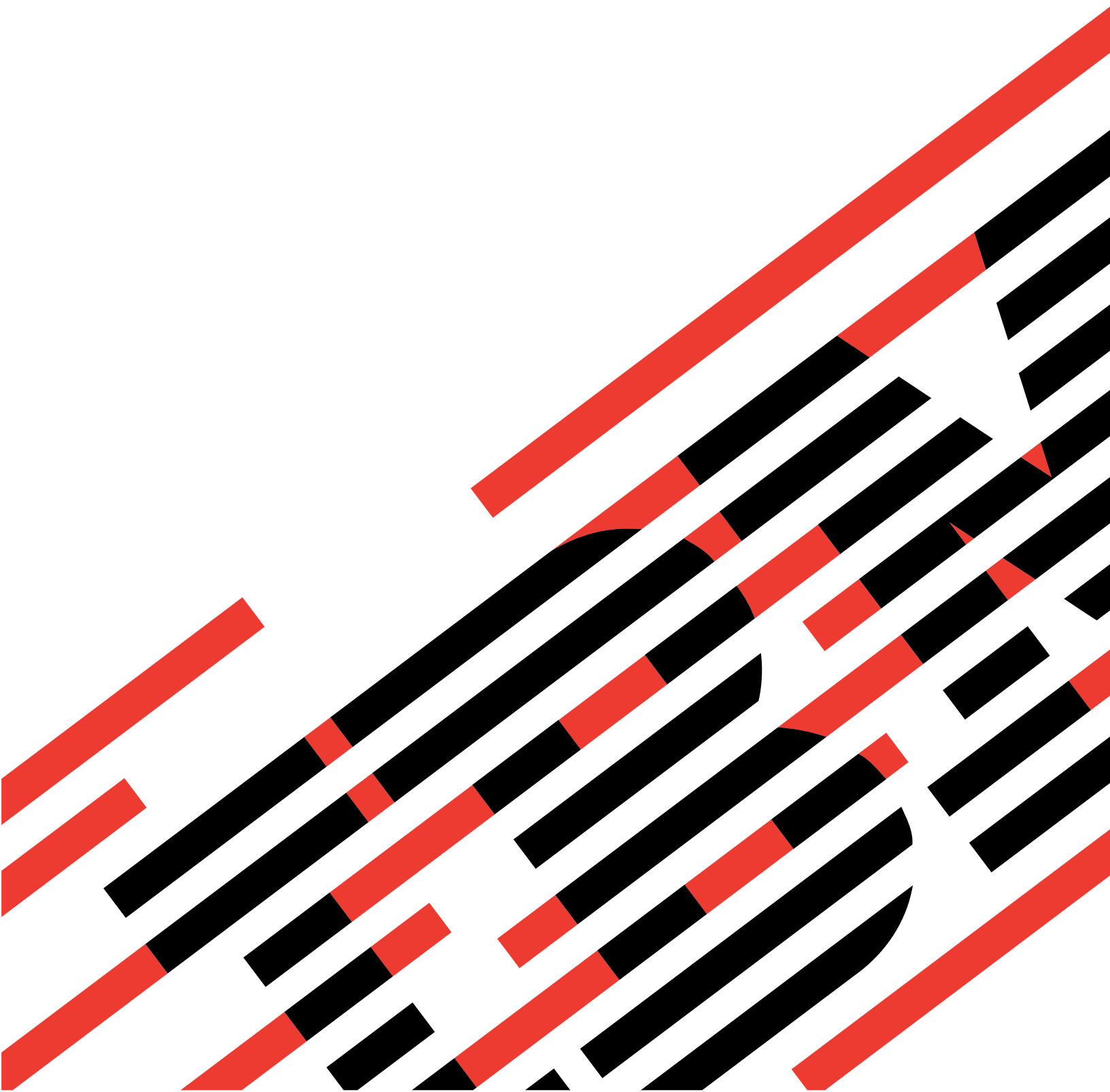




IBM Systems - iSeries
Connexion universelle

Version 5.4





IBM Systems - iSeries
Connexion universelle

Version 5.4

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 73.

Troisième édition - février 2006

Réf. US : RZAT-J000-02

LE PRESENT DOCUMENT EST LIVRE "EN L'ETAT". IBM DECLINE TOUTE RESPONSABILITE, EXPRESSE OU IMPLICITE, RELATIVE AUX INFORMATIONS QUI Y SONT CONTENUES, Y COMPRIS EN CE QUI CONCERNE LES GARANTIES DE QUALITE 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.

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*

© Copyright IBM France 2005. Tous droits réservés.

© **Copyright International Business Machines Corporation 2004, 2006. All rights reserved.**

Table des matières

Avis aux lecteurs canadiens v

Connexion universelle 1

Impression de la rubrique	2
Concepts liés à la connexion universelle	2
Proxys d'application	3
Pare-feu de filtrage des paquets IP	3
Protocole SSL/TLS	5
Conversion d'adresses réseau (NAT)	5
SOCKS	6
Réseau privé virtuel (VPN)	7
Planification de la connexion universelle	7
Scénarios : Connexion universelle	8
Scénario : Configuration d'une connexion commutée point à point via AGNS	9
Scénario : Configuration d'une connexion commutée point à point pour un serveur fournissant une connectivité à d'autres systèmes via AGNS	15
Scénario : Configuration d'une connexion commutée point à point distante	23
Scénario : Configuration d'une connexion directe à Internet	29
Scénario : Configuration d'une connexion directe à Internet à partir d'un serveur qui fournit la connectivité pour d'autres systèmes ou partitions.	34

Scénario : Configuration d'une connexion PPP via un fournisseur d'accès Internet	40
Scénario : Configuration d'une connexion commutée point à point à partir d'un serveur fournissant une connectivité à d'autres systèmes via un fournisseur d'accès Internet	46
Scénario : Configuration d'une connexion multiple entre noeuds via un serveur distant	53
Configuration de la connexion universelle	58
Configuration d'une connexion commutée via AGNS	59
Configuration d'une connexion commutée point à point éloignée	61
Configuration d'une connexion directe à Internet	62
Configuration d'une connexion PPP via un fournisseur d'accès Internet	64
Configuration d'une connexion multiple entre noeuds	66
Procédures supplémentaires de configuration de la connexion universelle	67
Identification et résolution des incidents liés à l'assistant de connexion universelle	70

Annexe. Remarques 73

Marques	75
Dispositions	75

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
 (Post)		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.

Connexion universelle

| La connexion universelle vous permet de contrôler le mode de connexion de votre entreprise aux
| Téléservices IBM. Une fois que la connexion est établie, vous pouvez accéder à une grande variété
| d'options d'assistance client au fur et à mesure de vos besoins. Ce logiciel est basé sur l'utilisation du
| protocole TCP/IP (Transmission Control Protocol/Internet Protocol) et vous le configurez via un assistant
| ou une interface de commande qui vous permet de choisir le mode de connexion à IBM. Les options
| disponibles sont les suivantes :

- | • Connexion commutée directe via AT&T Global Network Services
- | • Connexion via un fournisseur d'accès Internet
- | • Connexion directe à Internet par le réseau local
- | • Connexion commutée distante via AT&T Global Network Services
- | • Connexion multiple entre noeuds via un réseau privé virtuel (VPN) distant
- | • Connexion proxy HTTP ou de maintenance et de support

Ces diverses options vous permettent de choisir la solution la mieux adaptée à votre entreprise, tout en bénéficiant d'une connexion sécurisée. Pour la plupart des utilisateurs, l'option de connexion universelle est la méthode la plus rapide et la plus pratique pour accéder aux Téléservices.

| L'assistant de connexion universelle vous guide tout au long des étapes de configuration de la connexion.
| IBM utilise cette configuration lorsque vous autorisez les applications suivantes à fournir la prise en
| charge, la maintenance et la documentation système :

- | • Téléservices
- | • Electronic Service Agent
- | • Mise à jour de l'Information Center

Remarque : Vous pouvez également configurer ces profils au moyen des commandes CL, dont les commandes GO SERVICE et CRTSRVCFG. Pour plus d'informations, voir Control language (CL).

Concepts liés à la connexion universelle

Découvrez les technologies de pare-feu et les protocoles utilisés par la connexion universelle.

Planification de la connexion universelle

La première étape permettant de configurer avec succès une connexion universelle aux services IBM est de s'assurer d'avoir sélectionné une méthode de connexion à IBM à partir du serveur et de remplir toutes les conditions préalables requises.

Scénarios : Connexion universelle

Pour vous familiariser avec l'utilisation de l'assistant de connexion universelle et avec les étapes de création d'une connexion universelle, consultez les scénarios suivants.

Configuration de la connexion universelle

Après avoir planifié la connexion universelle et consulté les scénarios, vous pouvez commencer la configuration. Cette section explique de façon générale comment utiliser l'assistant de connexion universelle et présente les autres tâches connexes que vous devrez effectuer lors de la création d'une connexion universelle vers les services IBM.

Identification et résolution des incidents liés à l'assistant de connexion universelle

Consultez cette section en cas d'incidents liés à l'utilisation de l'assistant de connexion universelle.

Impression de la rubrique

Pour afficher ou télécharger la version PDF de cette rubrique, sélectionnez Connexion universelle (environ 967 Ko).

Enregistrement de fichiers PDF

Pour sauvegarder un PDF sur votre poste de travail, le visualiser ou l'imprimer, procédez comme suit :

1. Cliquez avec le bouton droit de la souris sur le PDF dans votre navigateur. (Cliquez avec le bouton droit de la souris sur le lien ci-dessus.)
2. Cliquez sur **Enregistrer la cible sous...** si vous utilisez Internet Explorer. Cliquez sur **Enregistrer le lien sous...** si vous utilisez Netscape Communicator.
3. Naviguez jusqu'au répertoire où vous souhaitez sauvegarder le PDF.
4. Cliquez sur **Enregistrer**.

Téléchargement d'Adobe Acrobat Reader

Vous devez utiliser Adobe Acrobat Reader pour afficher ou imprimer ces fichiers PDF. Vous pouvez en télécharger une copie depuis le site Web d'Adobe (www.adobe.com/products/acrobat/readstep.html)



Concepts liés à la connexion universelle

Les concepts ci-après vous permettent de vous familiariser avec les détails techniques et de configuration impliqués par chaque connexion disponible avec la connexion universelle. Les informations présentées se concentrent sur les relations existant entre la technologie et l'établissement d'une connexion universelle. Chaque concept fait référence à des informations complémentaires au sujet de la rubrique.

Technologies de protection des données

Avant de commencer la création d'une configuration, vous devez comprendre comment la sécurité du réseau influence la configuration d'une connexion universelle.

Proxys d'application

Si la méthode utilisée pour accéder à Internet est une application proxy, certaines applications de connexion universelle pourront utiliser le proxy. Cependant, vous devez vous assurer que vous avez sélectionné une méthode de configuration qui permet la connexion de vos données de services restantes à partir de votre serveur IBM via la connexion universelle sans passer par une application proxy.

Pare-feu de filtrage des paquets IP

Il se peut que vous deviez modifier les règles de filtrage des paquets afin de permettre au trafic passant par la connexion universelle de circuler via votre pare-feu vers IBM.

Protocole SSL/TLS

Le protocole SSL/TLS permet d'assurer la confidentialité des données dans un réseau. La connexion universelle crée un espace de stockage de certificats contenant des certificats d'autorité d'accréditation sécurisés utilisés par le protocole SSL/TLS. Il n'est pas nécessaire de modifier cela. Certaines applications de service utilisent le protocole SSL/TLS pour protéger les flots de données vers IBM.

Conversion d'adresses réseau (NAT)

La fonction de conversion d'adresses réseau (NAT) transforme les adresses IP internes ou privées en

adresses IP publiques ou à réacheminement global. Le trafic circulant via la connexion universelle peut être acheminé vers IBM en passant par une fonction de conversion NAT. Ce système de transfert est activé automatiquement.

SOCKS

Un serveur ou un client SOCKS est une application proxy TCP/IP qui permet d'envoyer des informations via une grande variété de protocoles sans fournir les informations de réseau interne. Si le réseau inclut un serveur SOCKS, vous devez vous assurer que vous n'acheminez pas le trafic de la connexion universelle via ce serveur.

Réseau privé virtuel (VPN)

Découvrez comment le réseau privé virtuel (VPN) influence la protection des données lors de la configuration d'une connexion universelle entre votre serveur et les services d'assistance IBM. Certaines applications de service utilisent un réseau virtuel privé (VPN) pour protéger les flots de données vers IBM.

Proxys d'application

Un proxy d'application ou un serveur proxy d'application reçoit les demandes prévues pour un autre serveur et agit pour le compte du client (en tant que proxy du client) pour obtenir le service demandé. Un serveur proxy d'application est souvent utilisé lorsque le client et le serveur sont incompatibles pour une connexion directe. Par exemple, le client n'est pas en mesure de satisfaire les exigences d'authentification de sécurité du serveur mais doit néanmoins accéder à certains services. Les caractéristiques d'un proxy d'application sont notamment les suivantes :

- Il interrompt la connexion TCP/IP entre un client et le serveur ; le réacheminement IP n'est pas requis.
- Il masque les adresses IP internes client ; seule l'adresse IP publique du serveur proxy est visible depuis le réseau externe.
- Il fournit des historiques des accès détaillés.
- Il authentifie les utilisations.
- Il place les informations en mémoire cache.

Le type de proxy le plus courant est le proxy HTTP. La plupart des serveurs proxy traitent également les protocoles HTTPS (protocole de transport hypertexte sécurisé) et FTP (protocole de transfert de fichier). Le protocole SMTP (protocole de transfert de courrier simple) est un exemple de proxy d'application.

Le principal inconvénient des proxys d'application réside dans le fait que ceux-ci doivent prendre en charge l'application pour laquelle ils exécutent la fonction de proxy. Or, de nombreuses applications TCP/IP ne sont pas prises en charge par les serveurs proxy. En outre, les proxys d'application ne chiffrent normalement pas les données.

Certaines applications de connexion universelle peuvent circuler via un serveur proxy HTTP standard. Le serveur HTTP proxy doit prendre en charge l'établissement de tunnels SSL et peut éventuellement requérir une authentification standard HTTP.

La version 5.4 d'i5/OS englobe un proxy HTTP de maintenance et de support pouvant être utilisé pour les applications de connexion universelle si vous souhaitez qu'une partition ou un système fournisse une connexion aux autres systèmes ou partitions.

Pare-feu de filtrage des paquets IP

Un pare-feu de filtrage des paquets IP permet de créer un ensemble de règles qui rejettent ou acceptent un flux de données dans une connexion réseau. Le pare-feu lui-même n'affecte en aucune manière ce flux de données. Etant donné qu'un filtre de paquets ne peut rejeter que les flux de données qui lui sont envoyés, l'unité équipée du filtre de paquets doit soit effectuer le routage IP, soit constituer la cible du flux de données.

Un filtre de paquets dispose d'un ensemble de règles qui acceptent ou rejettent des actions. Lorsque ce filtre reçoit un paquet d'informations, il les compare à l'ensemble de règles préconfigurées. A la première mise en correspondance, le filtre de paquets accepte ou rejette le paquet d'informations. La plupart des filtres de paquets disposent d'une règle de rejet total implicite à la fin du fichier de règles.

Généralement, les filtres de paquets autorisent ou refusent les flux de données réseau en fonction des critères suivants :

- Adresses IP source et cible
- Protocole, tel que TCP, UDP ou ICMP
- Ports source et cible, ainsi que types et codes ICMP
- Balises situées dans l'en-tête TCP (par exemple, balise indiquant si le paquet est une demande de connexion)
- Direction (entrante ou sortante)
- Type d'interface physique traversée par le paquet

Tous les filtres de paquets possèdent une caractéristique commune qui peut engendrer des incidents : La sécurité est basée sur les adresses IP. Bien que ce type de sécurité ne soit pas suffisant pour la totalité d'un réseau, il est acceptable au niveau des composants.

La plupart des filtres de paquets IP ne possèdent pas d'état, ce qui signifie qu'ils ne mémorisent aucune information concernant les paquets qu'ils ont précédemment traités. Un filtre de paquets doté d'un état pourrait mémoriser certaines informations sur les flux précédents, ce qui vous donnerait la possibilité de configurer le système afin que seules les réponses aux demandes provenant du réseau interne soient autorisées à partir d'Internet. Les filtres de paquets ne disposant pas d'un état sont vulnérables et peuvent faire l'objet d'une interception d'informations car l'adresse IP source et le bit d'accusé de réception figurant dans l'en-tête du paquet peuvent facilement être contrefaits par des utilisateurs mal intentionnés.

i5/OS vous permet de spécifier des règles de filtrage de paquets sur des interfaces et des profils de services d'accès distant. Pour plus d'informations, consultez les sections suivantes : Create IP filter rules et Services d'accès distant : connexions PPP. Si vous utilisez un pare-feu de filtrage de paquets externe ou des règles de filtrage de paquets sur l'i5/OS et que les données de la connexion universelle passent à travers ces filtres, vous devez modifier ces règles de filtrage pour permettre la connexion à la passerelle VPN IBM :

Règles de filtrage IP	Valeurs de filtrage IP
Règle de filtrage du trafic entrant UDP	Autorise l'utilisation du port 4500 pour les adresses de passerelle VPN
Règle de filtrage du trafic entrant UDP	Autorise l'utilisation du port 500 pour les adresses de passerelle VPN
Règle de filtrage du trafic sortant UDP	Autorise l'utilisation du port 4500 pour les adresses IP de passerelle VPN
Règle de filtrage du trafic sortant UDP	Autorise l'utilisation du port 500 pour les adresses IP de passerelle VPN
Règle de filtrage du trafic entrant ESP	Autorise l'utilisation du protocole ESP (X'32') pour les adresses IP de passerelle VPN
Règle de filtrage du trafic sortant ESP	Autorise l'utilisation du protocole ESP (X'32') pour les adresses IP de passerelle VPN

Pour les applications de connexion universelle utilisant le protocole HTTP et HTTPS pour un transport, vous devez modifier les règles de filtrage pour autoriser les connexions aux destinations de service IBM en procédant comme suit :

Règles de filtrage IP	Valeurs de filtrage IP
Règle de filtrage du trafic entrant TCP	Autorise l'utilisation du port 80 pour les adresses de destination de service
Règle de filtrage du trafic entrant TCP	Autorise l'utilisation du port 443 pour les adresses de destination de service
Règle de filtrage du trafic sortant TCP	Autorise l'utilisation du port 80 pour les adresses de destination de service
Règle de filtrage du trafic sortant TCP	Autorise l'utilisation du port 443 pour les adresses de destination de service

Pour modifier les règles de filtrage, vous devez spécifier l'adresse réelle de la passerelle VPN IBM. Vous pouvez déterminer ces adresses (voir «Détermination des adresses de passerelle VPN IBM», à la page 69).

En outre, pour le trafic HTTP et HTTPS, certaines modifications des règles de filtrage peuvent entraîner la spécification des adresses de destination de service actuelles. Vous pouvez déterminer ces adresses (voir «Détermination des adresses de destination de services IBM», à la page 69).

Pour plus d'informations, voir Règles liées aux paquets - Concepts.

Protocole SSL/TLS

L'objectif du protocole TLS et de son prédécesseur le protocole SSL est d'assurer la confidentialité des données sur Internet. Les applications serveur et client TCP/IP qui sont compatibles avec SSL ont un mode de communication qui permet d'empêcher l'écoute clandestine, la contrefaçon des données ou la falsification des messages. Ces protocoles fournissent des fonctions de chiffrement, d'intégrité des données et d'authentification.

Le protocole TLS est une mise à jour du protocole SSL version 3.0. TLS fournit les mêmes fonctions que SSL, mais comporte quelques fonctions supplémentaires et une clarification des flux protocolaires pour les zones mal définies dans le protocole SSL. Le principal but du protocole TLS est de normaliser la définition et les mises en oeuvre du protocole SSL, de sécuriser le protocole SSL et de rendre la spécification de ce protocole plus concise et plus complète.

Le protocole SSL/TSL se compose de deux protocoles distincts : le protocole d'enregistrement et le protocole d'établissement de liaison. Le protocole d'établissement de liaison est encapsulé dans le protocole d'enregistrement. Le protocole d'établissement de liaison SSL établit une connexion sécurisée entre le client et le serveur.

La connexion universelle crée un espace de stockage utilisé par le protocole SSL. Il n'est pas nécessaire de modifier cela. En outre, certaines applications et certains flux de données de la connexion universelle sont protégés par l'utilisation de SSL ou de TLS.

Conversion d'adresses réseau (NAT)

La fonction de conversion d'adresses réseau (NAT) transforme les adresses IP internes ou privées en adresses IP publiques ou à réacheminement global et transforme également les ports. Pour que la connexion universelle avec IBM puisse être établie via une conversion NAT, vous devez activer le balayage NAT (voir NAT compatible IPSec) afin que la conversion de l'adresse ne brise pas le flux de données chiffrées. L'assistant de connexion universelle active automatiquement cette conversion.

La fonction de conversion NAT offre les avantages suivants :

- Elle permet de sauvegarder les adresses IP publiques. Etant donné qu'un client a uniquement besoin d'une adresse IP publique lorsqu'il communique avec Internet, le pool d'adresses IP à acheminement global peut être partagé avec d'autres clients. Vous avez donc besoin de moins d'adresses IP publiques que le nombre réel de clients internes devant accéder au réseau public si vous utilisez la fonction de conversion NAT. Lorsque votre adresse IP privée envoie des données via la fonction de conversion NAT, ce logiciel convertit l'adresse privée en adresse publique. Grâce à ce logiciel et à la possibilité qu'il offre de convertir l'adresse et le port IP (mappage de port via NAT), il est possible, dans de nombreuses applications de la fonction de conversion NAT, de n'utiliser qu'une adresse IP publique.
- La fonction de conversion NAT masque les adresses IP de réseau interne.
- Elle simplifie l'acheminement. Etant donné que le réseau interne affecte des adresses IP aux hôtes internes, les autres systèmes internes peuvent y accéder sans utiliser de routes ou de routeurs spécifiques. Il est possible d'accéder à ces mêmes hôtes à partir du réseau public via des adresses IP à acheminement global converties par la fonction NAT.
- La fonction de conversion NAT est transparente pour le client et vous permet donc de prendre en charge une plus grande gamme de clients.
- Elle prend en charge une vaste gamme de services avec cependant quelques exceptions. Toute application qui achemine et utilise l'adresse IP au sein de l'application ne peut fonctionner avec la fonction de conversion NAT.
- La fonction de conversion NAT consomme moins de ressources système et est plus efficace que les serveurs SOCKS et les serveurs proxy.
- La connexion universelle peut passer par la fonction de conversion NAT.

La fonction de conversion NAT présente cependant quelques inconvénients :

- Elle ne fournit qu'un niveau minimum de services d'ouverture de session.
- Vous devez activer la retransmission IP pour pouvoir utiliser la fonction de conversion NAT pour établir une connexion à Internet.
- Elle n'est pas aussi efficace que les serveurs SOCKS ou proxy pour la détection des attaques.
- Elle peut briser certaines applications ou rendre plus difficile leur exécution.

SOCKS

Un serveur SOCKS est une application de serveur proxy TCP/IP qui permet d'envoyer des informations via une grande variété de protocoles sans fournir les informations de réseau TCP/IP interne. Pour pouvoir utiliser un serveur SOCKS, le client doit prendre en charge le protocole SOCKS.

Certains systèmes (comme les systèmes i5/OS) prennent en charge un client SOCKS dans sa pile TCP/IP (clients polyvalents) afin que toutes les applications client puissent utiliser un serveur SOCKS. C'est la configuration du client qui indique le nom du serveur SOCKS à utiliser et les règles définissant quand le serveur doit être utilisé.

Les serveurs SOCKS n'ont pas connaissance du protocole d'application qu'ils utilisent. Ces serveurs, par exemple, ne connaissent pas le protocole Telnet HTTP. Par conséquent, il est possible d'écrire de façon beaucoup plus efficace sur les serveurs SOCKS que sur les autres serveurs proxy. L'inconvénient est que les serveurs SOCKS ne peuvent effectuer des opérations telles que la mise en mémoire cache ou la consignation dans le journal des adresses URL accessibles via le serveur.

| La connexion universelle ne prend pas en charge le flux de données circulant via un serveur SOCKS. Par
| conséquent, si votre client i5/OS accède au réseau via un serveur SOCKS, vous devez faire en sorte
| qu'aucune des informations circulant via la connexion universelle ne soit routée vers le serveur SOCKS
| en indiquant dans la configuration SOCKS que toutes les destinations sont de type DIRECT.

| Pour plus d'informations sur les serveurs SOCKS, voir Prise en charge du client SOCKS et «Vérification
| de la compatibilité avec SOCKS», à la page 68.

Réseau privé virtuel (VPN)

Un réseau privé virtuel (VPN) permet d'étendre le réseau intranet privé de votre entreprise à l'architecture d'un réseau public. Le VPN est basé sur la création de tunnels sécurisés virtuels entre les hôtes ou les passerelles connectés au réseau public. Pour participer à un tunnel sécurisé ou à une connexion VPN, l'extrémité du tunnel de type VPN doit mettre en oeuvre une suite compatible de protocoles VPN. VPN fournit les fonctions de sécurité suivantes :

- Authentification de l'origine des données afin de vérifier que chaque datagramme a été créé par l'émetteur indiqué.
- Intégrité des données afin de vérifier que le contenu d'un datagramme n'a pas été modifié délibérément ou en raison d'erreurs aléatoires.
- Chiffrement des données afin d'assurer la confidentialité des textes de messages.
- Protection contre la réexécution afin de s'assurer qu'aucun pirate ne peut intercepter les données et les lire de nouveau ultérieurement.
- Gestion des clés afin de s'assurer que la règle VPN que vous utilisez peut être mise en oeuvre dans tout le réseau étendu avec peu ou pas de configuration manuelle.

Dans certains scénarios, la connexion universelle crée une connexion VPN à IBM afin d'assurer la sécurisation des informations envoyées et reçues entre votre serveur iSeries et IBM (par exemple, VPN chiffre et authentifie les données). Les technologies VPN utilisées par la connexion universelle incluent L2TP, IKE et IPSec. Pour plus d'informations, voir Layer 2 Tunnel Protocol (L2TP), Implicit IKE et IP Security (IPSec) protocols. Pour certaines options de connectivité, la connexion universelle utilise uniquement L2TP pour les portions de la connexion qui ne nécessitent pas de chiffrement. Par exemple, si vous vous connectez à une partition à partir d'une autre partition puis que vous vous connectez à IBM via Internet, la connexion universelle utilise uniquement L2TP entre ces deux partitions, puis utilise L2TP protégé par IPSec pour la seconde portion de la connexion (portion nécessitant un chiffrement.)

Pour plus d'informations, voir Virtual private networking.

Planification de la connexion universelle

Avant de lancer l'assistant de connexion universelle, vous devez prendre certaines décisions. Durant la procédure de configuration, le système vous demande de choisir le type de connexion à utiliser pour la prise en charge des Téléservices IBM. Votre choix dépendra du réseau que vous utilisez et de l'accessibilité à Internet à partir de votre serveur iSeries. Lorsqu'ils utilisent le protocole IPSec compatible avec la fonction de conversion NAT, les serveurs iSeries prennent en charge une connexion même en présence d'un pare-feu NAT intermédiaire. La prise en charge des protocoles HTTP et HTTPS permet d'établir des connexions au travers de la plupart des pare-feux ou proxys fournis par le client ou IBM.

Avant de sélectionner le scénario de configuration de connexion universelle, prenez en considération les points suivants :

- Le matériel, les logiciels et la configuration du réseau :
 - Si votre serveur n'est pas en réseau ou est simplement en réseau privé et dispose d'un modem, vous pouvez sélectionner l'option **Connexion commutée via AT&T Global Network Services**. Cette option vous permet de disposer d'une connexion commutée sécurisée aux services de maintenance et support IBM et toutes les données sont protégées via un réseau privé virtuel (VPN) ou une fonction SSL.
 - Si votre système ou votre partition a accès à un système, à une partition ou à une console HMC doté(e) d'un modem, vous pouvez configurer ce système à l'aide de l'option **Connexion via un autre système ou une autre partition** en utilisant une connexion AT&T distante.
 - Si votre serveur dispose d'un accès direct (connexion à large bande avec une adresse IP fixe ou réseau local avec une adresse IP à acheminement global) à Internet (sans pare-feu intermédiaire) ou si votre serveur possède une adresse IP privée mais peut accéder à Internet via un pare-feu en utilisant la fonction de conversion NAT, vous pouvez sélectionner l'option **Connexion directe à**

Internet. Il s'agit de l'option recommandée qui permet d'obtenir l'accès le plus rapide et le plus sécurisé aux services de maintenance et support IBM.

- Si vous utilisez un fournisseur d'accès Internet auquel le serveur se connecte et qui tient lieu de point de connexion pour les autres serveurs ou les autres partitions, vous pouvez sélectionner l'option **Connexion via un fournisseur d'accès Internet**. Cette option prend en charge une connexion sécurisée aux services de maintenance et support IBM simultanément et via la même connexion commutée que celle utilisée par votre serveur iSeries pour accéder à Internet.
- Si votre serveur se trouve dans un réseau privé, ne possède pas d'adresse IP globale et a accès à un routeur ou à un serveur permettant au serveur iSeries d'établir une connexion à Internet via un fournisseur d'accès Internet, sélectionnez l'option **Connexion multiple entre noeuds à Internet**.
- Outre les configurations susmentionnées, si votre entreprise possède un proxy HTTP ou que vous configurez un proxy de maintenance et de support sur une ou plusieurs de vos partitions logiques, vous pouvez le configurer de sorte que les applications de service prenant en charge les proxys HTTP et/ou HTTPS puissent utiliser ces proxys.

Remarque : Vous pouvez configurer une configuration principale et de secours et un proxy principal et secondaire.

- La stratégie de sécurité réseau de votre entreprise
- Configuration des règles de sécurité des paquets : Vous devez vous assurer que le trafic inhérent à la connexion universelle est autorisé via le pare-feu. Pour plus d'informations, voir «Pare-feu de filtrage des paquets IP», à la page 3.
- Sécurité SOCKS : Vous devez vous assurer qu'aucune des données transmises par le biais de la connexion universelle n'est dirigée via un serveur SOCKS. Pour plus d'informations, voir Prise en charge du client SOCKS.
- Serveur de noms de domaine (DNS) : Les applications de service utiliseront un système de nom de domaine pour la vérification des adresses de service cible. Ce système offre une tolérance aux pannes supplémentaire. Aussi, nous vous recommandons de rendre votre système de nom de domaine disponible pour les serveurs iSeries appropriés à l'aide de la commande CL CHGTCPDMN.

Remarque : Vous devez effectuer certaines tâches de configuration lorsque vous utilisez un modem HMC pour vous connecter à IBM via une partition i5/OS ou lorsque vous disposez d'une console HMC se connectant à IBM via la connexion VPN ou modem d'une partition i5/OS. Pour des informations supplémentaires, consultez la rubrique Configuration de votre environnement de maintenance de l'IBM Systems Hardware Information Center.

Scénarios : Connexion universelle

Les scénarios ci-après vous permettent de vous familiariser avec les détails techniques et de configuration impliqués par chaque connexion disponible avec la connexion universelle. Ces scénarios illustrent la connexion aux Téléservices IBM mais vous pouvez tout aussi bien utiliser l'assistant de connexion universelle pour mettre à jour l'Information Center.

Remarques :

1. Avant de passer en revue ces scénarios, lisez «Planification de la connexion universelle», à la page 7 pour sélectionner une méthode de connexion qui répond aux besoins de votre entreprise. Vous pouvez ensuite sélectionner un scénario adapté à votre configuration.
2. Vous pouvez également configurer ces profils au moyen des commandes CL, dont les commandes GO SERVICE et CRTSRVCFG. Pour plus d'informations, voir Control language (CL).

Connexion commutée point à point vers AT&T Global Network Services via un serveur local
Dans ce scénario, MaSociété souhaite établir une connexion universelle entre votre serveur et les Téléservices IBM via une connexion point à point vers AT&T Global Network Service (AGNS).

Configuration d'une connexion commutée point à point via AGNS vers un serveur fournissant une connectivité à d'autres systèmes

Ce scénario permet à MaSociété de créer une connexion universelle pour un serveur qui tient lieu de point de connexion pour d'autres systèmes par le biais d'une connexion point à point via AGNS vers les Téléservices.

Connexion commutée point à point vers AGNS à partir d'un serveur éloigné ou d'une console HMC

Ce scénario explique comment MaSociété crée une connexion universelle via un serveur éloigné qui tient lieu de point de connexion via AGNS vers les Téléservices.

Connexion Internet directe via un serveur local

Ce scénario explique comment MaSociété utilise l'assistant de connexion universelle pour établir une connexion entre son serveur et les Téléservices via une connexion Internet directe.

Connexion Internet directe via un serveur local qui fournit la connectivité pour d'autres systèmes

Dans ce scénario, MaSociété souhaite configurer un serveur local qui tienne lieu de point de connexion vers des services électroniques via une connexion directe à Internet.

Connexion point à point à l'aide d'un serveur local via un fournisseur d'accès Internet

Ce scénario explique comment MaSociété utilise l'assistant de connexion universelle pour établir une connexion entre son serveur et les Téléservices via une connexion locale de fournisseur d'accès Internet.

Connexion point à point à l'aide d'un serveur local qui fournit la connectivité pour d'autres systèmes via un fournisseur d'accès Internet

Dans ce scénario, MaSociété crée une connexion point à point à l'aide d'un serveur local qui tient lieu de point de connexion pour d'autres systèmes via un fournisseur d'accès Internet.

Connexion multiple entre noeuds via un serveur distant

Ce scénario montre comment MaSociété peut configurer une connexion universelle multiple entre noeuds vers les Téléservices à l'aide d'un serveur distant via un fournisseur d'accès Internet.

Scénario : Configuration d'une connexion commutée point à point via AGNS

Situation

Supposons que vous êtes responsable de la gestion d'un serveur iSeries pour MaSociété, une petite entreprise de fabrication située à Boone, dans l'Iowa. Pour fournir cette prise en charge, vous devez établir une connexion entre les Téléservices d'IBM et le serveur iSeries de MaSociété. Comme MaSociété ne dispose pas d'une connexion de réseau Internet, vous pouvez créer une connexion à partir de votre serveur iSeries par le biais d'une liaison commutée point à point (PPP) en utilisant votre modem interne. Comme vous n'avez pas besoin de fournir des connexions pour d'autres systèmes, vous n'avez pas besoin non plus de fournir des connexions pour d'autres serveurs ou partitions.

Solution

Créez une connexion universelle vers IBM via AT&T Global Network Services (AGNS). Dans ce cas, vous devez établir une connexion via le gestionnaire de connexions sur votre serveur iSeries local par le biais d'une connexion point à point AGNS vers les Téléservices.

Avantages

Ce scénario offre les avantages suivants :

- MaSociété n'a pas besoin d'investir dans du matériel ou du logiciel supplémentaire pour bénéficier des Téléservices. Vous pouvez configurer cette connexion en utilisant le modem interne dont vous disposez déjà, à l'aide de l'assistant de connexion universelle ou des commandes **CL GO SERVICE** ou **CRTSRVCFG**.
- La connexion AGNS fournit à MaSociété une méthode simple pour accéder aux Téléservices qui permettent de faciliter la résolution des incidents liés au serveur, le suivi du matériel et du logiciel système en cours ou la réception de mises à jour et de correctifs de logiciel.
- L'AGNS offre une connexion sécurisée entre MaSociété et IBM en mettant en oeuvre sa propre sécurité pour établir cette connexion. Vous n'avez pas besoin de fournir une sécurité supplémentaire.

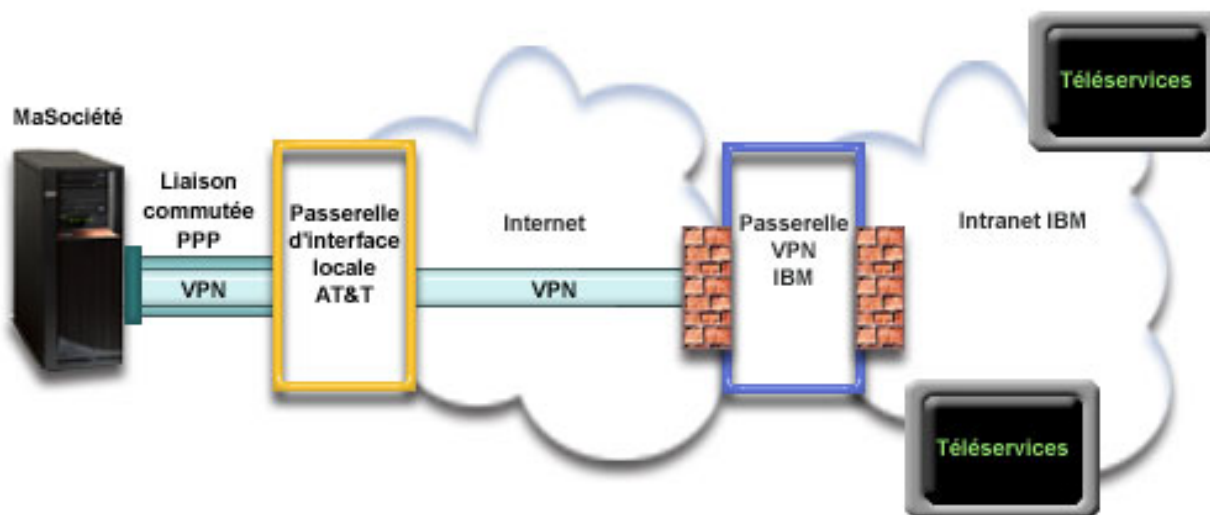
Objectifs

Dans ce scénario, MaSociété souhaite s'assurer qu'IBM peut prendre en charge son système informatique à la demande de l'administrateur réseau de la société. Les objectifs de ce scénario sont les suivants :

- Pour créer une connexion commutée point à point sécurisée entre MaSociété et les Téléservices via AT&T Global Network Services
- Automatiser le service d'assistance à la clientèle via les Téléservices et différents services
- Permettre aux Téléservices de créer un inventaire matériel et logiciel du système iSeries de MaSociété.
- Demander que les Téléservices envoient des correctifs et des mises à jour de logiciel à MaSociété via le réseau.

Détails

Le schéma suivant illustre la connexion du serveur iSeries de MaSociété aux Téléservices via une connexion AT&T Global Network Services.



Configuration de la connexion universelle

- iSeries Navigator lance l'assistant de connexion universelle pour configurer la connexion. Cette opération n'a besoin d'être exécutée qu'une seule fois sauf si des numéros de téléphone AT&T ou d'autres informations doivent être mis à jour.

Utilisation de la connexion universelle

Lorsqu'une application de service souhaite utiliser la connexion universelle pour communiquer avec IBM, les événements suivants ont lieu :

- Une connexion point à point est établie via une interface de passerelle locale (LIG) AT&T.
- Un réseau virtuel privé (VPN) est établi, si l'application de service ne fournit pas ses propres communications cryptées, via la LIG AT&T LIG et Internet vers une passerelle de réseau privé virtuel chez IBM.
- L'application de service communique avec les serveurs IBM appropriés pour exécuter le service demandé.

Conditions requises et préalables

Les conditions requises pour pouvoir activer les Téléservices via une connexion AGNS sont les suivantes :

- Vérifiez qu'iSeries Access for Windows et iSeries Navigator sont installés sur votre ordinateur personnel (voir iSeries Access for Windows - Installation et configuration).
- Assurez-vous d'avoir installé tous les Service Packs les plus récents pour iSeries Navigator. Les scénarios présentés utilisent la version 5.4 du logiciel.
- Vérifiez que TCP/IP est actif. Vous pouvez démarrer TCP/IP via la commande STRTCP (Démarrer TCP/IP).
- Pour pouvoir configurer la connexion à partir de l'assistant de connexion universelle, vous devez disposer du droit de responsable de la sécurité (*SECOFR) associé aux droits spéciaux *ALLOBJ, *IOSYSCFG et *SECADM dans votre profil utilisateur i5/OS et du droit *USE sur WRKCNTINF.
- Vous devez installer les utilitaires de connectivité TCP/IP (5722-TC1).
- Pour que le réseau privé virtuel (VPN) et la couche SSL fonctionnent, vous devez installer Digital Certificate Manager (DCM) (5722-SS1 option 34).
- Assurez-vous que la valeur système QRETSVRSEC a pour valeur 1. Pour cela, utilisez la commande DSPSYSVAL (Afficher une valeur système). Si cette valeur n'est pas fixée à 1, entrez la commande CHGSYSVAL (Modifier une valeur système). L'ID utilisateur et le mot de passe du compte peuvent ainsi être enregistrés sur le serveur iSeries.
- Si vous utilisez un modem interne tel que le modem 56 Kbps fourni avec la carte 9793, vérifiez que l'attribut de réseau MDMCOUNTRYID est correctement défini. Pour cela, utilisez la commande DSPNETA (Afficher les attributs du réseau). Si cet attribut n'est pas correctement défini, modifiez sa valeur à l'aide de la commande CHGNETA (Modifier les attributs du réseau).

Etapes de configuration du système en cours

Si la configuration TCP/IP existe déjà et est fonctionnelle, exécutez les étapes suivantes pour configurer la connexion universelle si vous vous connectez aux Téléservices via le serveur local de MaSociété :

1. Complétez le formulaire de planification.
2. Démarrez iSeries Navigator et sélectionnez l'assistant de connexion universelle.
3. Indiquez les informations demandées (service, adresse et pays) dans les boîtes de dialogue de l'assistant de connexion universelle.
4. Sous Connexion à partir du système en cours, sélectionnez la connexion par ligne commutée utilisant AT&T Global Network Services comme type de connexion.
5. Sélectionnez une ressource matérielle, un numéro de téléphone principal et un numéro de téléphone de secours pour la création d'une connexion via le modem.
6. Pour l'option de proxy, configurez un serveur proxy cible.
7. Indiquez que ce serveur ne fournit pas de connexion aux autres serveurs ou partitions.
8. Passez en revue la fenêtre Récapitulatif afin de vérifier que la configuration répond à vos besoins et cliquez sur **Terminer** pour enregistrer la configuration.
9. Lorsque vous y êtes invité, testez la connexion aux Téléservices à partir de votre serveur.

- 10. Configurez une configuration de sauvegarde.

Remarque : Répétez ce processus pour chaque application de service à utiliser.

Détails du scénario : Configuration d'une connexion commutée point à point à AGNS

Une fois que les conditions requises sont réunies, vous pouvez commencer la configuration de la connexion universelle via l'assistant.

Etape 1 : Complétez le formulaire de planification.

Le formulaire de planification suivant illustre le type d'informations dont vous avez besoin pour pouvoir configurer la connexion AGNS. Vous utilisez ces informations lors de l'exécution de l'assistant de connexion universelle.

Formulaire de planification	Réponses
Informations relatives à la maintenance <ul style="list-style-type: none"> • Société • Nom du contact • Numéro de téléphone • Service d'assistance ou numéro de messagerie • Numéro de télécopie • Numéro de fax secondaire 	<ul style="list-style-type: none"> • MaSociété • Jean Dupont • 515-870-9990 • 515-870-9942 • 515-870-5586 • 515-870-5587
Adresse de la société <ul style="list-style-type: none"> • Adresse postale • Ville ou localité • Etat ou province • Pays (ou région) • Code postal • Version en langue nationale • Adresse de courrier électronique • Adresse de courrier électronique secondaire • Support pour les PTF (correctifs) 	<ul style="list-style-type: none"> • 94 West Proctor St. • Boone • Iowa • Etats-Unis • 55902 • Anglais (2924) • monnom@société.com • monnom@autresociété.com • Sélection automatique
Emplacement <ul style="list-style-type: none"> • Pays (ou région) • Etat 	<ul style="list-style-type: none"> • Etats-Unis • Iowa
Méthode de connexion	Via le serveur local (en cours) iSeries
Type de connexion	Une connexion commutée via AT&T Global Network Services
Ressource matériel	CMN08

- Si vous préférez utiliser les commandes CL pour créer la configuration, utilisez les commandes Modifier point de contact (CHGCNTINF) et Création d'une configuration de maintenance (CRTSRVCFG).

Etape 2 : Démarrez iSeries Navigator et sélectionnez l'assistant de connexion universelle.

Pour démarrer l'assistant de connexion universelle et commencer à établir votre connexion, procédez comme suit :

1. Ouvrez le logiciel iSeries Navigator.
2. Sélectionnez sous le dossier Mes connexions le serveur à configurer pour les Téléservices.
3. Développez l'arborescence de **Réseau**.
4. Développez l'arborescence de **Services d'accès distant**.
5. Cliquez à l'aide du bouton droit de la souris sur **Profils de connexion de l'expéditeur**.

6. Sélectionnez **Configuration de connexion universelle** pour démarrer l'assistant de connexion universelle. La boîte de dialogue de bienvenue apparaît.

| **Remarque :** Une barre de progression indique qu'iSeries Navigator charge l'assistant de connexion universelle. En cas d'incident pendant l'exécution de l'assistant, consultez la section «Identification et résolution des incidents liés à l'assistant de connexion universelle», à la page 70 pour trouver une solution. Relancez l'assistant après avoir résolu l'incident.

Etape 3 : Indiquez les informations demandées (service, adresse et pays) dans les boîtes de dialogue de l'assistant.

Pour entrer des informations sur votre entreprise et vos connexions, procédez comme suit :

1. Dans la boîte de dialogue Choix d'une configuration, sélectionnez **Configuration de connexion principale** ou **Configuration de connexion de secours**. La configuration par défaut est la configuration de connexion principale. Cochez la case **Affichage et modification des informations concernant le contact** et cliquez sur **Suivant**.
2. Dans la boîte de dialogue Informations de maintenance, entrez les informations suivantes sur MaSociété et cliquez sur **Suivant** :
 - Société – MaSociété
 - Nom du contact – Jean Dupont
 - Numéro de téléphone – 515-870-9990
 - Service d'assistance ou numéro de messagerie — 515-870-9999
 - Numéro de fax — 515-870-5586
 - Numéro de fax secondaire — 515-870-9942

Si ces informations existent sur votre serveur, les données relatives à votre société s'affichent dans les zones correspondantes. Par exemple, si MaSociété a déjà créé une configuration, l'assistant extrait les données de la configuration existante.


3. Dans la boîte de dialogue Adresse de la société, entrez l'adresse de MaSociété et cliquez sur **Suivant**.
 - Adresse postale – 94 West Proctor St.
 - Ville ou localité – Boone
 - Etat ou province – Iowa
 - Pays ou région – Etats-Unis
 - Code postal – 55902
 - Version en langue nationale – English (2924)
 - Adresse de courrier électronique – monnom@société.com
 - Adresse de courrier électronique secondaire – monnom@autresociété.com
 - Support pour les PTF – Sélection automatique
4. Dans la boîte de dialogue Emplacement, sélectionnez le pays (ou la région) et l'état ou la province dans lesquels est situé votre serveur iSeries puis cliquez sur **Suivant**.
 - Pays ou région – Etats-Unis
 - Etat – Iowa

| **Etape 4 : Sous Connexion à partir du système en cours, sélectionnez la connexion commutée en utilisant le type de connexion AT&T Global Network Services.**

| **Remarque :** Il existe une case à cocher **Configuration supplémentaire d'une connexion proxy** . Si cette case est cochée, une étape 6 apparaîtra. Si votre société possède un proxy HTTP ou que vous avez configuré un proxy de maintenance et de support sur un autre système ou une autre partition et que vous souhaitez utiliser les applications de connexion universelle prenant en charge la connexion via un proxy, cochez cette case.

| **Etape 5 : Sélectionnez une ressource matérielle, un numéro de téléphone principal et un numéro de téléphone de secours pour la création d'une connexion via le modem.**

- | Pour indiquer les ressources matériel, les lignes téléphoniques et les modems :
- | 1. Sélectionnez une ressource matériel existante dans la liste de la boîte de dialogue et cliquez sur **Suivant**. Vous pouvez trier la liste des ressources matériel des manières suivantes :
 - | • Liste des ressources du modem interne uniquement
 - | • Liste de toutes les ressources par nom.
 - | • Liste de toutes les ressources par emplacement
 - | 2. Sélectionnez le pays ou la région, et l'état appropriés dans la boîte de dialogue Numéro de téléphone. Un groupe de villes et de numéros de téléphone correspondants s'affiche dans la liste Ville. Sélectionnez un numéro de téléphone dans la liste. Si votre emplacement requiert un préfixe de numérotation (tel que le 9) ou ne nécessite pas que vous spécifiez une partie du numéro de téléphone (telle que l'indicatif régional), modifiez le numéro de téléphone sélectionné. Si un espace est requis entre le préfixe de numérotation et le reste du numéro, insérez une virgule afin d'ajouter un espace. Cliquez sur **Suivant**. L'assistant affiche la boîte de dialogue Numéro de téléphone secondaire.

| **Remarque :** Si vous n'avez jamais connecté votre serveur via AT&T, les numéros de téléphone peuvent ne pas être à jour. Vérifiez vos sélections de numéros de téléphone sur le site Web AT&T Business Internet Services (www.attbusiness.net) .
 - | 3. Facultatif : Sélectionnez le pays ou la région, et l'état appropriés dans la boîte de dialogue Numéro de téléphone secondaire. Un groupe de villes et de numéros de téléphone correspondants s'affiche dans la liste Ville. Sélectionnez un numéro de téléphone dans la liste, modifiez-le (si nécessaire) comme indiqué ci-avant et cliquez sur **Suivant**.

| Si votre serveur dispose d'un modem externe associé à la ressource matériel et la ligne, l'assistant vous amène dans la boîte de dialogue Modem (voir étape 4). Si la ressource est sélectionnée pour un modem interne, l'assistant vous amène à l'étape 8.
 - | 4. Facultatif : Si votre serveur utilise un modem externe, sélectionnez un nom de modem dans la liste et cliquez sur **Suivant**.

| **Etape 6 : Pour l'option de proxy, configurez un serveur proxy cible.**

| **Remarque :** Cet écran apparaît uniquement si vous avez choisi l'option de serveur proxy au cours de l'étape 4.

| Pour configurer un serveur proxy cible

- | 1. **Essayez d'abord d'établir une connexion au serveur proxy**
 - | a. Choisissez cette option si vous souhaitez que le proxy ait la priorité sur la configuration de ce scénario.
 - | b. Si nécessaire, cochez la case **Le serveur proxy cible requiert une authentification standard HTTP** et remplissez les champs **Nom d'utilisateur** et **Mot de passe**.
 - | c. Cliquez sur **Suivant** et passez à l'étape suivante.
- | 2. **Essayez d'établir une connexion si la configuration préalablement définie échoue**
 - | a. Choisissez cette option si le proxy doit uniquement être utilisé lorsque la configuration de ce scénario échoue.
 - | b. Complétez le champ **Adresse IP ou nom d'hôte du proxy**.
 - | c. Complétez le champ **Port du serveur proxy**.
 - | d. Si nécessaire, cochez la case **Le serveur proxy cible requiert une authentification standard HTTP** et remplissez les champs **Nom d'utilisateur** et **Mot de passe**.
 - | e. Cliquez sur **Suivant** et passez à l'étape suivante.

| **Etape 7 : Indiquez que ce serveur ne fournit pas de connexion aux autres serveurs ou partitions.**

| Cliquez sur **Non** pour indiquer que ce serveur possède une connexion directe avec les Téléservices mais qu'il ne fournit pas de connexion aux autres systèmes ou partitions.

| **Etape 8 : Passez en revue la fenêtre Récapitulatif afin de vérifier que la configuration répond à vos besoins et cliquez sur Terminer pour enregistrer la configuration.**

| Pour terminer la configuration du serveur et la sauvegarder, procédez comme suit :

- | 1. Consultez le récapitulatif de la configuration. Cliquez sur **Précédent** si vous devez modifier une valeur dans l'une des boîtes de dialogue de l'assistant.
- | 2. Lorsque la configuration est correcte, cliquez sur **Terminer** pour sauvegarder la configuration. Une barre de progression vous indique que l'assistant est en train de sauvegarder la configuration.

| **Etape 9 : Testez la connexion aux Téléservices à partir de votre serveur.**

| Pour tester la configuration, procédez comme suit :

- | 1. Cliquez sur **Oui** lorsque l'assistant vous invite à tester la configuration. La boîte de dialogue Vérification de la connexion universelle s'affiche.
- | 2. Notez les erreurs éventuelles pendant que l'assistant affiche la progression de la vérification.
- | 3. Cliquez sur **OK** lorsque l'assistant indique que la vérification est terminée.
- | 4. Si l'assistant détecte des erreurs, redémarrez l'assistant de connexion universelle, apportez les corrections nécessaires, sauvegardez, puis testez à nouveau la configuration corrigée.

| **Etape 10 : Configurez une configuration de sauvegarde.**

| Si une méthode de connexion supplémentaire est disponible, nous vous recommandons de réexécuter l'assistant afin de configurer une sauvegarde. Cette sauvegarde sera utilisée automatiquement en cas d'échec de la connexion principale.

Scénario : Configuration d'une connexion commutée point à point pour un serveur fournissant une connectivité à d'autres systèmes via AGNS

Situation

Dans ce scénario, vous êtes responsable de la gestion d'un serveur iSeries pour MaSociété, une petite entreprise de fabrication située à Boone, dans l'Iowa. Dans le cadre de cette gestion, vous devez établir une connexion entre les Téléservices et les quatre serveurs iSeries de MaSociété. Comme MaSociété ne dispose pas d'une connexion de réseau Internet, vous pourriez accéder par liaison commutée à AT&T pour connecter vos serveurs iSeries à IBM via une connexion point à point. Par ailleurs, le seul modem dont vous disposez est un modem 7852-400 externe et vous souhaitez utiliser ce modem pour tous vos serveurs.

Solution

Créez une connexion universelle vers IBM via AT&T Global Network Services (AGNS). Dans ce cas, vous devez établir une connexion via le gestionnaire de connexions sur le serveur iSeries doté d'un modem par le biais d'une connexion point à point AGNS vers les Téléservices. Le serveur iSeries tient lieu de point de connexion vers les trois autres serveurs.

- | (Facultatif) Votre système peut tenir lieu de point de connexion pour les trois autres serveurs MaSociété de votre entreprise qui ont besoin de se connecter aux Téléservices, comme décrit dans Configuration d'une connexion commutée point à point éloignée. Dans ce cas, vous devez soit sélectionner un profil de réponse L2TP existant, soit laisser l'assistant de connexion universelle créer un profil de réponse L2TP. Pour plus d'informations sur les profils de réponse L2TP, consultez la rubrique L2TP (ligne virtuelle).

Avantages

Ce scénario offre les avantages suivants :

- MaSociété n'a pas besoin d'investir dans du matériel ou du logiciel supplémentaire pour bénéficier des Téléservices. Vous pouvez configurer cette connexion à l'aide de l'assistant de connexion universelle en utilisant votre modem externe existant ou les commandes CL.
- Les trois autres serveurs de MaSociété peuvent se connecter à distance aux Téléservices via un serveur unique. MaSociété n'a donc besoin que d'un seul modem et non d'un modem distinct pour chaque système ou partition.
- La connexion AGNS fournit à MaSociété une méthode simple pour accéder aux Téléservices qui permettent de faciliter la résolution des incidents liés au serveur, le suivi du matériel et du logiciel système en cours ou la réception de mises à jour et de correctifs de logiciel.
- L'AGNS offre une connexion sécurisée entre MaSociété et IBM en mettant en oeuvre sa propre sécurité pour établir cette connexion. Vous n'avez pas besoin de fournir une sécurité supplémentaire.

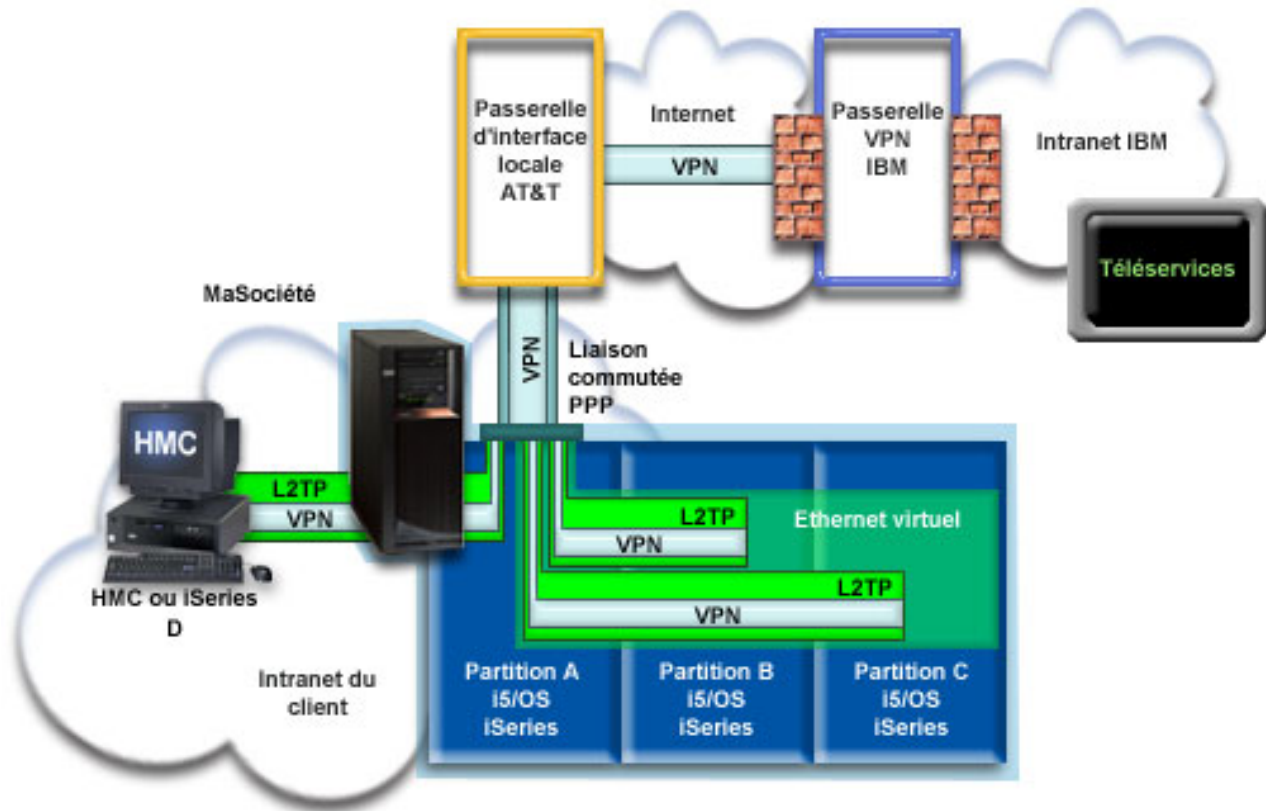
Objectifs

Dans ce scénario, le client souhaite s'assurer qu'IBM peut prendre en charge le système MaSociété sur le réseau via une connexion point à point utilisant AT&T Global Network Services. Les objectifs de ce scénario sont les suivants :

- Créer une connexion commutée point à point sécurisée entre les quatre serveurs de MaSociété et les Téléservices via AT&T Global Network Services
- Automatiser le service d'assistance à la clientèle via les Téléservices et différents services
- Permettre aux Téléservices de créer un inventaire matériel et logiciel du système iSeries de MaSociété.
- Permettre aux Téléservices d'envoyer des correctifs et des mises à jour de logiciel à MaSociété via le réseau

Détails

Le schéma suivant illustre la connexion du serveur iSeries de MaSociété aux Téléservices via une connexion AT&T Global Network Services.



Configuration de la connexion universelle

- iSeries Navigator lance l'assistant de connexion universelle pour configurer la connexion. Cette opération a besoin d'être exécutée une seule fois sur le système qui fournit la connectivité, ainsi que sur chacun des systèmes qui utilisent cette connectivité.

Utilisation de la connexion universelle

Lorsqu'une application de service souhaite utiliser la connexion universelle pour communiquer avec IBM, les événements suivants ont lieu :

- Si l'iSeries A doit se connecter, une connexion point à point est établie via le modem local vers une interface de passerelle locale (LIG) AT&T. Si l'iSeries B, C ou D doit se connecter, une connexion point à point est établie via un tunnel L2TP utilisant le modem éloigné vers AT&T.
- Un réseau virtuel privé (VPN) est établi, si l'application de service ne fournit pas ses propres communications cryptées, via l'interface de passerelle locale AT&T et Internet vers une passerelle de réseau privé virtuel chez IBM.
- L'application de service communique avec les serveurs IBM appropriés pour exécuter le service demandé.

Conditions requises et préalables

Les conditions requises pour pouvoir activer les Téléservices via une connexion AGNS sont les suivantes :

- Vérifiez qu'iSeries Access for Windows et iSeries Navigator sont installés sur votre ordinateur personnel (voir iSeries Access for Windows - Installation et configuration).
- Assurez-vous d'avoir installé tous les Service Packs les plus récents pour iSeries Navigator. Les scénarios présentés utilisent la version 5.4 du logiciel.

- Vérifiez que TCP/IP est actif. Vous pouvez démarrer TCP/IP via la commande STRTCP (Démarrer TCP/IP).
- Pour pouvoir configurer la connexion à partir de l'assistant de connexion universelle, vous devez disposer du droit de responsable de la sécurité (*SECOFR) associé aux droits spéciaux *ALLOBJ, *IOSYSCFG et *SECADM dans votre profil utilisateur i5/OS et du droit *USE sur WRKCNTINF.
- Vous devez installer les utilitaires de connectivité TCP/IP (5722-TC1).
- Pour que le réseau privé virtuel (VPN) et la couche SSL fonctionnent, vous devez installer Digital Certificate Manager (DCM) (5722-SS1 option 34).
- Assurez-vous que la valeur système QRETSVRSEC a pour valeur 1. Pour cela, utilisez la commande DSPSYSVAL (Afficher une valeur système). Si cette valeur n'est pas fixée à 1, entrez la commande CHGSYSVAL (Modifier une valeur système).
- Si vous utilisez un modem interne tel que le modem 56 Kbps fourni avec la carte 9793, vérifiez que l'attribut de réseau MDMCOUNTRYID est correctement défini. Pour cela, utilisez la commande DSPSYSVAL (Afficher une valeur système). Si cet attribut n'est pas correctement défini, modifiez sa valeur à l'aide de la commande CHGSYSVAL (Modifier une valeur système). L'ID utilisateur et le mot de passe du compte peuvent ainsi être enregistrés sur le serveur iSeries.
- Si une connectivité IP est requise entre le système ou la partition comportant le modem et les systèmes ou partitions souhaitant l'utiliser.

Etapes de configuration du système ou de la partition en cours

Si la configuration TCP/IP existe déjà et est fonctionnelle, exécutez les étapes suivantes pour configurer la connexion universelle lorsque votre serveur local tient lieu de point de connexion pour les trois autres serveurs de MaSociété :

1. Complétez le formulaire de planification.
2. Démarrez iSeries Navigator et sélectionnez l'assistant de connexion universelle.
3. Indiquez les informations demandées (service, adresse et pays) dans les boîtes de dialogue de l'assistant de connexion universelle.
4. Sous Connexion à partir du système en cours, sélectionnez la connexion par ligne commutée utilisant le type de connexion AT&T Global Network Services.
5. Sélectionnez une ressource matérielle, un numéro de téléphone principal et un numéro de téléphone de secours pour la création d'une connexion via le modem.
6. Pour l'option de serveur, configurez un serveur proxy de maintenance et de support.
7. Précisez que vous souhaitez que ce serveur iSeries fournisse une connexion aux autres systèmes qui se connectent aux Téléservices.
8. Sélectionnez une interface que les autres serveurs utiliseront lors de leur connexion aux Téléservices.
9. Créez ou sélectionnez des profils de réponse L2TP. Ces profils sont nécessaires pour fournir la connectivité aux autres systèmes ou serveurs qui se connectent aux Téléservices via votre serveur.
10. Configurez un serveur proxy de maintenance et de support.
11. Passez en revue la fenêtre Récapitulatif afin de vérifier que la configuration répond à vos besoins et cliquez sur **Terminer** pour enregistrer la configuration.
12. Lorsque vous y êtes invité, testez la connexion aux Téléservices à partir de votre serveur.
13. Configurez une configuration de sauvegarde (facultatif).

Détails du scénario : Configuration d'une connexion commutée point à point à un serveur fournissant une connexion aux autres systèmes

Une fois que les conditions requises sont réunies, vous pouvez commencer la configuration de la connexion universelle via l'assistant.

Étape 1 : Complétez le formulaire de planification.

Le formulaire de planification suivant illustre le type d'informations dont vous avez besoin pour pouvoir configurer la connexion AGNS. Vous utilisez ces informations lors de l'exécution de l'assistant de

connexion universelle.

Formulaire de planification	Réponses
Informations relatives à la maintenance <ul style="list-style-type: none">• Société• Nom du contact• Numéro de téléphone• Service d'assistance ou numéro de messagerie• Numéro de télécopie• Numéro de fax secondaire	<ul style="list-style-type: none">• MaSociété• Jean Dupont• 515-870-9990• 515-870-9942• 515-870-5586• 515-870-5587
Adresse de la société <ul style="list-style-type: none">• Adresse postale• Ville ou localité• Etat ou province• Pays (ou région)• Code postal• Version en langue nationale• Adresse de courrier électronique• Adresse de courrier électronique secondaire• Support pour les PTF (correctifs)	<ul style="list-style-type: none">• 94 West Proctor St.• Boone• Iowa• Etats-Unis• 55902• Anglais (2924)• monnom@société.com• monnom@autresociété.com• Sélection automatique
Emplacement <ul style="list-style-type: none">• Pays (ou région)• Etat	<ul style="list-style-type: none">• Etats-Unis• Iowa
Méthode de connexion	Via le serveur iSeries en cours
Type de connexion	Une connexion commutée utilisant AT&T Global Network Services
Ressource matériel	CMN07
Type de modem (si vous utilisez un modem externe)	IBM 7852-400
Description de l'interface pour les autres systèmes à utiliser lors de la connexion à ce système via une adresse TCP/IP	10.1.1.1 (Ethernet)

Si vous préférez utiliser les commandes CL pour créer la configuration, utilisez les commandes Modifier point de contact (CHGCNTINF) et Création d'une configuration de maintenance (CRTSRVCFG).

Etape 2 : Démarrez iSeries Navigator et sélectionnez l'assistant de connexion universelle.

Pour démarrer l'assistant de connexion universelle et commencer à établir votre connexion, procédez comme suit :

1. Ouvrez le logiciel iSeries Navigator.
2. Sélectionnez sous le dossier Mes connexions le serveur à configurer pour les Téléservices.
3. Développez l'arborescence de **Réseau**.
4. Développez l'arborescence de **Services d'accès distant**.
5. Cliquez à l'aide du bouton droit de la souris sur **Profils de connexion de l'expéditeur**.
6. Sélectionnez **Configuration de connexion universelle** pour démarrer l'assistant de connexion universelle. La boîte de dialogue de bienvenue apparaît.

Remarque : Une barre de progression indique qu'iSeries Navigator charge l'assistant de connexion universelle. En cas d'incident pendant l'exécution de l'assistant, consultez la section «Identification et résolution des incidents liés à l'assistant de connexion universelle», à la page 70 pour trouver une solution. Relancez l'assistant après avoir résolu l'incident.

Etape 3 : Indiquez les informations demandées (service, adresse et pays) dans les boîtes de dialogue de l'assistant.

Pour entrer des informations sur votre entreprise et vos connexions, procédez comme suit :

1. Dans la boîte de dialogue Choix d'une configuration, sélectionnez **Configuration de connexion principale** ou **Configuration de connexion de secours**. La configuration par défaut est la configuration de connexion principale. Cochez la case **Affichage et modification des informations concernant le contact** et cliquez sur **Suivant**.
2. Dans la boîte de dialogue Informations de maintenance, entrez les informations suivantes sur MaSociété et cliquez sur **Suivant** :
 - Société – MaSociété
 - Nom du contact – Jean Dupont
 - Numéro de téléphone – 515-870-9990
 - Service d'assistance ou numéro de messagerie — 515-870-9999
 - Numéro de fax — 515-870-5586
 - Numéro de fax secondaire — 515-870-9942

Si ces informations existent sur votre serveur, les données relatives à votre société s'affichent dans les zones correspondantes. Par exemple, si MaSociété a déjà créé une configuration, l'assistant extrait les données de la configuration existante.

3. Dans la boîte de dialogue Adresse de la société, entrez l'adresse de MaSociété et cliquez sur **Suivant**.
 - Adresse postale – 94 West Proctor St.
 - Ville ou localité – Boone
 - Etat ou province – Iowa
 - Pays ou région – Etats-Unis
 - Code postal – 55902
 - Version en langue nationale – English (2924)
 - Adresse de courrier électronique – monnom@société.com
 - Adresse de courrier électronique secondaire – monnom@autresociété.com
 - Support pour les PTF – Sélection automatique
4. Dans la boîte de dialogue Emplacement, sélectionnez le pays (ou la région) et l'état ou la province dans lesquels est situé votre serveur iSeries puis cliquez sur **Suivant**.
 - Pays ou région – Etats-Unis
 - Etat – Iowa


Etape 4 : Sous Connexion à partir du système en cours, sélectionnez la connexion commutée en utilisant le type de connexion AT&T Global Network Services.

Remarque : Il existe une case à cocher **Configuration supplémentaire d'une connexion proxy** . Si votre société possède un proxy HTTP ou que vous avez configuré un proxy de maintenance et de support sur un autre système ou une autre partition et que vous souhaitez utiliser les applications de connexion universelle prenant en charge la connexion via un proxy, cochez cette case. Si cette case est cochée, une étape 6 apparaîtra.

Etape 5 : Sélectionnez une ressource matérielle, un numéro de téléphone principal et un numéro de téléphone de secours pour la création d'une connexion via le modem.

Pour indiquer les ressources matériel, les lignes téléphoniques et les modems :

1. Sélectionnez une ressource matériel existante dans la liste de la boîte de dialogue et cliquez sur **Suivant**. Vous pouvez trier la liste des ressources matériel des manières suivantes :
 - Liste des ressources du modem interne uniquement
 - Liste de toutes les ressources par nom.
 - Liste de toutes les ressources par emplacement
2. Sélectionnez le pays ou la région, et l'état appropriés dans la boîte de dialogue Numéro de téléphone. Un groupe de villes et de numéros de téléphone correspondants s'affiche dans la liste Ville. Sélectionnez un numéro de téléphone dans la liste. Si votre emplacement requiert un préfixe de numérotation (tel que le 9) ou ne nécessite pas que vous spécifiez une partie du numéro de téléphone (telle que l'indicatif régional), modifiez le numéro de téléphone sélectionné. Si un espace est requis entre le préfixe de numérotation et le reste du numéro, insérez une virgule afin d'ajouter un espace. Cliquez sur **Suivant**. L'assistant affiche la boîte de dialogue Numéro de téléphone secondaire.

Remarque : Si vous n'avez jamais connecté votre serveur via AT&T, les numéros de téléphone peuvent ne pas être à jour. Vérifiez vos sélections de numéros de téléphone sur le site Web AT&T Business Internet Services (www.attbusiness.net) .
3. Facultatif : Sélectionnez le pays ou la région, et l'état appropriés dans la boîte de dialogue Numéro de téléphone secondaire. Un groupe de villes et de numéros de téléphone correspondants s'affiche dans la liste Ville. Sélectionnez un numéro de téléphone dans la liste, modifiez-le (si nécessaire) comme indiqué ci-avant et cliquez sur **Suivant**.

Si votre serveur dispose d'un modem externe associé à la ressource matériel et la ligne, l'assistant vous amène dans la boîte de dialogue Modem (voir étape 4). Si la ressource est sélectionnée pour un modem interne, l'assistant vous amène à l'étape 8.
4. Facultatif : Si votre serveur utilise un modem externe, sélectionnez un nom de modem dans la liste et cliquez sur **Suivant**.

Etape 6 : Pour l'option de proxy, configurez un serveur proxy cible.

Remarque : Cet écran apparaît uniquement si vous avez choisi l'option de serveur proxy au cours de l'étape 4.

Pour configurer un serveur proxy cible

1. **Essayez d'abord d'établir une connexion au serveur proxy**
 - a. Choisissez cette option si vous souhaitez que le proxy ait la priorité sur la configuration de ce scénario.
 - b. Si nécessaire, cochez la case **Le serveur proxy cible requiert une authentification standard HTTP** et remplissez les champs **Nom d'utilisateur** et **Mot de passe**.
 - c. Cliquez sur **Suivant** et passez à l'étape suivante.
2. **Essayez d'établir une connexion si la configuration préalablement définie échoue**
 - a. Choisissez cette option si le proxy doit uniquement être utilisé lorsque la configuration de ce scénario échoue.
 - b. Complétez le champ **Adresse IP ou nom d'hôte du proxy**.
 - c. Complétez le champ **Port du serveur proxy**.
 - d. Si nécessaire, cochez la case **Le serveur proxy cible requiert une authentification standard HTTP** et remplissez les champs **Nom d'utilisateur** et **Mot de passe**.
 - e. Cliquez sur **Suivant** et passez à l'étape suivante.

Etape 7 : Précisez que vous souhaitez que ce serveur iSeries fournisse une connexion aux autres systèmes qui se connectent aux Téléservices.

Sélectionnez **Oui** pour indiquer que ce serveur fournit une connexion aux autres serveurs ou partitions et cliquez sur **Suivant**.

| **Etape 8 : Sélectionnez une interface que les autres serveurs utiliseront lors de leur connexion aux Téléservices.**

Sélectionnez les interfaces utilisées par les serveurs MaSociété pour se connecter à IBM. Sélectionnez l'une des options suivantes :

- Cliquez sur **Tout type d'interface** pour que la connexion universelle puisse accepter des connexions de toutes les interfaces TCP/IP.
 - Cliquez sur **Sélection des interfaces** afin de sélectionner des interfaces pour écouter les demandes de connexion. La boîte à liste devient active. Sélectionnez toutes les interfaces appropriées. L'assistant crée automatiquement un profil de réponse L2TP pour chaque interface non associée à un profil de réponse. Si des profils de réponse L2TP sont associés à une interface, l'assistant vous invite à sélectionner le profil de réponse à associer en particulier à cette interface.
- | Vous pouvez sélectionner plusieurs interfaces avec la touche CTRL.

| **Remarque :** En outre, l'assistant configure le serveur proxy HTTP de maintenance et de support pour démarrer en même temps que le TCP et pour écouter des requêtes de connexion sur l'interface sélectionnée.

Dans notre cas, MaSociété sélectionne l'interface Ethernet 10.1.1.1.

| **Etape 9 : Créez ou sélectionnez les profils de réponse L2TP.**

1. Sélectionnez un profil de réponse L2TP pour chacune des interfaces sélectionnées. Sélectionnez l'une des options suivantes :

- Cliquez sur **Créer un nouveau profil QL2TP mm** où mm représente un chiffre compris entre 0 et 99. Avec cette option, l'assistant crée, nomme et numérote de façon consécutive le nouveau profil L2TP.
- Cliquez sur **Sélectionner un profil existant** afin de choisir un profil L2TP spécifique pour l'interface associée.

Dans notre cas, MaSociété laisse l'assistant de connexion universelle créer un profil L2TP.

2. Vérifiez que la case **Démarrer le profil de réponse L2TP en même temps que TCP/IP** est cochée. En effet, MaSociété souhaite démarrer ce profil en même temps que TCP/IP.

Remarque : En démarrant le profil de réponse L2TP sélectionné avec TCP/IP, tous les autres profils L2TP pour cette interface seront modifiés pour ne pas démarrer avec TCP/IP.

Si vous indiquez que vous ne souhaitez pas démarrer les profils de réponse L2TP sélectionnés en même temps que TCP/IP, vous devez démarrer manuellement le profil de réponse L2TP avant d'utiliser la connexion aux systèmes.

| **Etape 10 : Configurez un serveur proxy de maintenance et de support.**

| Pour configurer le serveur proxy de maintenance et de support :

1. Complétez le champ **Port serveur**.
2. Si vous le souhaitez, cochez la case **Requiert une authentification standard HTTP** et complétez les champs **Nom d'utilisateur** et **Mot de passe**. L'authentification est facultative. Si vous spécifiez ces champs, toutes les autres partitions ou tous les autres systèmes utilisant ce serveur proxy doivent entrer les données d'identification de sécurité.
3. Cliquez sur **Suivant** et passez à l'étape suivante.

| **Etape 11 : Passez en revue la fenêtre Récapitulatif afin de vérifier que la configuration répond à vos besoins et cliquez sur Terminer pour enregistrer la configuration.**

Pour terminer la configuration du serveur et la sauvegarder, procédez comme suit :

1. Consultez le récapitulatif de la configuration. Cliquez sur **Précédent** si vous devez modifier une valeur dans l'une des boîtes de dialogue de l'assistant.
2. Lorsque la configuration est correcte, cliquez sur **Terminer** pour sauvegarder la configuration. Une barre de progression vous indique que l'assistant est en train de sauvegarder la configuration.

| **Etape 12 : Testez la connexion aux Téléservices à partir de votre serveur.**

Pour tester la configuration, procédez comme suit :

1. Cliquez sur **Oui** lorsque l'assistant vous invite à tester la configuration. La boîte de dialogue Vérification de la connexion universelle s'affiche.
2. Notez les erreurs éventuelles pendant que l'assistant affiche la progression de la vérification.
3. Cliquez sur **OK** lorsque l'assistant indique que la vérification est terminée.
4. Si l'assistant détecte des erreurs, redémarrez l'assistant de connexion universelle, apportez les corrections nécessaires, sauvegardez, puis testez à nouveau la configuration corrigée.

Remarque : Une fois l'exécution de ce scénario terminée, le système est prêt à communiquer avec IBM et à accepter les demandes de connexion éloignée provenant des autres systèmes. Le scénario Configuration d'une connexion commutée point à point éloignée doit être répété pour chaque système ou partition qui devra utiliser ce système pour accéder aux Téléservices IBM.

| **Etape 13 : Configurez une configuration de sauvegarde (facultatif).**

| Si une méthode de connexion supplémentaire est disponible, nous vous recommandons de réexécuter l'assistant afin de configurer une sauvegarde. Cette sauvegarde sera utilisée automatiquement en cas d'échec de la connexion principale.

Scénario : Configuration d'une connexion commutée point à point distante

Situation

| Supposons que vous acquériez un serveur iSeries supplémentaire pour MaSociété, une petite entreprise de fabrication située à Boone, dans l'Iowa. Dans le cadre de cette gestion, vous devez établir une connexion entre les Téléservices et le serveur iSeries de MaSociété. Comme ce serveur ne comprend pas de modem et que MaSociété ne dispose pas d'une connexion réseau liée à Internet, vous pourriez configurer une connexion distante via un autre serveur iSeries ou une console HMC qui dispose déjà d'une connexion commutée point à point avec les Téléservices. Pour plus d'informations sur la configuration dans le cas d'un environnement HMC, consultez la rubrique Configuration de votre environnement de maintenance de l'IBM Systems Hardware Information Center.

Solution

Créez une connexion universelle vers IBM via AT&T Global Network Services (AGNS). Dans ce cas, vous devez établir une connexion à l'aide du gestionnaire de connexions sur votre serveur iSeries éloigné via une connexion point à point AGNS vers les Téléservices.

Avantages

Ce scénario offre les avantages suivants :

- MaSociété n'a pas besoin d'investir dans un modem, des câbles ou du logiciel supplémentaires pour bénéficier des Téléservices. Vous pouvez configurer cette connexion à l'aide de l'assistant de connexion universelle ou des commandes CL.

- La connexion AGNS fournit à MaSociété une méthode simple pour accéder aux Téléservices qui permettent de faciliter la résolution des incidents liés au serveur, le suivi du matériel et du logiciel système en cours ou la réception de mises à jour et de correctifs de logiciel.
- L'AGNS offre une connexion sécurisée entre MaSociété et IBM en mettant en oeuvre sa propre sécurité pour établir cette connexion. Vous n'avez pas besoin de fournir une sécurité supplémentaire.

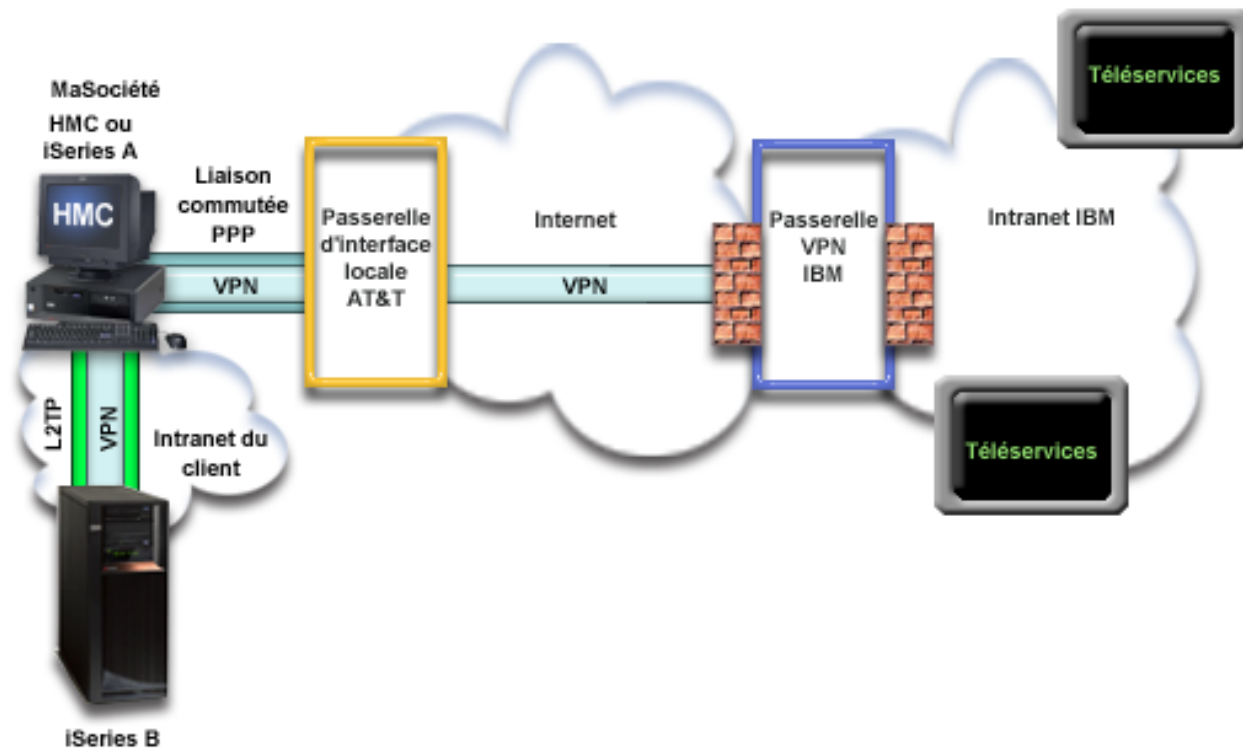
Objectifs

Dans ce scénario, le client souhaite s'assurer qu'IBM peut prendre en charge le serveur MaSociété éloigné sur le réseau via une connexion point à point utilisant AT&T Global Network Services. Les objectifs de ce scénario sont les suivants :

- Créer une connexion commutée point à point éloignée entre le client et les Téléservices via AT&T Global Network Services
- Automatiser le service d'assistance à la clientèle via les Téléservices et différents services
- Permettre aux Téléservices éloignés de créer un inventaire matériel et logiciel des serveurs iSeries de MaSociété.
- Permettre aux Téléservices d'envoyer des correctifs et des mises à jour de logiciel au serveur iSeries MaSociété éloigné via le réseau

Détails

Le schéma suivant illustre la création d'une connexion éloignée vers un autre serveur pour accéder aux Téléservices via une connexion AT&T Global Network Services.



Conditions requises et préalables

Les conditions requises pour pouvoir activer les Téléservices via une connexion AGNS éloignée sont les suivantes :

- Vérifiez qu'iSeries Access for Windows et iSeries Navigator sont installés sur votre ordinateur personnel (voir iSeries Access for Windows - Installation et configuration).

- Assurez-vous d'avoir installé tous les Service Packs les plus récents pour iSeries Navigator. Les scénarios présentés utilisent la version V5R4 du logiciel.
- Vérifiez que TCP/IP est actif. Vous pouvez démarrer TCP/IP via la commande STRTCP (Démarrer TCP/IP).
- Pour pouvoir configurer la connexion à partir de l'assistant de connexion universelle, vous devez disposer du droit de responsable de la sécurité (*SECOFR) associé aux droits spéciaux *ALLOBJ, *IOSYSCFG et *SECADM dans votre profil utilisateur i5/OS et du droit *USE sur WRKCNTINF.
- Vous devez installer les utilitaires de connectivité TCP/IP (5722-TC1).
- Vous devez installer Digital Certificate Manager (DCM) (5722-SS1 option 34).

Remarque : Ce scénario est pris en charge pour les systèmes 5.1, 5.2, 5.3 et 5.4. Cependant, iSeries Navigator 5.3 ou version ultérieure est requis pour configurer cette option. Le réseau privé virtuel (VPN) sera utilisé sur AT&T uniquement si votre serveur est de niveau 5.3 ou supérieur.

- Assurez-vous que la valeur système QRETSVRSEC a pour valeur 1. Pour cela, utilisez la commande DSPSYSVAL (Afficher une valeur système). Si cette valeur n'est pas fixée à 1, entrez la commande CHGSYSVAL (Modifier une valeur système).
- La connexion universelle depuis le serveur vers le modem doit avoir été configurée pour fournir la connectivité AT&T aux autres serveurs pour que vous puissiez utiliser la connexion éloignée. Pour plus d'informations sur la configuration de la console HMC pour une utilisation avec le modem s'il est connecté, voir Configuration de votre environnement de maintenance, dans l'IBM Systems Hardware Information Center.
- Vous devez avoir configuré la connectivité TCP/IP entre ce système et le système comportant le modem.

Étapes de configuration du serveur distant

Si la configuration TCP/IP existe déjà et est fonctionnelle, exécutez les étapes suivantes pour configurer la connexion universelle si vous vous connectez aux Téléservices via un serveur éloigné :

1. Complétez le formulaire de planification.
2. Démarrez iSeries Navigator et sélectionnez l'assistant de connexion universelle.
3. Indiquez les informations demandées (service, adresse et pays ou région) dans les boîtes de dialogue de cet assistant.
4. Sous Connexion via un autre système ou une autre partition, sélectionnez la connexion par ligne commutée utilisant le type de connexion AT&T Global Network Services.
5. Pour créer une connexion distante à IBM, indiquez l'adresse de la passerelle ou le nom d'hôte du serveur qui se connecte à IBM.
6. Pour l'option de proxy, configurez un serveur proxy cible.
7. Indiquez que ce serveur ne fournit pas de connexion aux autres serveurs ou partitions.
8. Passez en revue la fenêtre Récapitulatif afin de vérifier que la configuration répond à vos besoins et cliquez sur **Terminer** pour enregistrer la configuration.
9. Lorsque vous y êtes invité, testez la connexion aux Téléservices à partir de votre serveur.
10. Configurez une configuration de sauvegarde (facultatif).

Détails du scénario : Configuration d'une connexion commutée point à point éloignée

Une fois que les conditions requises sont réunies, vous pouvez commencer la configuration de la connexion universelle via l'assistant.

Étape 1 : Complétez le formulaire de planification.

Le formulaire de planification suivant illustre le type d'informations dont vous avez besoin pour pouvoir configurer la connexion AGNS. Vous utilisez ces informations lors de l'exécution de l'assistant de connexion universelle.

Formulaire de planification	Réponses
Informations relatives à la maintenance <ul style="list-style-type: none"> • Société • Nom du contact • Numéro de téléphone • Service d'assistance ou numéro de messagerie • Numéro de télécopie • Numéro de fax secondaire 	<ul style="list-style-type: none"> • MaSociété • Jean Dupont • 515-870-9990 • 515-870-9942 • 515-870-5586 • 515-870-5587
Adresse de la société <ul style="list-style-type: none"> • Adresse postale • Ville ou localité • Etat ou province • Pays (ou région) • Code postal • Version en langue nationale • Adresse de courrier électronique • Adresse de courrier électronique secondaire • Support pour les PTF (correctifs) 	<ul style="list-style-type: none"> • 94 West Proctor St. • Boone • Iowa • Etats-Unis • 55902 • Anglais (2924) • monnom@société.com • monnom@autresociété.com • Sélection automatique
Emplacement <ul style="list-style-type: none"> • Pays (ou région) • Etat 	<ul style="list-style-type: none"> • Etats-Unis • Iowa
Méthode de connexion	Via un serveur éloigné
Type de connexion	Une connexion commutée utilisant AT&T Global Network Services
Adresse de la passerelle du serveur éloigné ou nom d'hôte	192.168.1.1. (Vous pouvez aussi fournir à la place le nom d'hôte [charles.masociété.com] si le système en cours de configuration est du niveau 5.3 ou supérieur.)

Si vous préférez utiliser les commandes CL pour créer la configuration, utilisez les commandes Modifier point de contact (CHGCNTINF) et Création d'une configuration de maintenance (CRTSRVCFG).

Etape 2 : Démarrez iSeries Navigator et sélectionnez l'assistant de connexion universelle.

Pour démarrer l'assistant de connexion universelle et commencer à établir votre connexion, procédez comme suit :

1. Ouvrez le logiciel iSeries Navigator.
2. Sélectionnez sous le dossier Mes connexions le serveur à configurer pour les Téléservices.
3. Développez l'arborescence de **Réseau**.
4. Développez l'arborescence de **Services d'accès distant**.
5. Cliquez à l'aide du bouton droit de la souris sur **Profils de connexion de l'expéditeur**.
6. Sélectionnez **Configuration de connexion universelle** pour démarrer l'assistant de connexion universelle. La boîte de dialogue de bienvenue apparaît.

Remarque : Une barre de progression indique qu'iSeries Navigator charge l'assistant de connexion universelle. En cas d'incident pendant l'exécution de l'assistant, consultez la section «Identification et résolution des incidents liés à l'assistant de connexion universelle», à la page 70 pour trouver une solution. Relancez l'assistant après avoir résolu l'incident.

Etape 3 : Indiquez les informations demandées (service, adresse et pays (ou région)) dans les boîtes de dialogue de l'assistant.

Pour entrer des informations sur votre entreprise et vos connexions, procédez comme suit :

1. Dans la boîte de dialogue Choix d'une configuration, sélectionnez **Configuration de connexion principale** ou **Configuration de connexion de secours**. La configuration par défaut est la configuration de connexion principale. Cochez la case **Affichage et modification des informations concernant le contact** et cliquez sur **Suivant**.

2. Dans la boîte de dialogue Informations de maintenance, entrez les informations suivantes sur MaSociété et cliquez sur **Suivant** :

- Société – MaSociété
- Nom du contact – Jean Dupont
- Numéro de téléphone – 515-870-9990
- Service d'assistance ou numéro de messagerie — 515-870-9999
- Numéro de fax — 515-870-5586
- Numéro de fax secondaire — 515-870-9942

Si ces informations existent sur votre serveur, les données relatives à votre société s'affichent dans les zones correspondantes. Par exemple, si MaSociété a déjà créé une configuration, l'assistant extrait les données de la configuration existante.

3. Dans la boîte de dialogue Adresse de la société, entrez l'adresse de MaSociété et cliquez sur **Suivant**.

- Adresse postale – 94 West Proctor St.
- Ville ou localité – Boone
- Etat ou province – Iowa
- Pays ou région – Etats-Unis
- Code postal – 55902
- Version en langue nationale – English (2924)
- Adresse de courrier électronique – monnom@société.com
- Adresse de courrier électronique secondaire – monnom@autresociété.com
- Support pour les PTF – Sélection automatique

4. Dans la boîte de dialogue Emplacement, sélectionnez le pays (ou la région) et l'état ou la province dans lesquels est situé votre serveur iSeries puis cliquez sur **Suivant**.

- Pays ou région – Etats-Unis
- Etat – Iowa

Etape 4 : Sous Connexion via un autre système ou une autre partition, sélectionnez la connexion par ligne commutée utilisant le type de connexion AT&T Global Network Services.

Remarque : Il existe une case à cocher **Configuration supplémentaire d'une connexion proxy** . Si cette case est cochée, une étape 6 apparaîtra. Si vous utilisez un modem sur un système ou une partition i5/OS éloigné(é) de niveau 5.4 ou supérieur, vous pouvez spécifier le proxy de maintenance et de support. Si votre société possède un serveur proxy HTTP, vous pouvez le spécifier.

Etape 5 : Pour créer une connexion éloignée à IBM, indiquez l'adresse de la passerelle ou le nom d'hôte du serveur qui se connecte à IBM.

Indiquez l'adresse de la passerelle du serveur éloigné ou le nom du serveur éloigné et cliquez sur **Suivant**. L'adresse de la passerelle est 192.168.1.1. Dans ce scénario, le nom du serveur MaSociété est Charles.masociété.com.

Etape 6 : Pour l'option de proxy, configurez un serveur proxy cible.

Remarque : Cet écran apparaît uniquement si vous avez choisi l'option de serveur proxy au cours de l'étape 4.

Pour configurer un serveur proxy cible

1. **Essayez d'abord d'établir une connexion au serveur proxy**

- a. Choisissez cette option si vous souhaitez que le proxy ait la priorité sur la configuration de ce scénario.

- | b. Si nécessaire, cochez la case **Le serveur proxy cible requiert une authentification standard HTTP** et remplissez les champs **Nom d'utilisateur** et **Mot de passe**.
- | c. Cliquez sur **Suivant** et passez à l'étape suivante.
- | **2. Essayez d'établir une connexion si la configuration préalablement définie échoue**
- | a. Choisissez cette option si le proxy doit uniquement être utilisé lorsque la configuration de ce scénario échoue.
- | b. Complétez le champ **Adresse IP ou nom d'hôte du proxy**.
- | c. Complétez le champ **Port du serveur proxy**.
- | d. Si nécessaire, cochez la case **Le serveur proxy cible requiert une authentification standard HTTP** et remplissez les champs **Nom d'utilisateur** et **Mot de passe**.
- | e. Cliquez sur **Suivant** et passez à l'étape suivante.

| **Etape 7 : Indiquez que ce serveur ne fournit pas de connexion aux autres serveurs ou partitions.**

| Cliquez sur **Non** pour indiquer que ce serveur possède une connexion directe avec les Téléservices mais qu'il ne fournit pas de connexion aux autres systèmes ou partitions.

| **Etape 8 : Passez en revue la fenêtre Récapitulatif afin de vérifier que la configuration répond à vos besoins et cliquez sur Terminer pour enregistrer la configuration.**

| Pour terminer la configuration du serveur et la sauvegarder, procédez comme suit :

- | 1. Consultez le récapitulatif de la configuration. Cliquez sur **Précédent** si vous devez modifier une valeur dans l'une des boîtes de dialogue de l'assistant.
- | 2. Lorsque la configuration est correcte, cliquez sur **Terminer** pour sauvegarder la configuration. Une barre de progression vous indique que l'assistant est en train de sauvegarder la configuration.

| **Etape 9 : Testez la connexion aux Téléservices à partir de votre serveur.**

Pour tester la configuration, procédez comme suit :

Remarque : Vérifiez que le profil de réponse L2TP est actif sur le serveur éloigné ou, si le serveur éloigné est une console HMC, vérifiez qu'il a été configuré de façon à permettre l'accès par liaison commutée au moyen du modem local.

- 1. Cliquez sur **Oui** lorsque l'assistant vous invite à tester la configuration. La boîte de dialogue Vérification de la connexion universelle s'affiche.
- 2. Notez les erreurs éventuelles pendant que l'assistant affiche la progression de la vérification.
- 3. Cliquez sur **OK** lorsque l'assistant indique que la vérification est terminée.
- 4. Si l'assistant détecte des erreurs, redémarrez l'assistant de connexion universelle, apportez les corrections nécessaires, sauvegardez, puis testez à nouveau la configuration corrigée.

| **Etape 10 : Configurez une configuration de sauvegarde (facultatif).**

| Si une méthode de connexion supplémentaire est disponible, nous vous recommandons de réexécuter l'assistant afin de configurer une sauvegarde. Cette sauvegarde sera utilisée automatiquement en cas d'échec de la connexion principale.

Scénario : Configuration d'une connexion directe à Internet

Situation

Supposons que vous êtes responsable de la gestion d'un serveur iSeries pour MaSociété, une petite entreprise de fabrication située à Boone, dans l'Iowa. Dans le cadre de cette gestion, vous devez établir une connexion entre les Téléservices et le serveur iSeries de MaSociété. Comme MaSociété dispose d'une connexion Internet et que son serveur iSeries possède une adresse IP à acheminement global fixe ou se trouve derrière un pare-feu NAT (pour plus d'informations, voir NAT compatible IPSec), vous pouvez créer une connexion depuis votre serveur iSeries via votre connexion Internet. Comme vous n'avez pas besoin de fournir de connexion pour d'autres systèmes, vous n'avez pas besoin non plus de fournir des connexions pour d'autres serveurs ou partitions.

Solution

Créez une connexion universelle vers IBM via une connexion Internet directe. L'assistant de connexion universelle crée toutes les définitions requises pour la connexion vers les Téléservices.

Avantages

Ce scénario offre les avantages suivants :

- MaSociété peut utiliser son matériel et son fournisseur Internet existants pour bénéficier des Téléservices. Vous pouvez configurer cette connexion à l'aide de l'assistant de connexion universelle ou des commandes CL.
- L'utilisation d'une connexion Internet existante fournit à MaSociété une méthode simple pour accéder aux Téléservices qui permettent de faciliter la résolution des incidents liés au serveur, le suivi du matériel et du logiciel système en cours ou la réception de mises à jour et de correctifs de logiciel.
- Cette option offre des connexions à plus haut débit que les solutions reposant sur un modem.

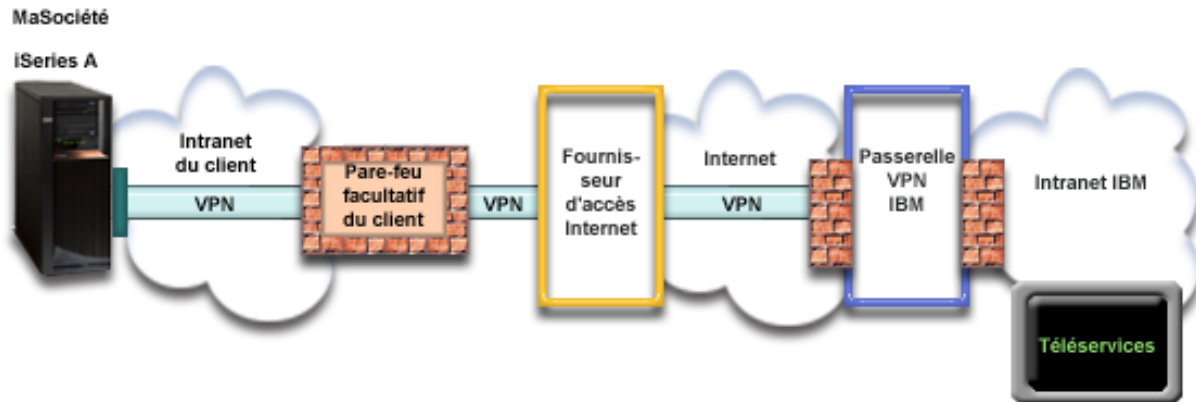
Objectifs

Dans ce scénario, le client souhaite s'assurer qu'IBM peut prendre en charge le système MaSociété sur le réseau via une connexion directe à Internet. Les objectifs de ce scénario sont les suivants :

- Créer une connexion Internet entre MaSociété et les Téléservices en utilisant le câble de modem de MaSociété ou une autre connexion haut débit via une connexion Internet directe
- Automatiser le service d'assistance à la clientèle via les Téléservices et différents services
- Permettre aux Téléservices de créer un inventaire matériel et logiciel du système iSeries de MaSociété.
- Permettre aux Téléservices d'envoyer des correctifs et des mises à jour de logiciel à MaSociété via le réseau

Détails

Le schéma suivant illustre la connexion du serveur iSeries de MaSociété aux Téléservices via une connexion directe à Internet.



Configuration de la connexion universelle

- iSeries Navigator lance l'assistant de connexion universelle pour configurer la connexion. Cette opération n'a besoin d'être exécutée qu'une seule fois sauf si des informations doivent être mises à jour.

Utilisation de la connexion universelle

Lorsqu'une application de service souhaite utiliser la connexion universelle pour communiquer avec IBM, les événements suivants ont lieu :

- Un réseau privé virtuel (VPN) est établi via votre connexion Internet existante vers une passerelle de réseau privé virtuel chez IBM si l'application de service ne prend pas en charge la sécurité.
- L'application de service communique avec les serveurs IBM appropriés pour exécuter le service demandé.

Conditions requises et préalables

Les conditions requises pour pouvoir activer les Téléservices via une connexion directe à Internet sont les suivantes :

- Le serveur iSeries doit disposer d'une adresse IP à acheminement global ou doit se trouver derrière un pare-feu NAT avec une adresse à acheminement global.
- Vérifiez qu'iSeries Access for Windows et iSeries Navigator sont installés sur votre ordinateur personnel (voir iSeries Access for Windows - Installation et configuration).
- Assurez-vous d'avoir installé tous les Service Packs les plus récents pour iSeries Navigator. Les scénarios présentés utilisent la version 5.4 du logiciel.
- Vérifiez que TCP/IP est actif. Vous pouvez démarrer TCP/IP via la commande STRTCP (Démarrer TCP/IP).
- Pour pouvoir configurer la connexion à partir de l'assistant de connexion universelle, vous devez disposer du droit de responsable de la sécurité (*SECOFR) associé aux droits spéciaux *ALLOBJ, *IOSYSCFG et *SECADM dans votre profil utilisateur i5/OS et du droit *USE sur WRKCNTINF.
- Vous devez installer les utilitaires de connectivité TCP/IP (5722-TC1).
- Vous devez installer Digital Certificate Manager (DCM) (5722-SS1 option 34).
- Assurez-vous que la valeur système QRETSVRSEC a pour valeur 1. Pour cela, utilisez la commande DSPSYSVAL (Afficher une valeur système). Si cette valeur n'est pas fixée à 1, entrez la commande CHGSYSVAL (Modifier une valeur système).
- Vérifiez que la route TCP/IP par défaut ou qu'une route hôte achemine le trafic en provenance de l'interface TCP/IP appropriée vers Internet afin que la connexion VPN ou d'autres connexions de service puissent être établies avec IBM. Pour des informations supplémentaires, consultez les rubriques «Détermination des adresses de passerelle VPN IBM», à la page 69 et «Détermination des adresses de destination de services IBM», à la page 69.

- Assurez-vous que vos règles de filtrage autorisent l'acheminement sur Internet du trafic de la connexion universelle. Pour plus d'informations, voir «Pare-feu de filtrage des paquets IP», à la page 3.

Etapas de configuration du système **en cours**

Si la configuration TCP/IP existe déjà et est fonctionnelle, exécutez les étapes suivantes pour configurer la connexion universelle si vous vous connectez aux Téléservices via le serveur local de MaSociété :

1. Complétez le formulaire de planification.
2. Démarrez iSeries Navigator et sélectionnez l'assistant de connexion universelle.
3. Indiquez les informations demandées (service, adresse et pays) dans les boîtes de dialogue de l'assistant de connexion universelle.
4. Sous Connexion à partir du système en cours, sélectionnez le type de connexion Connexion directe à Internet.
5. Pour l'option de proxy, configurez un serveur proxy cible.
6. Indiquez que ce serveur ne fournit pas de connexion aux autres serveurs ou partitions.
7. Passez en revue la fenêtre Récapitulatif afin de vérifier que la configuration répond à vos besoins et cliquez sur **Terminer** pour enregistrer la configuration.
8. Lorsque vous y êtes invité, testez la connexion aux Téléservices à partir de votre serveur.
9. Configurez une configuration de sauvegarde.

Détails du scénario : Configuration d'une connexion directe à Internet

Une fois que les conditions requises sont réunies, vous pouvez commencer la configuration de la connexion universelle via l'assistant.

Etape 1 : Complétez le formulaire de planification.

Le formulaire de planification suivant illustre le type d'informations dont vous avez besoin pour pouvoir configurer la connexion directe à Internet. Vous utilisez ces informations lors de l'exécution de l'assistant de connexion universelle.

Formulaire de planification	Réponses
Informations relatives à la maintenance <ul style="list-style-type: none"> Société Nom du contact Numéro de téléphone Service d'assistance ou numéro de messagerie Numéro de télécopie Numéro de fax secondaire 	<ul style="list-style-type: none"> MaSociété Jean Dupont 515-870-9990 515-870-9942 515-870-5586 515-870-5587
Adresse de la société <ul style="list-style-type: none"> Adresse postale Ville ou localité Etat ou province Pays (ou région) Code postal Version en langue nationale Adresse de courrier électronique Adresse de courrier électronique secondaire Support pour les PTF (correctifs) 	<ul style="list-style-type: none"> 94 West Proctor St. Boone Iowa Etats-Unis 55902 Anglais (2924) monnom@société.com monnom@autresociété.com Sélection automatique
Emplacement <ul style="list-style-type: none"> Pays (ou région) Etat 	<ul style="list-style-type: none"> Etats-Unis Iowa
Méthode de connexion	Via le serveur local iSeries
Type de connexion	Directe

- | Si vous préférez utiliser les commandes CL pour créer la configuration, utilisez les commandes Modifier point de contact (CHGCNTINF) et Création d'une configuration de maintenance (CRTSRVCFG).

Etape 2 : Démarrez iSeries Navigator et sélectionnez l'assistant de connexion universelle.

Pour démarrer l'assistant de connexion universelle et commencer à établir votre connexion, procédez comme suit :

1. Ouvrez le logiciel iSeries Navigator.
2. Sélectionnez sous le dossier Mes connexions le serveur à configurer pour les Téléservices.
3. Développez l'arborescence de **Réseau**.
4. Développez l'arborescence de **Services d'accès distant**.
5. Cliquez à l'aide du bouton droit de la souris sur **Profils de connexion de l'expéditeur**.
6. Sélectionnez **Configuration de connexion universelle** pour démarrer l'assistant de connexion universelle. La boîte de dialogue de bienvenue apparaît.

- | **Remarque :** Une barre de progression indique qu'iSeries Navigator charge l'assistant de connexion universelle. En cas d'incident pendant l'exécution de l'assistant, consultez la section «Identification et résolution des incidents liés à l'assistant de connexion universelle», à la page 70 pour trouver une solution. Relancez l'assistant après avoir résolu l'incident.

Etape 3 : Indiquez les informations demandées (service, adresse et pays) dans les boîtes de dialogue de l'assistant.

Pour entrer des informations sur votre entreprise et vos connexions, procédez comme suit :

- | 1. Dans la boîte de dialogue Choix d'une configuration, sélectionnez **Configuration de connexion principale** ou **Configuration de connexion de secours**. La configuration par défaut est la configuration de connexion principale. Cochez la case **Affichage et modification des informations concernant le contact** et cliquez sur **Suivant**.
- | 2. Dans la boîte de dialogue Informations de maintenance, entrez les informations suivantes sur MaSociété et cliquez sur **Suivant** :
 - Société – MaSociété
 - Nom du contact – Jean Dupont
 - Numéro de téléphone – 515-870-9990
 - | • Service d'assistance ou numéro de messagerie — 515-870-9999
 - | • Numéro de fax — 515-870-5586
 - | • Numéro de fax secondaire — 515-870-9942

Si ces informations existent sur votre serveur, les données relatives à votre société s'affichent dans les zones correspondantes. Par exemple, si MaSociété a déjà créé une configuration, l'assistant extrait les données de la configuration existante.

- | 3. Dans la boîte de dialogue Adresse de la société, entrez l'adresse de MaSociété et cliquez sur **Suivant**.
 - Adresse postale – 94 West Proctor St.
 - | • Ville ou localité – Boone
 - | • Etat ou province – Iowa
 - | • Pays ou région – Etats-Unis
 - | • Code postal – 55902
 - | • Version en langue nationale – English (2924)
 - | • Adresse de courrier électronique – monnom@société.com
 - | • Adresse de courrier électronique secondaire – monnom@autresociété.com
 - | • Support pour les PTF – Sélection automatique
- | 4. Dans la boîte de dialogue Emplacement, sélectionnez le pays (ou la région) et l'état ou la province dans lesquels est situé votre serveur iSeries puis cliquez sur **Suivant**.
 - Pays ou région – Etats-Unis
 - Etat – Iowa

| **Etape 4 : Sous Connexion à partir du système en cours, sélectionnez le type de connexion Connexion directe à Internet.**

| **Remarque :** Il existe une case à cocher **Configuration supplémentaire d'une connexion proxy** . Si votre société possède un proxy HTTP ou que vous avez configuré un proxy de maintenance et de support sur un autre système ou une autre partition et que vous souhaitez utiliser les applications de connexion universelle prenant en charge la connexion via un proxy, cochez cette case. Si cette case est cochée, une étape 5 apparaîtra.

| **Etape 5 : Pour l'option de proxy, configurez un serveur proxy cible.**

| **Remarque :** Cet écran apparaît uniquement si vous avez choisi l'option de serveur proxy au cours de l'étape 4.

| Pour configurer un serveur proxy cible

| 1. **Essayez d'abord d'établir une connexion au serveur proxy**

- | a. Choisissez cette option si vous souhaitez que le proxy ait la priorité sur la configuration de ce scénario.
- | b. Si nécessaire, cochez la case **Le serveur proxy cible requiert une authentification standard HTTP** et remplissez les champs **Nom d'utilisateur** et **Mot de passe**.
- | c. Cliquez sur **Suivant** et passez à l'étape suivante.

| 2. **Essayez d'établir une connexion si la configuration préalablement définie échoue**

- | a. Choisissez cette option si le proxy doit uniquement être utilisé lorsque la configuration de ce scénario échoue.
- | b. Complétez le champ **Adresse IP ou nom d'hôte du proxy**.
- | c. Complétez le champ **Port du serveur proxy**.
- | d. Si nécessaire, cochez la case **Le serveur proxy cible requiert une authentification standard HTTP** et remplissez les champs **Nom d'utilisateur** et **Mot de passe**.
- | e. Cliquez sur **Suivant** et passez à l'étape suivante.

| **Etape 6 : Indiquez que ce serveur ne fournit pas de connexion aux autres serveurs ou partitions.**

| Cliquez sur **Non** pour indiquer que ce serveur possède une connexion directe avec les Téléservices mais qu'il ne fournit pas de connexion aux autres serveurs ou partitions.

| **Etape 7 : Passez en revue la fenêtre Récapitulatif afin de vérifier que la configuration répond à vos besoins et cliquez sur Terminer pour enregistrer la configuration.**

| Pour terminer la configuration du serveur et la sauvegarder, procédez comme suit :

- | 1. Consultez le récapitulatif de la configuration. Cliquez sur **Précédent** si vous devez modifier une valeur dans l'une des boîtes de dialogue de l'assistant.
- | 2. Lorsque la configuration est correcte, cliquez sur **Terminer** pour sauvegarder la configuration. Une barre de progression vous indique que l'assistant est en train de sauvegarder la configuration.

| **Etape 8 : Testez la connexion aux Téléservices à partir de votre serveur.**

| Pour tester la configuration, procédez comme suit :

- | 1. Cliquez sur **Oui** lorsque l'assistant vous invite à tester la configuration. La boîte de dialogue Vérification de la connexion universelle s'affiche.
- | 2. Notez les erreurs éventuelles pendant que l'assistant affiche la progression de la vérification.
- | 3. Cliquez sur **OK** lorsque l'assistant indique que la vérification est terminée.
- | 4. Si l'assistant détecte des erreurs, redémarrez l'assistant de connexion universelle, apportez les corrections nécessaires, sauvegardez, puis testez à nouveau la configuration corrigée.

| Etape 9 : Configurez une configuration de sauvegarde (facultatif).

| Si une méthode de connexion supplémentaire est disponible, nous vous recommandons de réexécuter l'assistant afin de configurer une sauvegarde. Cette sauvegarde sera utilisée automatiquement en cas d'échec de la connexion principale.

| **Remarque :** Un scénario de sauvegarde approprié pourrait être l'utilisation d'une ligne commutée. Dans l'éventualité d'un échec du réseau LAN, la ligne commutée permet de contacter les services IBM.

Scénario : Configuration d'une connexion directe à Internet à partir d'un serveur qui fournit la connectivité pour d'autres systèmes ou partitions

Situation

| Supposons que vous êtes responsable de la gestion d'un serveur iSeries pour MaSociété, une petite entreprise de fabrication située à Boone, dans l'Iowa. Dans le cadre de cette gestion, vous devez établir une connexion entre les Téléservices et le serveur iSeries de MaSociété. Comme MaSociété dispose d'une connexion Internet et d'un modem à câble à adresse IP à acheminement global fixe, vous pouvez créer une connexion depuis votre serveur iSeries via votre modem. Avec ce système, votre serveur fournit la connectivité (sous la forme d'une passerelle à noeuds multiples VPN ou d'un proxy de maintenance et de support) pour les trois autres serveurs MaSociété que vous devez connecter aux Téléservices.

Solution

| Créez une connexion universelle vers IBM via une connexion Internet directe. L'assistant de connexion universelle crée toutes les définitions requises pour la connexion vers les Téléservices. Afin de fournir la connectivité pour d'autres systèmes, l'assistant va créer un profil de réponse L2TP. Vous pouvez également sélectionner un profil de réponse L2TP existant. Pour plus d'informations sur les profils de réponse L2TP, consultez la rubrique L2TP (ligne virtuelle). En outre, l'assistant procédera à la configuration du proxy de maintenance et de support.

Avantages

Ce scénario offre les avantages suivants :

- | • MaSociété peut utiliser son matériel et son fournisseur Internet existants pour bénéficier des Téléservices. Vous pouvez configurer cette connexion à l'aide de l'assistant de connexion universelle ou des commandes CL.
- | • La connexion Internet fournit à MaSociété une méthode simple pour accéder aux Téléservices qui permettent de faciliter la résolution des incidents liés au serveur, le suivi du matériel et du logiciel système en cours ou la réception de mises à jour et de correctifs de logiciel.
- | • Les trois autres serveurs de MaSociété peuvent se connecter à distance aux Téléservices via un serveur unique. MaSociété a besoin uniquement de la connectivité fournie par un système.
- | • Une connexion Internet directe offre une connexion haut débit vers les services électroniques.
- | • Avec ce scénario, les autres serveurs de MaSociété sont protégés contre un accès via Internet.

Objectifs

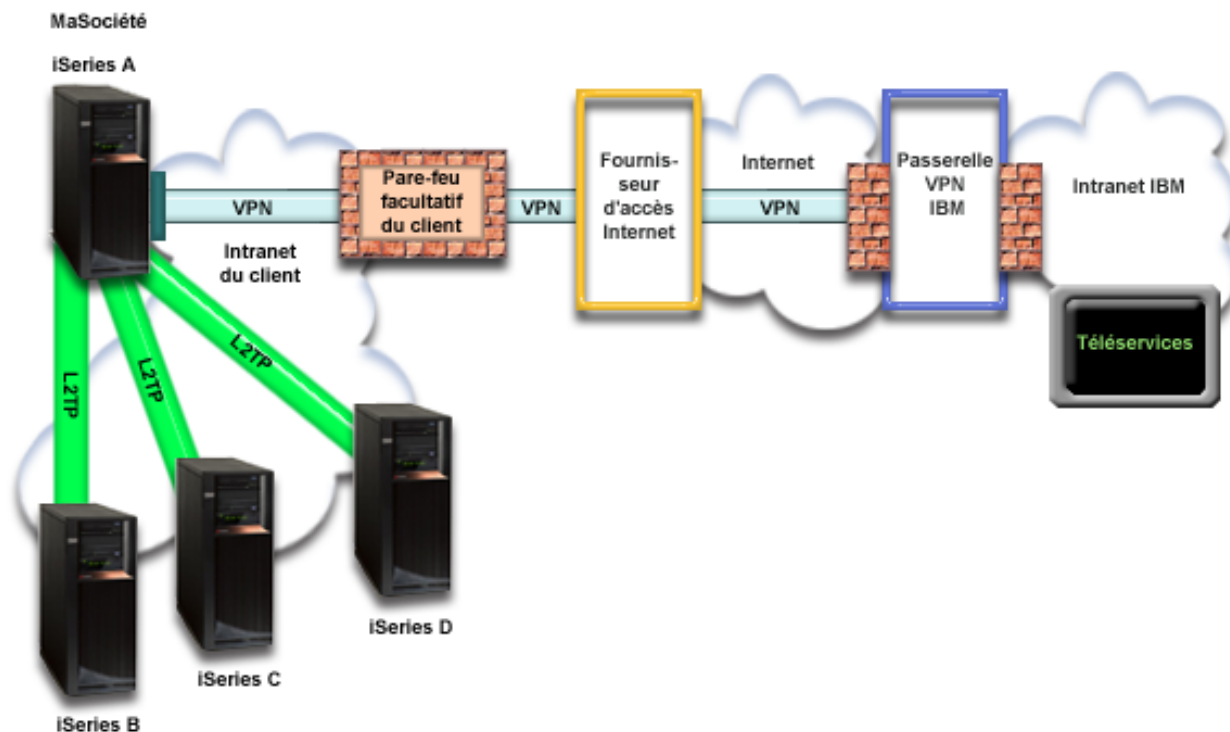
Dans ce scénario, le client souhaite s'assurer qu'IBM peut prendre en charge le système MaSociété via une connexion directe à Internet. Les objectifs de ce scénario sont les suivants :

- | • Créer une connexion directe entre les quatre serveurs de MaSociété et les Téléservices via Internet.
- | • Automatiser le service d'assistance à la clientèle via les Téléservices et différents services
- | • Permettre aux Téléservices de créer un inventaire matériel et logiciel du système iSeries de MaSociété.

- Permettre aux Téléservices d'envoyer des correctifs et des mises à jour de logiciel à MaSociété via le réseau

Détails

Le schéma suivant illustre la connexion du serveur iSeries de MaSociété aux Téléservices via une connexion directe à Internet.



Configuration de la connexion universelle

- iSeries Navigator lance l'assistant de connexion universelle pour configurer la connexion. Cette opération n'a besoin d'être exécutée qu'une seule fois sauf si des informations doivent être mises à jour.

Utilisation de la connexion universelle

Lorsqu'une application de service souhaite utiliser la connexion universelle pour communiquer avec IBM, les événements suivants ont lieu :

- **Si l'application de service ne prend pas en charge la sécurité et qu'iSeries A se connecte :** un réseau privé virtuel (VPN) est établi via votre connexion Internet existante vers une passerelle de réseau privé virtuel chez IBM.
- **Si l'application de service ne prend pas en charge la sécurité et qu'iSeries B, C, ou D se connecte :** un tunnel L2TP est établi vers l'iSeries A qui démarre un réseau privé virtuel via votre connexion Internet existante vers une passerelle de réseau privé virtuel chez IBM.
- **Si l'application de service prend en charge la sécurité et qu'iSeries A se connecte :** une connexion HTTP ou HTTPS est établie avec les serveurs IBM appropriés.
- **Si l'application de service prend en charge la sécurité, qu'iSeries B, C ou D se connecte et qu'un serveur proxy est pris en charge :** une connexion HTTP ou HTTPS est établie via le serveur proxy de maintenance et de support.

L'application de service communique avec les serveurs IBM appropriés pour exécuter le service demandé.

Conditions requises et préalables

Les conditions requises pour pouvoir activer les Téléservices via une connexion directe à Internet sont les suivantes :

- Le serveur iSeries doit disposer d'une adresse IP à acheminement global ou doit se trouver derrière un pare-feu NAT avec une adresse à acheminement global.
- Vérifiez qu'iSeries Access for Windows et iSeries Navigator sont installés sur votre ordinateur personnel (voir iSeries Access for Windows - Installation et configuration).
- Assurez-vous d'avoir installé tous les Service Packs les plus récents pour iSeries Navigator. Les scénarios présentés utilisent la version 5.4 du logiciel.
- Vérifiez que TCP/IP est actif. Vous pouvez démarrer TCP/IP via la commande STRTCP (Démarrer TCP/IP).
- Pour pouvoir configurer la connexion à partir de l'assistant de connexion universelle, vous devez disposer du droit de responsable de la sécurité (*SECOFR) associé aux droits spéciaux *ALLOBJ, *IOSYSCFG et *SECADM dans votre profil utilisateur i5/OS et du droit *USE sur WRKCNTINF.
- Vous devez installer les utilitaires de connectivité TCP/IP (5722-TC1).
- Vous devez installer Digital Certificate Manager (DCM) (5722-SS1 option 34).
- Assurez-vous que la valeur système QRETSVRSEC a pour valeur 1. Pour cela, utilisez la commande DSPSYSVAL (Afficher une valeur système). Si cette valeur n'est pas fixée à 1, entrez la commande CHGSYSVAL (Modifier une valeur système).
- Vérifiez que la route TCP/IP par défaut ou qu'une route hôte achemine le trafic en provenance de l'interface TCP/IP appropriée vers Internet afin que la connexion VPN ou d'autres connexions de service puissent être établies avec IBM. Pour des informations supplémentaires sur le réseau virtuel privé (VPN), consultez les rubriques «Détermination des adresses de passerelle VPN IBM», à la page 69 et «Détermination des adresses de destination de services IBM», à la page 69.
- Assurez-vous que vos règles de filtrage autorisent l'acheminement sur Internet du trafic de la connexion universelle. Pour plus d'informations, voir «Pare-feu de filtrage des paquets IP», à la page 3.

Étapes de configuration du système **en cours**

Si la configuration TCP/IP existe déjà et est fonctionnelle, exécutez les étapes suivantes pour configurer la connexion universelle lorsque votre serveur local tient lieu de point de connexion pour les trois autres serveurs de MaSociété :

1. Complétez le formulaire de planification.
2. Démarrez iSeries Navigator et sélectionnez l'assistant de connexion universelle.
3. Indiquez les informations demandées (service, adresse et pays) dans les boîtes de dialogue de l'assistant de connexion universelle.
4. Sous Connexion à partir du système en cours, sélectionnez le type de connexion Connexion directe à Internet.
5. Pour l'option de proxy, configurez un serveur proxy cible.
6. Précisez que vous souhaitez que ce serveur iSeries fonctionne en tant que point de connexion par le biais duquel les autres serveurs ou partitions pourront se connecter aux Téléservices.
7. Sélectionnez une interface que les autres serveurs utiliseront lors de leur connexion aux Téléservices.
8. Créez ou sélectionnez des profils de réponse L2TP.
9. Configurez un serveur proxy de maintenance et de support.
10. Passez en revue la fenêtre Récapitulatif afin de vérifier que la configuration répond à vos besoins et cliquez sur **Terminer** pour enregistrer la configuration.
11. Lorsque vous y êtes invité, testez la connexion aux Téléservices à partir de votre serveur.
12. Configurez une configuration de sauvegarde (facultatif).

Détails du scénario : Configuration d'une connexion directe à Internet à partir d'un serveur qui joue le rôle de point de connexion pour les autres systèmes

Une fois que les conditions requises sont réunies, vous pouvez commencer la configuration de la connexion universelle via l'assistant.

Etape 1 : Complétez le formulaire de planification.

Le formulaire de planification suivant illustre le type d'informations dont vous avez besoin pour pouvoir configurer la connexion directe à Internet. Vous utilisez ces informations lors de l'exécution de l'assistant de connexion universelle.

Formulaire de planification	Réponses
Informations relatives à la maintenance <ul style="list-style-type: none"> • Société • Nom du contact • Numéro de téléphone • Service d'assistance ou numéro de messagerie • Numéro de télécopie • Numéro de fax secondaire 	<ul style="list-style-type: none"> • MaSociété • Jean Dupont • 515-870-9990 • 515-870-9942 • 515-870-5586 • 515-870-5587
Adresse de la société <ul style="list-style-type: none"> • Adresse postale • Ville ou localité • Etat ou province • Pays (ou région) • Code postal • Version en langue nationale • Adresse de courrier électronique • Adresse de courrier électronique secondaire • Support pour les PTF (correctifs) 	<ul style="list-style-type: none"> • 94 West Proctor St. • Boone • Iowa • Etats-Unis • 55902 • Anglais (2924) • monnom@société.com • monnom@autresociété.com • Sélection automatique
Emplacement <ul style="list-style-type: none"> • Pays (ou région) • Etat 	<ul style="list-style-type: none"> • Etats-Unis • Iowa
Méthode de connexion	Via le serveur iSeries en cours
Description de l'interface pour les autres systèmes à utiliser comme point de connexion	10.1.1.1
Nom du profil de réponse L2TP	QL2TP00

Si vous préférez utiliser les commandes CL pour créer la configuration, utilisez les commandes Modifier point de contact (CHGCNTINF) et Création d'une configuration de maintenance (CRTSRVCFG).

Etape 2 : Démarrez iSeries Navigator et sélectionnez l'assistant de connexion universelle.

Pour démarrer l'assistant de connexion universelle et commencer à établir votre connexion, procédez comme suit :

1. Ouvrez le logiciel iSeries Navigator.
2. Sélectionnez sous le dossier Mes connexions le serveur à configurer pour les Téléservices.
3. Développez l'arborescence de **Réseau**.
4. Développez l'arborescence de **Services d'accès distant**.
5. Cliquez à l'aide du bouton droit de la souris sur **Profils de connexion de l'expéditeur**.
6. Sélectionnez **Configuration de connexion universelle** pour démarrer l'assistant de connexion universelle. La boîte de dialogue de bienvenue apparaît.

Remarque : Une barre de progression indique qu'iSeries Navigator charge l'assistant de connexion universelle. En cas d'incident pendant l'exécution de l'assistant, consultez la section

«Identification et résolution des incidents liés à l'assistant de connexion universelle», à la page 70 pour trouver une solution. Relancez l'assistant après avoir résolu l'incident.

Etape 3 : Indiquez les informations demandées (service, adresse et pays) dans les boîtes de dialogue de l'assistant.

Pour entrer des informations sur votre entreprise et vos connexions, procédez comme suit :

1. Dans la boîte de dialogue Choix d'une configuration, sélectionnez **Configuration de connexion principale** ou **Configuration de connexion de secours**. La configuration par défaut est la configuration de connexion principale. Cochez la case **Affichage et modification des informations concernant le contact** et cliquez sur **Suivant**.
2. Dans la boîte de dialogue Informations de maintenance, entrez les informations suivantes sur MaSociété et cliquez sur **Suivant** :
 - Société – MaSociété
 - Nom du contact – Jean Dupont
 - Numéro de téléphone – 515-870-9990
 - Service d'assistance ou numéro de messagerie — 515-870-9999
 - Numéro de fax — 515-870-5586
 - Numéro de fax secondaire — 515-870-9942

Si ces informations existent sur votre serveur, les données relatives à votre société s'affichent dans les zones correspondantes. Par exemple, si MaSociété a déjà créé une configuration, l'assistant extrait les données de la configuration existante.

3. Dans la boîte de dialogue Adresse de la société, entrez l'adresse de MaSociété et cliquez sur **Suivant**.
 - Adresse postale – 94 West Proctor St.
 - Ville ou localité – Boone
 - Etat ou province – Iowa
 - Pays ou région – Etats-Unis
 - Code postal – 55902
 - Version en langue nationale – English (2924)
 - Adresse de courrier électronique – monnom@société.com
 - Adresse de courrier électronique secondaire – monnom@autresociété.com
 - Support pour les PTF – Sélection automatique
4. Dans la boîte de dialogue Emplacement, sélectionnez le pays (ou la région) et l'état ou la province dans lesquels est situé votre serveur iSeries puis cliquez sur **Suivant**.
 - Pays ou région – Etats-Unis
 - Etat – Iowa

Etape 4 : Sous Connexion à partir du système en cours, sélectionnez le type de connexion Connexion directe à Internet.

Remarque : Il existe une case à cocher **Configuration supplémentaire d'une connexion proxy** . Si votre société possède un proxy HTTP ou que vous avez configuré un proxy de maintenance et de support sur un autre système ou une autre partition et que vous souhaitez utiliser les applications de connexion universelle prenant en charge la connexion via un proxy, cochez cette case. Si cette case est cochée, une étape 5 apparaîtra.

Etape 5 : Pour l'option de proxy, configurez un serveur proxy cible.

Remarque : Cet écran apparaît uniquement si vous avez choisi l'option de serveur proxy au cours de l'étape 4.

Pour configurer un serveur proxy cible

1. **Essayez d'abord d'établir une connexion au serveur proxy**
 - a. Choisissez cette option si vous souhaitez que le proxy ait la priorité sur la configuration de ce scénario.

- | b. Si nécessaire, cochez la case **Le serveur proxy cible requiert une authentification standard HTTP** et remplissez les champs **Nom d'utilisateur** et **Mot de passe**.
- | c. Cliquez sur **Suivant** et passez à l'étape suivante.
- | 2. **Essayez d'établir une connexion si la configuration préalablement définie échoue**
 - | a. Choisissez cette option si le proxy doit uniquement être utilisé lorsque la configuration de ce scénario échoue.
 - | b. Complétez le champ **Adresse IP ou nom d'hôte du proxy**.
 - | c. Complétez le champ **Port du serveur proxy**.
 - | d. Si nécessaire, cochez la case **Le serveur proxy cible requiert une authentification standard HTTP** et remplissez les champs **Nom d'utilisateur** et **Mot de passe**.
 - | e. Cliquez sur **Suivant** et passez à l'étape suivante.

| **Etape 6 : Précisez que vous souhaitez que ce serveur iSeries fonctionne en tant que point de connexion par le biais duquel les autres serveurs ou partitions pourront se connecter aux Téléservices.**

| Sélectionnez **Oui** pour indiquer que ce serveur fournit une connexion aux autres serveurs ou partitions et cliquez sur **Suivant**.

| **Etape 7 : Sélectionnez une interface que les autres serveurs utiliseront lors de leur connexion aux Téléservices.**

| Sélectionnez les interfaces utilisées par les serveurs MaSociété pour se connecter à IBM. Sélectionnez l'une des options suivantes :

- | • Cliquez sur **Tout type d'interface** pour que la connexion universelle puisse accepter des connexions de toutes les interfaces TCP/IP.
 - | • Cliquez sur **Sélection des interfaces** afin de sélectionner des interfaces pour écouter les demandes de connexion. La boîte à liste devient active. Sélectionnez toutes les interfaces appropriées. L'assistant crée automatiquement un profil de réponse L2TP pour chaque interface non associée à un profil de réponse. Si des profils de réponse L2TP sont associés à une interface, l'assistant vous invite à sélectionner le profil de réponse à associer en particulier à cette interface.
- | Vous pouvez sélectionner plusieurs interfaces avec la touche CTRL.

| **Remarque :** En outre, l'assistant configure le serveur proxy HTTP de maintenance et de support pour démarrer en même temps que le TCP et pour écouter des requêtes de connexion sur l'interface sélectionnée.

| Dans notre cas, MaSociété sélectionne l'interface Ethernet 10.1.1.1.

| **Etape 8 : Créez ou sélectionnez les profils de réponse L2TP.**

- | 1. Sélectionnez un profil de réponse L2TP pour chacune des interfaces sélectionnées. Sélectionnez l'une des options suivantes :
 - | • Cliquez sur **Créer un nouveau profil QL2TP $_{nn}$** où nn représente un chiffre compris entre 0 et 99. Avec cette option, l'assistant crée, nomme et numérote de façon consécutive le nouveau profil L2TP.
 - | • Cliquez sur **Sélectionner un profil existant** afin de choisir un profil L2TP spécifique pour l'interface associée.
- | Dans notre cas, MaSociété laisse l'assistant de connexion universelle créer un profil L2TP.
- | 2. Vérifiez que la case **Démarrer le profil de réponse L2TP en même temps que TCP/IP** est cochée. En effet, MaSociété souhaite démarrer ce profil en même temps que TCP/IP.

| **Remarque :** En démarrant le profil de réponse L2TP sélectionné avec TCP/IP, tous les autres profils L2TP pour cette interface seront modifiés pour ne pas démarrer avec TCP/IP.

Si vous indiquez que vous ne souhaitez pas démarrer les profils de réponse L2TP sélectionnés en même temps que TCP/IP, vous devez démarrer manuellement le profil de réponse L2TP avant d'utiliser la connexion aux systèmes.

Etape 9 : Configurez un serveur proxy de maintenance et de support.

Pour configurer le serveur proxy de maintenance et de support :

1. Complétez le champ **Port serveur**.
2. Si vous le souhaitez, cochez la case **Requiert une authentification standard HTTP** et complétez les champs **Nom d'utilisateur** et **Mot de passe**. L'authentification est facultative. Si vous spécifiez ces champs, toutes les autres partitions ou tous les autres systèmes utilisant ce serveur proxy doivent entrer les données d'identification de sécurité.
3. Cliquez sur **Suivant** et passez à l'étape suivante.

Etape 10 : Passez en revue la fenêtre Récapitulatif afin de vérifier que la configuration répond à vos besoins et cliquez sur Terminer pour enregistrer la configuration.

Pour terminer la configuration du serveur et la sauvegarder, procédez comme suit :

1. Consultez le récapitulatif de la configuration. Cliquez sur **Précédent** si vous devez modifier une valeur dans l'une des boîtes de dialogue de l'assistant.
2. Lorsque la configuration est correcte, cliquez sur **Terminer** pour sauvegarder la configuration. Une barre de progression vous indique que l'assistant est en train de sauvegarder la configuration.

Etape 11 : Testez la connexion aux Téléservices à partir de votre serveur.

Pour tester la configuration, procédez comme suit :

1. Cliquez sur **Oui** lorsque l'assistant vous invite à tester la configuration. La boîte de dialogue Vérification de la connexion universelle s'affiche.
2. Notez les erreurs éventuelles pendant que l'assistant affiche la progression de la vérification.
3. Cliquez sur **OK** lorsque l'assistant indique que la vérification est terminée.
4. Si l'assistant détecte des erreurs, redémarrez l'assistant de connexion universelle, apportez les corrections nécessaires, sauvegardez, puis testez à nouveau la configuration corrigée.

Remarque : Si la connexion fonctionne, vous êtes prêt à accepter les demandes de connexion provenant d'autres systèmes ou partitions. Consultez la section Configuration d'une connexion multiple entre noeuds via un serveur éloigné pour configurer d'autres systèmes et vous connecter à la connexion universelle via ce serveur.

Etape 12 : Configurez une configuration de sauvegarde (facultatif).

Si une méthode de connexion supplémentaire est disponible, nous vous recommandons de réexécuter l'assistant afin de configurer une sauvegarde. Cette sauvegarde sera utilisée automatiquement en cas d'échec de la connexion principale.

Scénario : Configuration d'une connexion PPP via un fournisseur d'accès Internet

Situation

Supposons que vous êtes responsable de la gestion d'un serveur iSeries pour MaSociété, une petite entreprise de fabrication située à Boone, dans l'Iowa. Dans le cadre de cette gestion, vous devez établir une connexion entre les Téléservices et le serveur iSeries de MaSociété.

Comme MaSociété dispose d'une connexion commutée Internet, vous pouvez créer une connexion à partir de votre serveur iSeries via votre modem et une liaison commutée vers votre fournisseur d'accès Internet (ISP). Comme vous n'avez pas besoin de fournir des connexions pour d'autres systèmes, vous n'avez pas besoin non plus de fournir des connexions pour d'autres serveurs ou partitions.

Solution

- | Créez une connexion universelle vers IBM par le biais d'une liaison commutée via Internet. Dans ce cas,
- | vous devez établir une connexion à l'aide du gestionnaire de connexions sur votre serveur iSeries local
- | via une connexion point à point Internet vers les Téléservices.

Avantages

Ce scénario offre les avantages suivants :

- | • MaSociété n'a pas besoin d'investir dans du matériel ou du logiciel supplémentaire pour bénéficier des
- | Téléservices. Vous pouvez configurer cette connexion à l'aide de l'assistant de connexion universelle ou
- | des commandes CL.
- La connexion Internet fournit à MaSociété une méthode simple pour accéder aux Téléservices qui permettent de faciliter la résolution des incidents liés au serveur, le suivi du matériel et du logiciel système en cours ou la réception de mises à jour et de correctifs de logiciel.
- Vous pouvez utiliser votre connexion de fournisseur d'accès Internet existante pour les Téléservices pour ne pas avoir à vous déconnecter de votre fournisseur pour vous connecter à IBM.

Remarque : Dans ce scénario, MaSociété utilise une connexion de fournisseur d'accès Internet commutée. Vous pouvez utiliser d'autres types de connexions de fournisseur d'accès Internet, telles qu'une ligne louée ou une connexion Ethernet point à point.

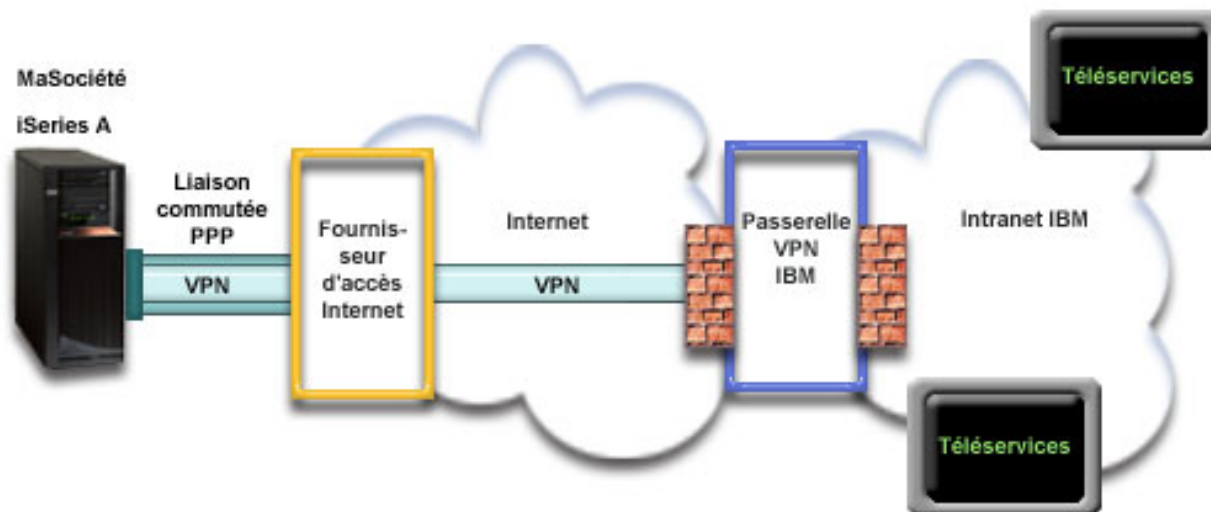
Objectifs

Dans ce scénario, le client souhaite s'assurer qu'IBM peut prendre en charge le système MaSociété sur le réseau via une connexion de fournisseur d'accès Internet point à point. Les objectifs de ce scénario sont les suivants :

- Créer une connexion sécurisée entre MaSociété et les Téléservices via la connexion de fournisseur d'accès Internet point à point de MaSociété
- Automatiser le service d'assistance à la clientèle via les Téléservices et différents services
- Permettre aux Téléservices de créer un inventaire matériel et logiciel du système iSeries de MaSociété.
- Permettre aux Téléservices d'envoyer des correctifs et des mises à jour de logiciel à MaSociété via le réseau

Détails

Le schéma suivant illustre la connexion du serveur iSeries de MaSociété aux Téléservices via une connexion de fournisseur d'accès Internet.



Configuration de la connexion universelle

- iSeries Navigator lance l'assistant de connexion universelle pour configurer la connexion. Cette opération n'a besoin d'être exécutée qu'une seule fois sauf si des informations doivent être mises à jour.

Utilisation de la connexion universelle

Lorsqu'une application de service souhaite utiliser la connexion universelle pour communiquer avec IBM, les événements suivants ont lieu :

- Si la connexion à votre fournisseur d'accès Internet n'est pas active, le profil indiqué est lancé pour permettre des connexions à Internet.
- Un réseau privé virtuel (VPN) est établi via votre connexion Internet existante vers une passerelle de réseau privé virtuel chez IBM si l'application de service ne prend pas en charge la sécurité.
- L'application de service communique avec les serveurs IBM appropriés pour exécuter le service demandé.

Conditions requises et préalables

Les conditions requises pour pouvoir activer les Téléservices via une connexion de fournisseur d'accès Internet point à point sont les suivantes :

- Vérifiez qu'iSeries Access for Windows et iSeries Navigator sont installés sur votre ordinateur personnel (voir iSeries Access for Windows - Installation et configuration).
- Assurez-vous d'avoir installé tous les Service Packs les plus récents pour iSeries Navigator. Les scénarios présentés utilisent la version 5.4 du logiciel.
- Vérifiez que TCP/IP est actif. Vous pouvez démarrer TCP/IP via la commande STRTCP (Démarrer TCP/IP).
- Pour pouvoir configurer la connexion à partir de l'assistant de connexion universelle, vous devez disposer du droit de responsable de la sécurité (*SECOFR) associé aux droits spéciaux *ALLOBJ, *IOSYSCFG et *SECADM dans votre profil utilisateur i5/OS et du droit *USE sur WRKCNTINF.
- Vous devez installer les utilitaires de connectivité TCP/IP (5722-TC1).
- Vous devez installer Digital Certificate Manager (DCM) (5722-SS1 option 34).
- Assurez-vous que la valeur système QRETSVRSEC a pour valeur 1. Pour cela, utilisez la commande DSPSYSVAL (Afficher une valeur système). Si cette valeur n'est pas fixée à 1, entrez la commande CHGSYSVAL (Modifier une valeur système).

- Si vous utilisez un modem interne tel que le modem 56 Kbps fourni avec la carte 9793, vérifiez que l'attribut de réseau MDMCOUNTRYID est correctement défini. Pour cela, utilisez la commande DSPNETA (Afficher les attributs du réseau). Si cet attribut n'est pas correctement défini, modifiez sa valeur à l'aide de la commande CHGNETA. L'ID utilisateur et le mot de passe du compte peuvent ainsi être enregistrés sur le serveur iSeries.
- Le profil utilisé pour se connecter à votre fournisseur d'accès Internet doit avoir déjà été configuré.
- Vérifiez qu'une route TCP/IP est associée au profil ISP afin qu'elle achemine le trafic de la connexion universelle vers votre fournisseur d'accès Internet. Dans la plupart des cas, la route par défaut fonctionne. Pour des informations supplémentaires sur le réseau virtuel privé (VPN), consultez les rubriques «Détermination des adresses de passerelle VPN IBM», à la page 69 et «Détermination des adresses de destination de services IBM», à la page 69.

Etapes de configuration du système **en cours**

Si la configuration TCP/IP existe déjà et est fonctionnelle, exécutez les étapes suivantes pour configurer la connexion universelle si vous vous connectez aux Téléservices via le serveur local de MaSociété :

1. Complétez le formulaire de planification.
2. Démarrez iSeries Navigator et sélectionnez l'assistant de connexion universelle.
3. Indiquez les informations demandées (service, adresse et pays) dans les boîtes de dialogue de l'assistant de connexion universelle.
4. Sous Connexion à partir du système ou de la partition en cours, sélectionnez l'option Connexion via un fournisseur d'accès Internet comme type de connexion.
5. Sélectionnez un profil de connexion pour votre fournisseur d'accès Internet à partir de la boîte de dialogue Sélection de profil.
6. Indiquez que ce serveur ne fournit pas de connexion aux autres serveurs ou partitions.
7. Pour l'option de proxy, configurez un serveur proxy cible.
8. Passez en revue la fenêtre Récapitulatif afin de vérifier que la configuration répond à vos besoins et cliquez sur Terminer pour enregistrer la configuration.
9. Testez la connexion aux Téléservices à partir de votre serveur.
10. Configurez une configuration de sauvegarde (facultatif).

Détails du scénario : Configuration d'une connexion point à point via un fournisseur d'accès Internet

Une fois que les conditions requises sont réunies, vous pouvez commencer la configuration de la connexion universelle via l'assistant.

Etape 1 : Complétez le formulaire de planification.

Le formulaire de planification suivant illustre le type d'informations dont vous avez besoin pour pouvoir configurer la connexion point à point via le fournisseur d'accès Internet MaSociété. Vous utilisez ces informations lors de l'exécution de l'assistant de connexion universelle.

Formulaire de planification	Réponses
Informations relatives à la maintenance <ul style="list-style-type: none"> • Société • Nom du contact • Numéro de téléphone • Service d'assistance ou numéro de messagerie • Numéro de télécopie • Numéro de fax secondaire 	<ul style="list-style-type: none"> • MaSociété • Jean Dupont • 515-870-9990 • 515-870-9942 • 515-870-5586 • 515-870-5587

Formulaire de planification	Réponses
Adresse de la société <ul style="list-style-type: none"> • Adresse postale • Ville ou localité • Etat ou province • Pays (ou région) • Code postal • Version en langue nationale • Adresse de courrier électronique • Adresse de courrier électronique secondaire • Support pour les PTF (correctifs) 	<ul style="list-style-type: none"> • 94 West Proctor St. • Boone • Iowa • Etats-Unis • 55902 • Anglais (2924) • monnom@société.com • monnom@autresociété.com • Sélection automatique
Emplacement <ul style="list-style-type: none"> • Pays (ou région) • Etat 	<ul style="list-style-type: none"> • Etats-Unis • Iowa
Méthode de connexion	Via le serveur local iSeries
Type de connexion	Via un profil de connexion de ligne commutée existant pour le fournisseur d'accès Internet MaSociété.
Profil de connexion	DIALPROF

Si vous préférez utiliser les commandes CL pour créer la configuration, utilisez les commandes Modifier point de contact (CHGCNTINF) et Création d'une configuration de maintenance (CRTSRVCFG).

Etape 2 : Démarrez iSeries Navigator et sélectionnez l'assistant de connexion universelle.

Pour démarrer l'assistant de connexion universelle et commencer à établir votre connexion, procédez comme suit :

1. Ouvrez le logiciel iSeries Navigator.
2. Sélectionnez sous le dossier Mes connexions le serveur à configurer pour les Téléservices.
3. Développez l'arborescence de **Réseau**.
4. Développez l'arborescence de **Services d'accès distant**.
5. Cliquez à l'aide du bouton droit de la souris sur **Profils de connexion de l'expéditeur**.
6. Sélectionnez **Configuration de connexion universelle** pour démarrer l'assistant de connexion universelle. La boîte de dialogue de bienvenue apparaît.

Remarque : Une barre de progression indique qu'iSeries Navigator charge l'assistant de connexion universelle. En cas d'incident pendant l'exécution de l'assistant, consultez la section «Identification et résolution des incidents liés à l'assistant de connexion universelle», à la page 70 pour trouver une solution. Relancez l'assistant après avoir résolu l'incident.

Etape 3 : Indiquez les informations demandées (service, adresse et pays) dans les boîtes de dialogue de l'assistant.

Pour entrer des informations sur votre entreprise et vos connexions, procédez comme suit :

1. Dans la boîte de dialogue Choix d'une configuration, sélectionnez **Configuration de connexion principale** ou **Configuration de connexion de secours**. La configuration par défaut est la configuration de connexion principale. Cochez la case **Affichage et modification des informations concernant le contact** et cliquez sur **Suivant**.
2. Dans la boîte de dialogue Informations de maintenance, entrez les informations suivantes sur MaSociété et cliquez sur **Suivant** :
 - Société – MaSociété
 - Nom du contact – Jean Dupont

- Numéro de téléphone – 515-870-9990
- Service d'assistance ou numéro de messagerie — 515-870-9999
- Numéro de fax — 515-870-5586
- Numéro de fax secondaire — 515-870-9942

Si ces informations existent sur votre serveur, les données relatives à votre société s'affichent dans les zones correspondantes. Par exemple, si MaSociété a déjà créé une configuration, l'assistant extrait les données de la configuration existante.

3. Dans la boîte de dialogue Adresse de la société, entrez l'adresse de MaSociété et cliquez sur **Suivant**.
 - Adresse postale – 94 West Proctor St.
 - Ville ou localité – Boone
 - Etat ou province – Iowa
 - Pays ou région – Etats-Unis
 - Code postal – 55902
 - Version en langue nationale – English (2924)
 - Adresse de courrier électronique – monnom@société.com
 - Adresse de courrier électronique secondaire – monnom@autresociété.com
 - Support pour les PTF – Sélection automatique
4. Dans la boîte de dialogue Emplacement, sélectionnez le pays (ou la région) et l'état ou la province dans lesquels est situé votre serveur iSeries puis cliquez sur **Suivant**.
 - Pays ou région – Etats-Unis
 - Etat – Iowa

Etape 4 : Sous Connexion à partir du système ou de la partition en cours, sélectionnez l'option Connexion via un fournisseur d'accès Internet comme type de connexion.

Remarque : Il existe une case à cocher **Configuration supplémentaire d'une connexion proxy**. Si votre société possède un proxy HTTP ou que vous avez configuré un proxy de maintenance et de support sur un autre système ou une autre partition et que vous souhaitez utiliser les applications de connexion universelle prenant en charge la connexion via un proxy, cochez cette case. Si cette case est cochée, une étape 7 apparaîtra.

Etape 5 : Sélectionnez un profil de connexion pour votre fournisseur d'accès Internet à partir de la boîte de dialogue Sélection de profil.

Sélectionnez le profil de connexion DIALFPROF (un type de connexion de ligne commutée).

Etape 6 : Indiquez que ce serveur ne fournit pas de connexion aux autres serveurs ou partitions.

Cliquez sur **Non** pour indiquer que ce serveur possède une connexion directe avec les Téléservices mais qu'il ne fournit pas de connexion aux autres serveurs ou partitions.

Etape 7 : Pour l'option de proxy, configurez un serveur proxy cible.

Remarque : Cet écran apparaît uniquement si vous avez choisi l'option de serveur proxy au cours de l'étape 4.

Pour configurer un serveur proxy cible

1. Essayez d'abord d'établir une connexion au serveur proxy

- a. Choisissez cette option si vous souhaitez que le proxy ait la priorité sur la configuration de ce scénario.
- b. Si nécessaire, cochez la case **Le serveur proxy cible requiert une authentification standard HTTP** et remplissez les champs **Nom d'utilisateur** et **Mot de passe**.
- c. Cliquez sur **Suivant** et passez à l'étape suivante.

2. Essayez d'établir une connexion si la configuration préalablement définie échoue

- | a. Choisissez cette option si le proxy doit uniquement être utilisé lorsque la configuration de ce scénario échoue.
- | b. Complétez le champ **Adresse IP ou nom d'hôte du proxy**.
- | c. Complétez le champ **Port du serveur proxy**.
- | d. Si nécessaire, cochez la case **Le serveur proxy cible requiert une authentification standard HTTP** et remplissez les champs **Nom d'utilisateur** et **Mot de passe**.
- | e. Cliquez sur **Suivant** et passez à l'étape suivante.

| **Etape 8 : Passez en revue la fenêtre Récapitulatif afin de vérifier que la configuration répond à vos besoins et cliquez sur Terminer pour enregistrer la configuration.**

| Pour terminer la configuration du serveur et la sauvegarder, procédez comme suit :

- | 1. Consultez le récapitulatif de la configuration. Cliquez sur **Précédent** si vous devez modifier une valeur dans l'une des boîtes de dialogue de l'assistant.
- | 2. Lorsque la configuration est correcte, cliquez sur **Terminer** pour sauvegarder la configuration. Une barre de progression vous indique que l'assistant est en train de sauvegarder la configuration.

| **Etape 9 : Testez la connexion aux Téléservices à partir de votre serveur.**

| Pour tester la configuration, procédez comme suit :

- | 1. Cliquez sur **Oui** lorsque l'assistant vous invite à tester la configuration. La boîte de dialogue Vérification de la connexion universelle s'affiche.
- | 2. Notez les erreurs éventuelles pendant que l'assistant affiche la progression de la vérification.
- | 3. Cliquez sur **OK** lorsque l'assistant indique que la vérification est terminée.
- | 4. Si l'assistant détecte des erreurs, redémarrez l'assistant de connexion universelle, apportez les corrections nécessaires, sauvegardez, puis testez à nouveau la configuration corrigée.

| **Etape 10 : Configurez une configuration de sauvegarde (facultatif).**

| Si une méthode de connexion supplémentaire est disponible, nous vous recommandons de réexécuter l'assistant afin de configurer une sauvegarde. Cette sauvegarde sera utilisée automatiquement en cas d'échec de la connexion principale.

Scénario : Configuration d'une connexion commutée point à point à partir d'un serveur fournissant une connectivité à d'autres systèmes via un fournisseur d'accès Internet

Situation

Supposons que vous êtes responsable de la gestion d'un serveur iSeries pour MaSociété, une petite entreprise de fabrication située à Boone, dans l'Iowa. Dans le cadre de cette gestion, vous devez établir une connexion entre les Téléservices et le serveur iSeries de MaSociété.

Comme MaSociété dispose d'une connexion de réseau relié à Internet, vous pouvez créer une connexion à partir de votre serveur iSeries via votre modem vers une liaison commutée point à point (PPP). Comme votre réseau comprend trois autres serveurs iSeries, vous souhaitez sans doute fournir une connectivité vers les Téléservices via la connexion universelle du serveur principal de MaSociété.

Solution

- | Créez une connexion universelle vers IBM par le biais d'une liaison commutée point à point via Internet.
- | Dans ce cas, vous devez établir une connexion à l'aide du gestionnaire de connexions sur votre serveur iSeries local via une connexion point à point Internet vers les Téléservices. Votre serveur principal peut

| alors tenir lieu de point de connexion pour les trois autres serveurs de MaSociété qui ont besoin de se
| connecter aux Téléservices (voir Configuration d'une connexion multiple entre noeuds via un serveur
| éloigné). Dans le cadre de l'installation et de la configuration de votre serveur, l'assistant va créer un
| profil de réponse L2TP. Vous pouvez également sélectionner un profil de réponse L2TP existant. Pour
| plus d'informations sur les profils de réponse L2TP, consultez la rubrique L2TP (ligne virtuelle). En outre,
| l'assistant procédera à la configuration du proxy de maintenance et de support.

Avantages

Ce scénario offre les avantages suivants :

- MaSociété n'a pas besoin d'investir dans du matériel ou du logiciel supplémentaire pour bénéficier des Téléservices. Vous pouvez configurer cette connexion à l'aide de l'assistant de connexion universelle ou des commandes CL.
- Les trois autres serveurs de MaSociété peuvent se connecter à distance aux Téléservices via un serveur unique. MaSociété n'a donc besoin que d'un seul modem et d'une connexion de fournisseur d'accès Internet commutée et non d'un modem distinct pour chaque système ou partition.

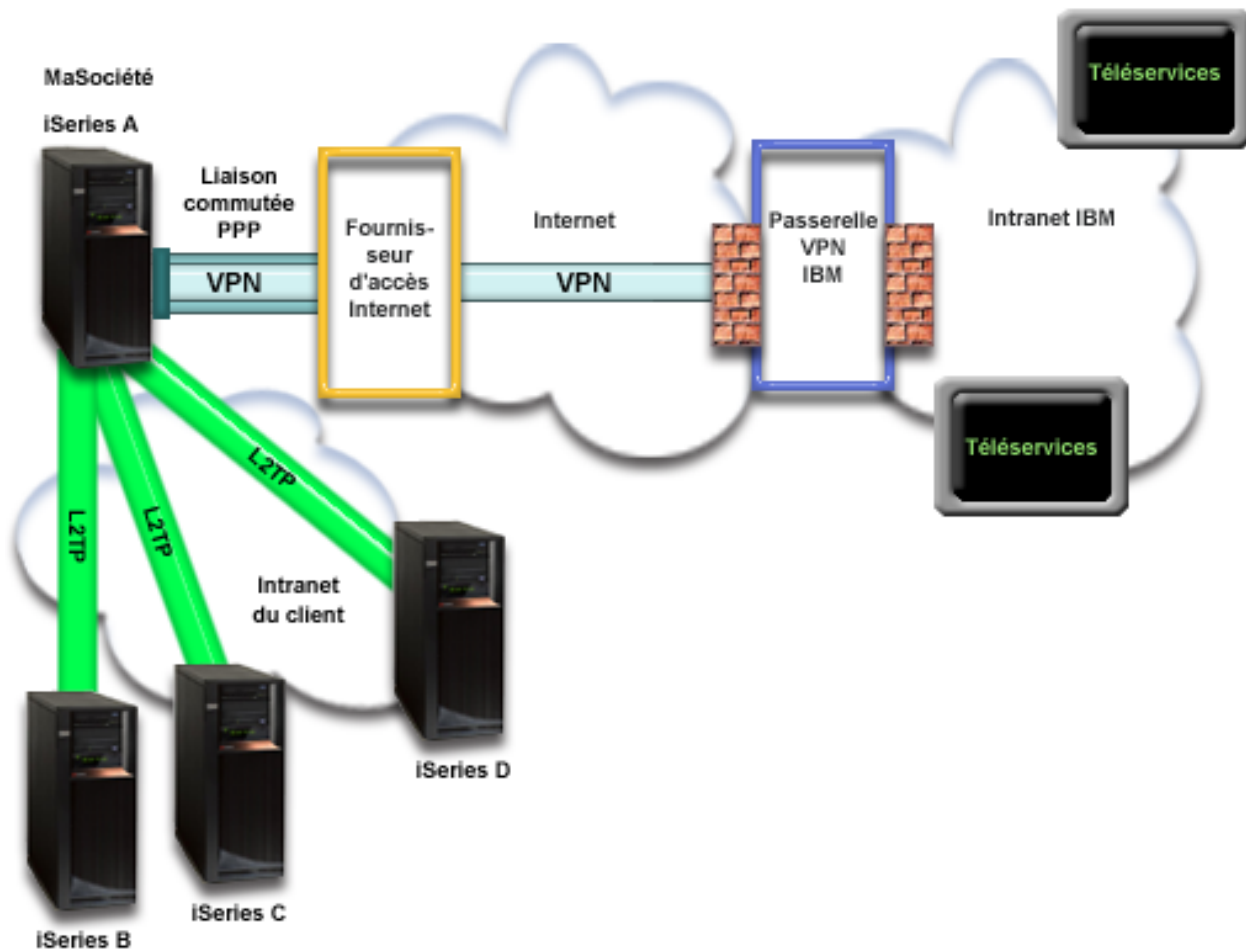
Objectifs

Dans ce scénario, le client souhaite s'assurer qu'IBM peut prendre en charge le système MaSociété sur le réseau via la connexion de fournisseur d'accès Internet de MaSociété. Les objectifs de ce scénario sont les suivants :

- Créer une connexion commutée point à point sécurisée entre les quatre serveurs de MaSociété et les Téléservices via le fournisseur d'accès Internet de MaSociété
- Automatiser le service d'assistance à la clientèle via les Téléservices et différents services
- Permettre aux Téléservices de créer un inventaire matériel et logiciel du système iSeries de MaSociété.
- Permettre aux Téléservices d'envoyer des correctifs et des mises à jour de logiciel à MaSociété via le réseau

Détails

Le schéma suivant illustre la connexion du serveur iSeries de MaSociété aux Téléservices via une connexion de fournisseur d'accès Internet point à point.



Configuration de la connexion universelle

- iSeries Navigator lance l'assistant de connexion universelle pour configurer la connexion. Cette opération n'a besoin d'être exécutée qu'une seule fois sauf si des informations doivent être mises à jour.

Utilisation de la connexion universelle

Lorsqu'une application de service souhaite utiliser la connexion universelle pour communiquer avec IBM, les événements suivants ont lieu :

- Si l'iSeries A doit se connecter et que la connexion à votre fournisseur d'accès Internet n'est pas active, le profil indiqué est lancé pour permettre des connexions à Internet. Si l'application de service sous iSeries B, C ou D ne prend pas en charge la sécurité, un tunnel L2TP est établi vers l'iSeries A. La connexion via un fournisseur d'accès Internet doit être active. Si l'application de service peut utiliser un proxy, une connexion HTTP ou HTTPS sera établie via un proxy de maintenance ou de support.
- Un réseau privé virtuel (VPN) est établi via votre connexion Internet existante vers une passerelle de réseau privé virtuel chez IBM si l'application de service ne prend pas en charge la sécurité.
- L'application de service communique avec les serveurs IBM appropriés pour exécuter le service demandé.

Conditions requises et préalables

Les conditions requises pour pouvoir activer les Téléservices via une connexion de fournisseur d'accès Internet point à point sont les suivantes :

- Vérifiez qu'iSeries Access for Windows et iSeries Navigator sont installés sur votre ordinateur personnel (voir iSeries Access for Windows - Installation et configuration).
- Assurez-vous d'avoir installé tous les Service Packs les plus récents pour iSeries Navigator. Les scénarios présentés utilisent la version 5.4 du logiciel.
- Vérifiez que TCP/IP est actif. Vous pouvez démarrer TCP/IP via la commande STRTCP (Démarrer TCP/IP).
- Pour pouvoir configurer la connexion à partir de l'assistant de connexion universelle, vous devez disposer du droit de responsable de la sécurité (*SECOFR) associé aux droits spéciaux *ALLOBJ, *IOSYSCFG et *SECADM dans votre profil utilisateur i5/OS et du droit *USE sur WRKCNTINF.
- Vous devez installer les utilitaires de connectivité TCP/IP (5722-TC1).
- Pour que le réseau privé virtuel (VPN) et la couche SSL fonctionnent, vous devez installer Digital Certificate Manager (DCM) (5722-SS1 option 34).
- Assurez-vous que la valeur système QRETSVRSEC a pour valeur 1. Pour cela, utilisez la commande DSPSYSVAL (Afficher une valeur système). Si cette valeur n'est pas fixée à 1, entrez la commande CHGSYSVAL (Modifier une valeur système). L'ID utilisateur et le mot de passe du compte peuvent ainsi être enregistrés sur le serveur iSeries.
- Si vous utilisez un modem interne tel que le modem 56 Kbps fourni avec la carte 9793, vérifiez que l'attribut de réseau MDMCOUNTRYID est correctement défini. Pour cela, utilisez la commande DSPNETA (Afficher les attributs du réseau). Si cet attribut n'est pas correctement défini, modifiez sa valeur à l'aide de la commande CHGNETA (Modifier les attributs du réseau).
- Si vous vous connectez pour d'autres serveurs, assurez-vous que la connexion au fournisseur d'accès Internet est active avant de vous connecter aux Téléservices.

Etapes de configuration du système **en cours**

Si la configuration TCP/IP existe déjà et est fonctionnelle, exécutez les étapes suivantes pour configurer la connexion universelle si vous vous connectez aux Téléservices IBM ou que le serveur local tient lieu de point de connexion pour les trois autres serveurs de MaSociété :

1. Complétez le formulaire de planification.
2. Démarrez iSeries Navigator et sélectionnez l'assistant de connexion universelle.
3. Indiquez les informations demandées (service, adresse et pays) dans les boîtes de dialogue de l'assistant de connexion universelle.
4. Sous Connexion à partir du système ou de la partition en cours, sélectionnez le type de connexion Fournisseur d'accès Internet.
5. Sélectionnez un profil de connexion pour votre fournisseur d'accès Internet à partir de la boîte de dialogue Sélection de profil.
6. Précisez que vous souhaitez que ce serveur iSeries fonctionne en tant que point de connexion par le biais duquel les autres serveurs ou partitions pourront se connecter aux Téléservices.
7. Sélectionnez une interface que les autres serveurs utiliseront lors de leur connexion aux Téléservices.
8. Créez ou sélectionnez un profil de réponse L2TP. Ces profils sont nécessaires pour fournir la connectivité aux autres systèmes qui se connectent aux Téléservices via votre serveur.
9. Configurez un serveur proxy de maintenance et de support.
10. Passez en revue la fenêtre Récapitulatif afin de vérifier que la configuration répond à vos besoins et cliquez sur **Terminer** pour enregistrer la configuration.
11. Lorsque vous y êtes invité, testez la connexion aux Téléservices à partir de votre serveur.
12. Configurez une configuration de sauvegarde.

Scénario : Configuration d'une connexion commutée point à point à partir d'un serveur fournissant une connectivité à d'autres systèmes via un fournisseur d'accès Internet

Une fois que les conditions requises sont réunies, vous pouvez commencer la configuration de la connexion universelle via l'assistant.

Etape 1 : Complétez le formulaire de planification.

Le formulaire de planification suivant illustre le type d'informations dont vous avez besoin pour pouvoir configurer la connexion point à point via un fournisseur d'accès Internet. Vous utilisez ces informations lors de l'exécution de l'assistant de connexion universelle.

Formulaire de planification	Réponses
Informations relatives à la maintenance <ul style="list-style-type: none"> • Société • Nom du contact • Numéro de téléphone • Service d'assistance ou numéro de messagerie • Numéro de télécopie • Numéro de fax secondaire 	<ul style="list-style-type: none"> • MaSociété • Jean Dupont • 515-870-9990 • 515-870-9942 • 515-870-5586 • 515-870-5587
Adresse de la société <ul style="list-style-type: none"> • Adresse postale • Ville ou localité • Etat ou province • Pays (ou région) • Code postal • Version en langue nationale • Adresse de courrier électronique • Adresse de courrier électronique secondaire • Support pour les PTF (correctifs) 	<ul style="list-style-type: none"> • 94 West Proctor St. • Boone • Iowa • Etats-Unis • 55902 • Anglais (2924) • monnom@société.com • monnom@autresociété.com • Sélection automatique
Emplacement <ul style="list-style-type: none"> • Pays (ou région) • Etat 	<ul style="list-style-type: none"> • Etats-Unis • Iowa
Méthode de connexion	Via le serveur iSeries en cours
Type de connexion	Via un profil de connexion de ligne commutée existant pour le fournisseur d'accès Internet MaSociété.
Profil de connexion	DIALPROF
Description de l'interface pour les autres systèmes à utiliser comme point de connexion	Tout type d'interface
Nom du profil de réponse L2TP	QL2TP00

Si vous préférez utiliser les commandes CL pour créer la configuration, utilisez les commandes Modifier point de contact (CHGCNTINF) et Création d'une configuration de maintenance (CRTSRVCFG).

Etape 2 : Démarrez iSeries Navigator et sélectionnez l'assistant de connexion universelle.

Pour démarrer l'assistant de connexion universelle et commencer à établir votre connexion, procédez comme suit :

1. Ouvrez le logiciel iSeries Navigator.
2. Sélectionnez sous le dossier Mes connexions le serveur à configurer pour les Téléservices.
3. Développez l'arborescence de **Réseau**.
4. Développez l'arborescence de **Services d'accès distant**.
5. Cliquez à l'aide du bouton droit de la souris sur **Profils de connexion de l'expéditeur**.
6. Sélectionnez **Configuration de connexion universelle** pour démarrer l'assistant de connexion universelle. La boîte de dialogue de bienvenue apparaît.

Remarque : Une barre de progression indique qu'iSeries Navigator charge l'assistant de connexion universelle. En cas d'incident pendant l'exécution de l'assistant, consultez la section «Identification et résolution des incidents liés à l'assistant de connexion universelle», à la page 70 pour trouver une solution. Relancez l'assistant après avoir résolu l'incident.

Etape 3 : Indiquez les informations demandées (service, adresse et pays) dans les boîtes de dialogue de l'assistant.

Pour entrer des informations sur votre entreprise et vos connexions, procédez comme suit :

1. Dans la boîte de dialogue Choix d'une configuration, sélectionnez **Configuration de connexion principale** ou **Configuration de connexion de secours**. La configuration par défaut est la configuration de connexion principale. Cochez la case **Affichage et modification des informations concernant le contact** et cliquez sur **Suivant**.
2. Dans la boîte de dialogue Informations de maintenance, entrez les informations suivantes sur MaSociété et cliquez sur **Suivant** :
 - Société – MaSociété
 - Nom du contact – Jean Dupont
 - Numéro de téléphone – 515-870-9990
 - Service d'assistance ou numéro de messagerie — 515-870-9999
 - Numéro de fax — 515-870-5586
 - Numéro de fax secondaire — 515-870-9942

Si ces informations existent sur votre serveur, les données relatives à votre société s'affichent dans les zones correspondantes. Par exemple, si MaSociété a déjà créé une configuration, l'assistant extrait les données de la configuration existante.

3. Dans la boîte de dialogue Adresse de la société, entrez l'adresse de MaSociété et cliquez sur **Suivant**.
 - Adresse postale – 94 West Proctor St.
 - Ville ou localité – Boone
 - Etat ou province – Iowa
 - Pays ou région – Etats-Unis
 - Code postal – 55902
 - Version en langue nationale – English (2924)
 - Adresse de courrier électronique – monnom@société.com
 - Adresse de courrier électronique secondaire – monnom@autresociété.com
 - Support pour les PTF – Sélection automatique
4. Dans la boîte de dialogue Emplacement, sélectionnez le pays (ou la région) et l'état ou la province dans lesquels est situé votre serveur iSeries puis cliquez sur **Suivant**.
 - Pays ou région – Etats-Unis
 - Etat – Iowa

Etape 4 : Sous Connexion à partir du système ou de la partition en cours, sélectionnez le type de connexion Fournisseur d'accès Internet.

Sélectionnez le type de connexion **Connexion via un fournisseur d'accès Internet**.

Etape 5 : Sélectionnez un profil de connexion pour votre fournisseur d'accès Internet à partir de la boîte de dialogue Sélection de profil.

Sélectionnez le profil de connexion DIALPROF (un type de connexion de ligne commutée).

Etape 6 : Précisez que vous souhaitez que ce serveur iSeries fonctionne en tant que point de connexion par le biais duquel les autres serveurs ou partitions pourront se connecter aux Téléservices.

Etape 7 : Sélectionnez une interface que les autres serveurs utiliseront lors de leur connexion aux Téléservices.

Sélectionnez les interfaces utilisées par les serveurs MaSociété pour se connecter à IBM. Sélectionnez l'une des options suivantes :

- Cliquez sur **Tout type d'interface** pour que la connexion universelle puisse accepter des connexions provenant de toutes les interfaces TCP/IP.

- Cliquez sur **Sélection des interfaces** afin de sélectionner des interfaces pour écouter les demandes de connexion. La boîte à liste devient active. Sélectionnez toutes les interfaces appropriées. L'assistant crée automatiquement un profil de réponse L2TP pour chaque interface non associée à un profil de réponse. Si des profils de réponse L2TP sont associés à une interface, l'assistant vous invite à sélectionner le profil de réponse à associer en particulier à cette interface.
- Vous pouvez sélectionner plusieurs interfaces avec la touche CTRL.

Remarque : En outre, l'assistant configure le serveur proxy HTTP de maintenance et de support pour démarrer en même temps que le TCP et pour écouter des requêtes de connexion sur l'interface sélectionnée.

Dans ce cas, MaSociété sélectionne l'option Tout type d'interface afin que les connexions soient acceptées à partir de toute interface TCP/IP active.

Etape 8 : Créez ou sélectionnez un profil de réponse L2TP.

1. Sélectionnez un profil de réponse L2TP pour chacune des interfaces sélectionnées. Sélectionnez l'une des options suivantes :
 - Cliquez sur **Créer un nouveau profil QL2TP $_{nn}$** où nn représente un chiffre compris entre 0 et 99. Avec cette option, l'assistant crée, nomme et numérote de façon consécutive le nouveau profil L2TP.
 - Cliquez sur **Sélectionner un profil existant** afin de choisir un profil L2TP spécifique pour l'interface associée.Dans notre cas, MaSociété laisse l'assistant de connexion universelle créer un profil L2TP.
2. Vérifiez que la case **Démarrer le profil de réponse L2TP en même temps que TCP/IP** est cochée. En effet, MaSociété souhaite démarrer ce profil en même temps que TCP/IP.

Remarque : En démarrant le profil de réponse L2TP sélectionné avec TCP/IP, tous les autres profils L2TP pour cette interface seront modifiés pour ne pas démarrer avec TCP/IP.

Si vous indiquez que vous ne souhaitez pas démarrer les profils de réponse L2TP sélectionnés en même temps que TCP/IP, vous devez démarrer manuellement le profil de réponse L2TP avant d'utiliser la connexion aux systèmes.

Etape 9 : Configurez un serveur proxy de maintenance et de support.

Pour configurer le serveur proxy de maintenance et de support :

1. Complétez le champ **Port serveur**.
2. Si vous le souhaitez, cochez la case **Requiert une authentification standard HTTP** et complétez les champs **Nom d'utilisateur** et **Mot de passe**. L'authentification est facultative. Si vous spécifiez ces champs, toutes les autres partitions ou tous les autres systèmes utilisant ce serveur proxy doivent entrer les données d'identification de sécurité.
3. Cliquez sur **Suivant** et passez à l'étape suivante.

Etape 10 : Passez en revue la fenêtre Récapitulatif afin de vérifier que la configuration répond à vos besoins et cliquez sur Terminer pour enregistrer la configuration.

Pour terminer la configuration du serveur et la sauvegarder, procédez comme suit :

1. Consultez le récapitulatif de la configuration. Cliquez sur **Précédent** si vous devez modifier une valeur dans l'une des boîtes de dialogue de l'assistant.
2. Lorsque la configuration est correcte, cliquez sur **Terminer** pour sauvegarder la configuration. Une barre de progression vous indique que l'assistant est en train de sauvegarder la configuration.

Etape 11 : Testez la connexion aux Téléservices à partir de votre serveur.

- | Pour tester la configuration, procédez comme suit :
- | 1. Cliquez sur **Oui** lorsque l'assistant vous invite à tester la configuration. La boîte de dialogue Vérification de la connexion universelle s'affiche.
- | 2. Notez les erreurs éventuelles pendant que l'assistant affiche la progression de la vérification.
- | 3. Cliquez sur **OK** lorsque l'assistant indique que la vérification est terminée.
- | 4. Si l'assistant détecte des erreurs, redémarrez l'assistant de connexion universelle, apportez les corrections nécessaires, sauvegardez, puis testez à nouveau la configuration corrigée.

| **Etape 12 : Configurez une configuration de sauvegarde.**

- | Si une méthode de connexion supplémentaire est disponible, nous vous recommandons de réexécuter l'assistant afin de configurer une sauvegarde. Cette sauvegarde sera utilisée automatiquement en cas d'échec de la connexion principale.

Scénario : Configuration d'une connexion multiple entre noeuds via un serveur distant

Situation

Supposons que vous êtes responsable de la gestion d'un serveur iSeries pour MaSociété, une moyenne entreprise de fabrication située à Boone, dans l'Iowa. Dans le cadre de cette gestion, vous devez établir une connexion entre les Téléservices et le serveur iSeries de MaSociété. MaSociété dispose d'un serveur iSeries sur un réseau privé qui accède à Internet via une passerelle à noeuds multiples VPN. La passerelle à noeuds multiples peut être un iSeries ou un routeur prenant en charge les connexions multiples entre noeuds L2TP (tunnels chaînés). Dans ce cas, vous créez une connexion depuis votre serveur iSeries via une connexion multiple entre noeuds. Comme vous n'avez pas besoin de fournir des connexions pour d'autres systèmes, vous n'avez pas besoin non plus de fournir des connexions pour d'autres serveurs ou partitions.

Remarque : Actuellement, la console HMC ne peut pas prendre en charge la passerelle à noeuds multiples.

Solution

Créez une connexion universelle vers IBM via la connexion multiple entre noeuds. Dans ce cas, vous devez établir une connexion entre deux tunnels de type VPN depuis un serveur éloigné vers les Téléservices.

Avantages

Ce scénario offre les avantages suivants :

- MaSociété peut établir une connexion à partir de son système iSeries sur un réseau privé via un autre iSeries ou routeur disposant d'une connectivité directe vers Internet.
- La connexion multiple entre noeuds fournit à MaSociété une méthode simple pour accéder aux Téléservices qui permettent de faciliter la résolution des incidents liés au serveur, le suivi du matériel et du logiciel système actuellement utilisés ou la réception de mises à jour et de correctifs de logiciel.
- Une connexion multiple entre noeuds offre un haut niveau de sécurité entre votre système iSeries et les Téléservices car elle protège votre système contre tout accès depuis Internet.
- Cette solution permet de bénéficier d'un accès haut débit aux Téléservices.

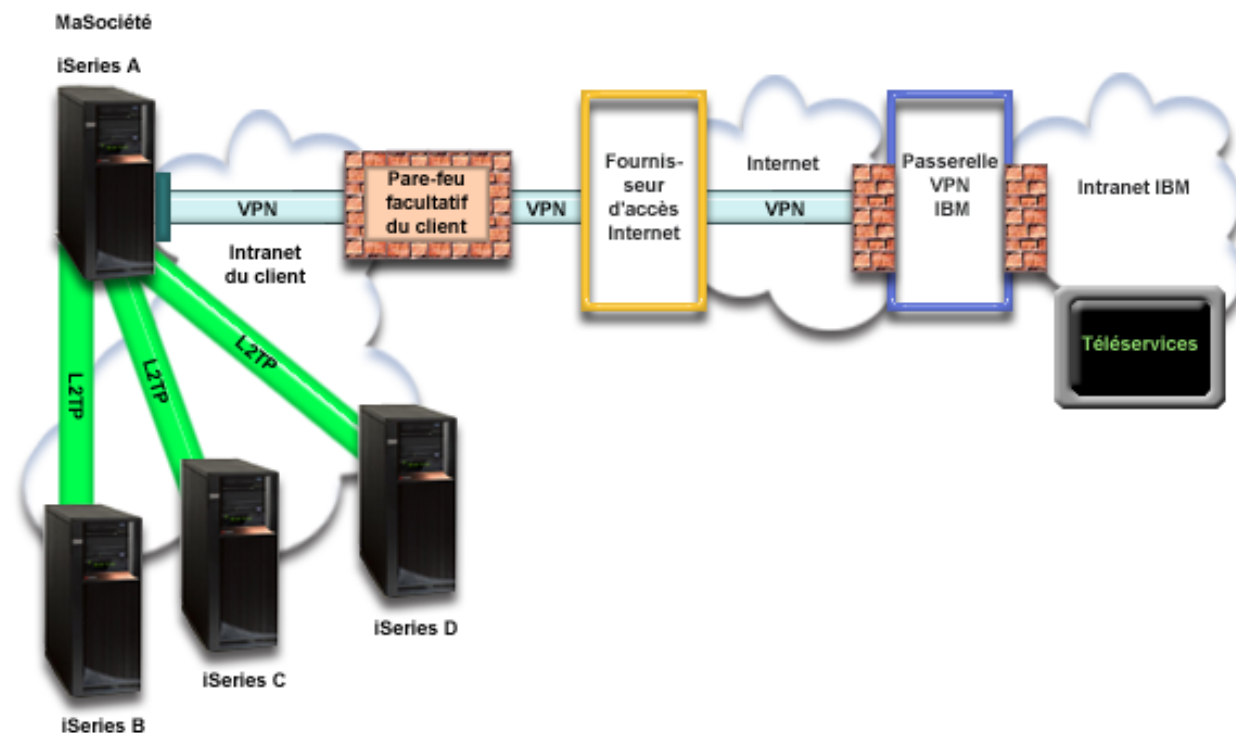
Objectifs

Dans ce scénario, le client souhaite s'assurer qu'IBM peut prendre en charge le système MaSociété par le biais d'une connexion multiple entre noeuds via Internet. Les objectifs de ce scénario sont les suivants :

- Créer une connexion multiple entre noeuds sécurisée entre MaSociété et les Téléservices via Internet
- Automatiser le service d'assistance à la clientèle via les Téléservices et différents services
- Permettre aux Téléservices de créer un inventaire matériel et logiciel du système iSeries de MaSociété.
- Permettre aux Téléservices d'envoyer des correctifs et des mises à jour de logiciel à MaSociété via le réseau

Détails

Le schéma suivant illustre la connexion du serveur iSeries de MaSociété aux Téléservices via une passerelle à noeuds multiples VPN.



Configuration de la connexion universelle

- iSeries Navigator lance l'assistant de connexion universelle pour configurer la connexion. Cette opération n'a besoin d'être exécutée qu'une seule fois sauf si des informations doivent être mises à jour.

Utilisation de la connexion universelle

Lorsqu'une application de service souhaite utiliser la connexion universelle pour communiquer avec IBM, les événements suivants ont lieu :

- Un tunnel L2TP est établi vers la passerelle à noeuds multiples VPN.
- Comme la demande de connexion concerne un service IBM, un réseau privé virtuel (VPN) est établi via votre connexion Internet existante vers une passerelle VPN chez IBM.
- Le tunnel L2TP est chaîné à la connexion VPN.
- L'application de service communique avec les serveurs IBM appropriés pour exécuter le service demandé.

Conditions requises et préalables

Les conditions requises pour pouvoir activer les Téléservices via une connexion multiple entre noeuds distante sont les suivantes :

- Le serveur iSeries doit disposer d'une connexion IP à la passerelle multiple entre noeuds VPN.
- Vérifiez qu'iSeries Access for Windows et iSeries Navigator sont installés sur votre ordinateur personnel (voir iSeries Access for Windows - Installation et configuration).
- Assurez-vous d'avoir installé tous les Service Packs les plus récents pour iSeries Navigator. Les scénarios présentés utilisent la version 5.4 du logiciel.
- Vérifiez que TCP/IP est actif. Vous pouvez démarrer TCP/IP via la commande STRTCP (Démarrer TCP/IP).
- Pour pouvoir configurer la connexion à partir de l'assistant de connexion universelle, vous devez disposer du droit de responsable de la sécurité (*SECOFR) associé aux droits spéciaux *ALLOBJ, *IOSYSCFG et *SECADM dans votre profil utilisateur i5/OS et du droit *USE sur WRKCNTINF.
- Vous devez installer les utilitaires de connectivité TCP/IP (5722-TC1).
- Vous devez installer Digital Certificate Manager (DCM) (5722-SS1 option 34).
- Assurez-vous que la valeur système QRETSVRSEC a pour valeur 1. Pour cela, utilisez la commande DSPSYSVAL (Afficher une valeur système). Si cette valeur n'est pas fixée à 1, entrez la commande CHGSYSVAL (Modifier une valeur système).
- Vérifiez que la passerelle à noeuds multiples VPN a été configurée pour permettre des connexions vers IBM. Si vous utilisez un iSeries comme passerelle à noeuds multiples VPN, voir Configuration d'une connexion directe à Internet à partir d'un serveur qui fournit la connectivité pour d'autres systèmes ou partitions. Pour les autres options, voir «Détermination des adresses de passerelle VPN IBM», à la page 69.

Etapes de configuration du système ou de la partition en cours

Pour configurer la connexion universelle si vous vous connectez aux Téléservices via une passerelle à noeuds multiples VPN et si la configuration TCP/IP existe déjà et est fonctionnelle, procédez comme suit :

1. Complétez le formulaire de planification.
2. Démarrez iSeries Navigator et sélectionnez l'assistant de connexion universelle.
3. Indiquez les informations demandées (service, adresse et pays) dans les boîtes de dialogue de l'assistant de connexion universelle.
4. Sous Connexion via un autre système ou une autre partition, sélectionnez l'option Connexion VPN multiple entre noeuds à Internet.
5. Indiquez une adresse de passerelle VPN ou un nom d'hôte qui permettra d'établir la connexion multiple entre noeuds VPN à IBM.
6. Pour l'option de proxy, configurez un serveur proxy cible.
7. Indiquez que ce serveur ne fournit pas de connexion aux autres serveurs ou partitions.
8. Passez en revue la fenêtre Récapitulatif afin de vérifier que la configuration répond à vos besoins et cliquez sur **Terminer** pour enregistrer la configuration.
9. Lorsque vous y êtes invité, testez la connexion aux Téléservices à partir de votre serveur.
10. Configurez une configuration de sauvegarde.

Détails du scénario : Configuration d'une connexion multiple entre noeuds via un serveur distant

Une fois que les conditions requises sont réunies, vous pouvez commencer la configuration de la connexion universelle via l'assistant.

Etape 1 : Complétez le formulaire de planification.

Le formulaire de planification suivant illustre le type d'informations dont vous avez besoin pour pouvoir configurer la connexion multiple entre noeuds éloignée aux Téléservices. Vous utilisez ces informations lors de l'exécution de l'assistant de connexion universelle.

Formulaire de planification	Réponses
Informations relatives à la maintenance <ul style="list-style-type: none"> • Société • Nom du contact • Numéro de téléphone • Service d'assistance ou numéro de messagerie • Numéro de télécopie • Numéro de fax secondaire 	<ul style="list-style-type: none"> • MaSociété • Jean Dupont • 515-870-9990 • 515-870-9942 • 515-870-5586 • 515-870-5587
Adresse de la société <ul style="list-style-type: none"> • Adresse postale • Ville ou localité • Etat ou province • Pays (ou région) • Code postal • Version en langue nationale • Adresse de courrier électronique • Adresse de courrier électronique secondaire • Support pour les PTF (correctifs) 	<ul style="list-style-type: none"> • 94 West Proctor St. • Boone • Iowa • Etats-Unis • 55902 • Anglais (2924) • monnom@société.com • monnom@autresociété.com • Sélection automatique
Emplacement <ul style="list-style-type: none"> • Pays (ou région) • Etat 	<ul style="list-style-type: none"> • Etats-Unis • Iowa
Méthode de connexion	Via un serveur éloigné
Type de connexion	Connexion multiple entre noeuds à Internet
Adresse de la passerelle VPN ou nom d'hôte	192.168.1.1 (vous pouvez aussi fournir à la place le nom d'hôte [charles@masociété.com])

Si vous préférez utiliser les commandes CL pour créer la configuration, utilisez les commandes Modifier point de contact (CHGCNTINF) et Création d'une configuration de maintenance (CRTSRVCFG).

Etape 2 : Démarrez iSeries Navigator et sélectionnez l'assistant de connexion universelle.

Pour démarrer l'assistant de connexion universelle et commencer à établir votre connexion, procédez comme suit :

1. Ouvrez le logiciel iSeries Navigator.
2. Sélectionnez sous le dossier Mes connexions le serveur à configurer pour les Téléservices.
3. Développez l'arborescence de **Réseau**.
4. Développez l'arborescence de **Services d'accès distant**.
5. Cliquez à l'aide du bouton droit de la souris sur **Profils de connexion de l'expéditeur**.
6. Sélectionnez **Configuration de connexion universelle** pour démarrer l'assistant de connexion universelle. La boîte de dialogue de bienvenue apparaît.

Remarque : Une barre de progression indique qu'iSeries Navigator charge l'assistant de connexion universelle. En cas d'incident pendant l'exécution de l'assistant, consultez la section «Identification et résolution des incidents liés à l'assistant de connexion universelle», à la page 70 pour trouver une solution. Relancez l'assistant après avoir résolu l'incident.

Etape 3 : Indiquez les informations demandées (service, adresse et pays) dans les boîtes de dialogue de l'assistant.

Pour entrer des informations sur votre entreprise et vos connexions, procédez comme suit :

1. Dans la boîte de dialogue Choix d'une configuration, sélectionnez **Configuration de connexion principale** ou **Configuration de connexion de secours**. La configuration par défaut est la configuration de connexion principale. Cochez la case **Affichage et modification des informations concernant le contact** et cliquez sur **Suivant**.

2. Dans la boîte de dialogue Informations de maintenance, entrez les informations suivantes sur MaSociété et cliquez sur **Suivant** :

- Société – MaSociété
- Nom du contact – Jean Dupont
- Numéro de téléphone – 515-870-9990
- Service d'assistance ou numéro de messagerie — 515-870-9999
- Numéro de fax — 515-870-5586
- Numéro de fax secondaire — 515-870-9942

Si ces informations existent sur votre serveur, les données relatives à votre société s'affichent dans les zones correspondantes. Par exemple, si MaSociété a déjà créé une configuration, l'assistant extrait les données de la configuration existante.

3. Dans la boîte de dialogue Adresse de la société, entrez l'adresse de MaSociété et cliquez sur **Suivant**.

- Adresse postale – 94 West Proctor St.
- Ville ou localité – Boone
- Etat ou province – Iowa
- Pays ou région – Etats-Unis
- Code postal – 55902
- Version en langue nationale – English (2924)
- Adresse de courrier électronique – monnom@société.com
- Adresse de courrier électronique secondaire – monnom@autresociété.com
- Support pour les PTF – Sélection automatique

4. Dans la boîte de dialogue Emplacement, sélectionnez le pays (ou la région) et l'état ou la province dans lesquels est situé votre serveur iSeries puis cliquez sur **Suivant**.

- Pays ou région – Etats-Unis
- Etat – Iowa

Etape 4 : Sous Connexion via un autre système ou une autre partition, sélectionnez l'option Connexion VPN multiple entre noeuds à Internet.

Remarque : Il existe une case à cocher **Configuration supplémentaire d'une connexion proxy** . Si votre société possède un proxy HTTP ou que vous avez configuré un proxy de maintenance et de support sur un autre système ou une autre partition et que vous souhaitez utiliser les applications de connexion universelle prenant en charge la connexion via un proxy, cochez cette case. Si cette case est cochée, une étape 6 apparaîtra.

Etape 5 : Indiquez une adresse de passerelle VPN ou un nom d'hôte qui permettra d'établir la connexion multiple entre noeuds VPN à IBM.

Indiquez l'adresse de passerelle de connexion multiple entre noeuds VPN ou le nom du serveur hôte qui se connecte aux Téléservices IBM.

Etape 6 : Pour l'option de proxy, configurez un serveur proxy cible.

Remarque : Cet écran apparaît uniquement si vous avez choisi l'option de serveur proxy au cours de l'étape 4.

Pour configurer un serveur proxy cible

1. **Essayez d'abord d'établir une connexion au serveur proxy**

- a. Choisissez cette option si vous souhaitez que le proxy ait la priorité sur la configuration de ce scénario.

- | b. Si nécessaire, cochez la case **Le serveur proxy cible requiert une authentification standard HTTP** et remplissez les champs **Nom d'utilisateur** et **Mot de passe**.
- | c. Cliquez sur **Suivant** et passez à l'étape suivante.
- | 2. **Essayez d'établir une connexion si la configuration préalablement définie échoue**
 - | a. Choisissez cette option si le proxy doit uniquement être utilisé lorsque la configuration de ce scénario échoue.
 - | b. Complétez le champ **Adresse IP ou nom d'hôte du proxy**.
 - | c. Complétez le champ **Port du serveur proxy**.
 - | d. Si nécessaire, cochez la case **Le serveur proxy cible requiert une authentification standard HTTP** et remplissez les champs **Nom d'utilisateur** et **Mot de passe**.
 - | e. Cliquez sur **Suivant** et passez à l'étape suivante.

| **Etape 7 : Indiquez que ce serveur ne fournit pas de connexion aux autres serveurs ou partitions.**

| Cliquez sur **Non** pour indiquer que ce serveur possède une connexion directe avec les Téléservices mais qu'il ne fournit pas de connexion aux autres serveurs ou partitions.

| **Etape 8 : Passez en revue la fenêtre Récapitulatif afin de vérifier que la configuration répond à vos besoins et cliquez sur Terminer pour enregistrer la configuration.**

| Pour terminer la configuration du serveur et la sauvegarder, procédez comme suit :

- | 1. Consultez le récapitulatif de la configuration. Cliquez sur **Précédent** si vous devez modifier une valeur dans l'une des boîtes de dialogue de l'assistant.
- | 2. Lorsque la configuration est correcte, cliquez sur **Terminer** pour sauvegarder la configuration. Une barre de progression vous indique que l'assistant est en train de sauvegarder la configuration.

| **Etape 9 : Testez la connexion aux Téléservices à partir de votre serveur.**

| Pour tester la configuration, procédez comme suit :

- | 1. Cliquez sur **Oui** lorsque l'assistant vous invite à tester la configuration. La boîte de dialogue Vérification de la connexion universelle s'affiche.
- | 2. Notez les erreurs éventuelles pendant que l'assistant affiche la progression de la vérification.
- | 3. Cliquez sur **OK** lorsque l'assistant indique que la vérification est terminée.
- | 4. Si l'assistant détecte des erreurs, redémarrez l'assistant de connexion universelle, apportez les corrections nécessaires, sauvegardez, puis testez à nouveau la configuration corrigée.

| **Etape 10 : Configurez une configuration de sauvegarde (facultatif).**

| Si une méthode de connexion supplémentaire est disponible, nous vous recommandons de réexécuter l'assistant afin de configurer une sauvegarde. Cette sauvegarde sera utilisée automatiquement en cas d'échec de la connexion principale.

Configuration de la connexion universelle

| Pour créer une connexion universelle entre votre serveur iSeries et les Téléservices IBM, définissez les procédures suivantes. Vous pouvez aussi consulter les scénarios de connexion universelle et suivre celui qui répond le mieux aux besoins de votre site en matière de configuration.

Procédures de l'assistant de connexion universelle

Les procédures suivantes impliquent la création d'une configuration via l'assistant de connexion universelle ou les commande CL. Après avoir préparé le système pour la configuration de la connexion universelle, choisissez la procédure de configuration qui répond le mieux aux besoins de votre site en matière de configuration matérielle et logicielle.

Remarque : Avant d'utiliser l'assistant pour créer une connexion universelle, assurez-vous d'avoir lu les informations de la section «Planification de la connexion universelle», à la page 7.

Configuration d'une connexion commutée via AGNS

Apprenez comment configurer à partir de votre serveur ou de votre partition une connexion vers une application de support IBM via AT&T Global Network Services (AGNS). Vous pouvez également configurer votre serveur afin qu'il agisse en tant que point de connexion via lequel les autres serveurs ou partitions accèdent à une application de support IBM.

Configuration d'une connexion commutée point à point éloignée

Apprenez comment configurer votre serveur ou votre partition afin qu'il puisse accéder aux Téléservices IBM via un serveur distant ou une console HMC.

Configuration d'une connexion directe à Internet

Apprenez comment configurer à partir de votre serveur ou de votre partition une connexion vers une application de support IBM via une connexion directe à Internet. Vous pouvez également configurer votre serveur afin qu'il agisse en tant que point de connexion via lequel les autres serveurs ou partitions accèdent à une application de support IBM.

Configuration d'une connexion point à point via un fournisseur d'accès Internet

Apprenez comment configurer à partir de votre serveur ou de votre partition une connexion vers une application de support IBM via un fournisseur d'accès Internet point à point. Vous pouvez également configurer votre serveur afin qu'il agisse en tant que point de connexion via lequel les autres serveurs ou partitions accèdent à une application de support IBM.

Configuration d'une connexion multiple entre noeuds

Apprenez comment configurer à partir de votre serveur ou de votre partition une connexion vers une application de support IBM via une connexion multiple entre noeuds distante.

Configuration d'une connexion commutée via AGNS

Utilisez l'assistant de connexion universelle de la façon indiquée ci-après pour créer une connexion universelle commutée à l'un des services suivants via AGNS (AT&T Global Network Services) :

- Téléservices
- Electronic Service Agent
- Mise à jour de l'Information Center

Remarque : Consultez le «Scénario : Configuration d'une connexion commutée point à point via AGNS», à la page 9 et le «Scénario : Configuration d'une connexion commutée point à point pour un serveur fournissant une connectivité à d'autres systèmes via AGNS», à la page 15 pour consulter des exemples de configuration spécifiques.

Conditions requises

Les conditions requises pour pouvoir activer les Téléservices via une connexion AGNS sont les suivantes :

- Vérifiez qu'iSeries Access for Windows et iSeries Navigator sont installés sur votre ordinateur personnel (voir iSeries Access for Windows - Installation et configuration).
- Assurez-vous d'avoir installé tous les Service Packs les plus récents pour iSeries Navigator. Les scénarios présentés utilisent la version 5.4 du logiciel.

- Vérifiez que TCP/IP est actif. Vous pouvez démarrer TCP/IP via la commande STRTCP (Démarrer TCP/IP).
- Pour pouvoir configurer la connexion à partir de l'assistant de connexion universelle, vous devez disposer du droit de responsable de la sécurité (*SECOFR) associé aux droits spéciaux *ALLOBJ, *IOSYSCFG et *SECADM dans votre profil utilisateur i5/OS et du droit *USE sur WRKCNTINF.
- Vous devez installer les utilitaires de connectivité TCP/IP (5722-TC1).
- Pour que le réseau privé virtuel (VPN) et la couche SSL fonctionnent, vous devez installer Digital Certificate Manager (DCM) (5722-SS1 option 34).
- Assurez-vous que la valeur système QRETSVRSEC a pour valeur 1. Pour cela, utilisez la commande DSPSYSVAL (Afficher une valeur système). Si cette valeur n'est pas fixée à 1, entrez la commande CHGSYSVAL (Modifier une valeur système). L'ID utilisateur et le mot de passe du compte peuvent ainsi être enregistrés sur le serveur iSeries.
- Si vous utilisez un modem interne tel que le modem 56 Kbps fourni avec la carte 9793, vérifiez que l'attribut de réseau MDMCOUNTRYID est correctement défini. Pour cela, utilisez la commande DSPNETA (Afficher les attributs du réseau). Si cet attribut n'est pas correctement défini, modifiez sa valeur à l'aide de la commande CHGNETA (Modifier les attributs du réseau).

Vous pouvez créer à partir du serveur une connexion universelle à un service IBM et vous avez également la possibilité de laisser le serveur agir en tant que point de connexion pour les autres serveurs ou les autres partitions du réseau.

Configuration d'une connexion commutée à partir du serveur via AGNS

Si la configuration TCP/IP existe déjà et est fonctionnelle, exécutez les étapes suivantes pour configurer une connexion universelle si vous vous connectez aux Téléservices IBM via un serveur local :

1. Démarrez iSeries Navigator et sélectionnez l'assistant de connexion universelle.
2. Sélectionnez une configuration de connexion principale ou de secours. La configuration par défaut est la configuration de connexion principale.
3. Cochez la case pour afficher et modifier les informations relatives aux points de contact.
4. Indiquez les informations demandées (service, adresse et pays ou région) dans les boîtes de dialogue de cet assistant.
5. Connectez-vous à partir du système en cours avec une connexion par ligne commutée utilisant AT&T Global Network Services comme type de connexion.
6. Cochez la case si vous souhaitez configurer un proxy.
7. Sélectionnez une ressource matérielle, un numéro de téléphone principal et un numéro de téléphone de secours pour la création d'une connexion via le modem.
8. Si vous choisissez de configurer un proxy, complétez les informations relatives au proxy. Le cas échéant, passez à l'étape suivante.
9. Indiquez que ce serveur ne fournit pas de connexion aux autres serveurs ou partitions.
10. Passez en revue la fenêtre Récapitulatif afin de vérifier que la configuration répond à vos besoins et cliquez sur **Terminer** pour enregistrer la configuration.
11. Lorsque vous y êtes invité, testez la connexion aux Téléservices à partir de votre serveur.

Configuration d'une connexion commutée à partir de votre serveur qui fournit aux autres systèmes une connexion via AGNS

Si la configuration TCP/IP existe déjà et est fonctionnelle, exécutez les étapes suivantes pour configurer une connexion universelle si vous vous connectez aux Téléservices IBM via un serveur local qui agit en tant que point de connexion pour les autres serveurs :

1. Démarrez iSeries Navigator et sélectionnez l'assistant de connexion universelle.

- | 2. Sélectionnez une configuration de connexion principale ou secondaire. La configuration par défaut est la configuration de connexion principale.
- | 3. Cochez la case pour afficher et modifier les informations relatives aux points de contact.
- | 4. Indiquez les informations demandées (service, adresse et pays ou région) dans les écrans de cet assistant.
- | 5. Connectez-vous à partir du système en cours avec une connexion par ligne commutée utilisant AT&T Global Network Services comme type de connexion.
- | 6. Cochez la case si vous souhaitez configurer un proxy.
- | 7. Sélectionnez une ressource matérielle, un numéro de téléphone principal et un numéro de téléphone de secours pour la création d'une connexion via le modem.
- | 8. Si vous choisissez de configurer un proxy, complétez les informations relatives au proxy. Le cas échéant, passez à l'étape suivante.
- | 9. Précisez que vous souhaitez que ce serveur iSeries fonctionne en tant que point de connexion par le biais duquel les autres serveurs et les autres partitions pourront se connecter aux Téléservices.
- | 10. Sélectionnez une ou plusieurs interfaces via lesquelles les autres serveurs ou les autres partitions pourront se connecter aux Téléservices.
- | 11. Créez ou sélectionnez un profil de réponse L2TP. Ce profil est nécessaire pour la reconnaissance des autres systèmes ou serveurs qui se connectent aux Téléservices via votre serveur.
- | 12. Configurez un serveur proxy de maintenance et de support.
- | 13. Passez en revue la fenêtre Récapitulatif afin de vérifier que la configuration répond à vos besoins et cliquez sur **Terminer** pour enregistrer la configuration.
- | 14. Lorsque vous y êtes invité, testez la connexion aux Téléservices IBM via votre serveur.

Configuration d'une connexion commutée point à point éloignée

| Utilisez l'assistant de connexion universelle de la façon indiquée ci-après pour créer une connexion universelle commutée à partir d'un serveur distant via un serveur, une partition ou une console HMC qui agit en tant que point de connexion :

- | • Téléservices
- | • Electronic Service Agent
- | • Mise à jour de l'Information Center

| **Remarque :** Consultez le «Scénario : Configuration d'une connexion commutée point à point via AGNS», à la page 9 et le «Scénario : Configuration d'une connexion commutée point à point pour un serveur fournissant une connectivité à d'autres systèmes via AGNS», à la page 15 pour consulter des exemples de configuration spécifique

| **Remarque :** Pour un exemple spécifique, consultez la rubrique «Scénario : Configuration d'une connexion commutée point à point distante», à la page 23.

Conditions requises

Les conditions requises pour pouvoir activer les Téléservices via une connexion AGNS éloignée sont les suivantes :

- Vérifiez qu'iSeries Access for Windows et iSeries Navigator sont installés sur votre ordinateur personnel (voir iSeries Access for Windows - Installation et configuration).
- Assurez-vous d'avoir installé tous les Service Packs les plus récents pour iSeries Navigator. Les scénarios présentés utilisent la version 5.4 du logiciel.
- Vérifiez que TCP/IP est actif. Vous pouvez démarrer TCP/IP via la commande STRTCP (Démarrer TCP/IP).

- | • Pour pouvoir configurer la connexion à partir de l'assistant de connexion universelle, vous devez disposer du droit de responsable de la sécurité (*SECOFR) associé aux droits spéciaux *ALLOBJ, *IOSYSCFG et *SECADM dans votre profil utilisateur i5/OS et du droit *USE sur WRKCNTINF.
- | • Vous devez installer les utilitaires de connectivité TCP/IP (5722-TC1).
- | • Vous devez installer Digital Certificate Manager (DCM) (5722-SS1 option 34).
- | • Assurez-vous que la valeur système QRETSVRSEC a pour valeur 1. Pour cela, utilisez la commande DSPSYSVAL (Afficher une valeur système). Si cette valeur n'est pas fixée à 1, entrez la commande CHGSYSVAL (Modifier une valeur système).
- | • Le point de connexion doit avoir été configuré sur le système ou sur la console HMC auquel ou à laquelle le modem est relié.

Configuration d'une connexion commutée à partir d'un serveur éloigné via AGNS

Si la configuration TCP/IP existe déjà et est fonctionnelle, exécutez les étapes suivantes pour configurer la connexion universelle si vous vous connectez aux Téléservices via un serveur éloigné :

- | 1. Démarrez iSeries Navigator et sélectionnez l'assistant de connexion universelle.
- | 2. Sélectionnez une configuration de connexion principale ou secondaire. La configuration par défaut est la configuration de connexion principale.
- | 3. Cochez la case pour afficher et modifier les informations relatives aux points de contact.
- | 4. Indiquez les informations demandées (service, adresse et pays ou région) dans les écrans de cet assistant.
- | 5. Connectez-vous à partir d'un autre système et d'une autre partition possédant une connexion par ligne commutée et utilisant AT&T Global Network Services comme type de connexion.
- | 6. Cochez la case si vous souhaitez configurer un proxy.
- | 7. Pour créer une connexion distante à IBM, indiquez l'adresse de la passerelle ou le nom d'hôte du serveur qui se connecte à IBM.
- | 8. Si vous choisissez de configurer un proxy, complétez les informations relatives au proxy. Le cas échéant, passez à l'étape suivante.
- | 9. Paramétrez l'option "Définir en tant que point de connexion pour les autres systèmes ou partitions" sur Non.
- | 10. Passez en revue la fenêtre Récapitulatif afin de vérifier que la configuration répond aux conditions requises et cliquez sur **Terminer** pour enregistrer la configuration.
- | 11. Lorsque vous y êtes invité, testez la connexion aux Téléservices IBM via votre serveur.

Configuration d'une connexion directe à Internet

| Utilisez l'assistant de connexion universelle de la façon indiquée ci-après pour créer une connexion universelle à l'un des services suivants via une connexion directe à Internet :

- | • Téléservices
- | • Electronic Service Agent
- | • Mise à jour de l'Information Center

| **Remarque :** Consultez le «Scénario : Configuration d'une connexion directe à Internet», à la page 29 et le «Scénario : Configuration d'une connexion directe à Internet à partir d'un serveur qui fournit la connectivité pour d'autres systèmes ou partitions», à la page 34 pour consulter des exemples de configuration spécifiques.

Conditions requises

| Les conditions requises pour pouvoir activer les Téléservices via une connexion directe à Internet sont les suivantes :

- Le serveur iSeries doit disposer d'une adresse IP à acheminement global ou doit se trouver derrière un pare-feu NAT avec une adresse à acheminement global.
- Assurez-vous d'avoir installé tous les Service Packs les plus récents pour iSeries Navigator. Les scénarios présentés utilisent la version 5.4 du logiciel.
- Vérifiez que TCP/IP est actif. Vous pouvez démarrer TCP/IP via la commande STRTCP (Démarrer TCP/IP).
- | • Pour pouvoir configurer la connexion à partir de l'assistant de connexion universelle, vous devez disposer du droit de responsable de la sécurité (*SECOFR) associé aux droits spéciaux *ALLOBJ, *IOSYSCFG et *SECADM dans votre profil utilisateur i5/OS et du droit *USE sur WRKCNTINF.
- | • Vous devez installer les utilitaires de connectivité TCP/IP (5722-TC1).
- | • Vous devez installer Digital Certificate Manager (DCM) (5722-SS1 option 34).
- | • Assurez-vous que la valeur système QRETSVRSEC a pour valeur 1. Pour cela, utilisez la commande DSPSYSVAL (Afficher une valeur système). Si cette valeur n'est pas fixée à 1, entrez la commande CHGSYSVAL (Modifier une valeur système).
- Vérifiez qu'il existe une route TCP/IP pour acheminer les paquets de la connexion universelle vers Internet. Dans la plupart des cas, la route par défaut fonctionne.
- Assurez-vous que vos règles de filtrage autorisent l'acheminement sur Internet du trafic de la connexion universelle. Pour plus d'informations, voir «Pare-feu de filtrage des paquets IP», à la page 3.

Configuration d'une connexion universelle à partir de votre serveur via une connexion directe à Internet

Si la configuration TCP/IP existe déjà et est fonctionnelle, exécutez les étapes suivantes pour configurer la connexion universelle si vous vous connectez aux Téléservices via un serveur local :

- | 1. Démarrez iSeries Navigator et sélectionnez l'assistant de connexion universelle.
- | 2. Sélectionnez une configuration de connexion principale ou secondaire. La configuration par défaut est la configuration de connexion principale.
- | 3. Cochez la case pour afficher et modifier les informations relatives aux points de contact.
- | 4. Indiquez les informations demandées (service, adresse et pays ou région) dans les boîtes de dialogue de cet assistant.
- | 5. Connectez-vous à partir du système en cours avec une connexion directe à Internet comme type de connexion.
- | 6. Cochez la case si vous choisissez de configurer un proxy et complétez les informations relatives au proxy.
- | 7. Indiquez que ce serveur ne fournit pas de connexion aux autres serveurs ou partitions.
- | 8. Passez en revue la fenêtre Récapitulatif afin de vérifier que la configuration répond aux conditions requises et cliquez sur **Terminer** pour enregistrer la configuration.
- | 9. Lorsque vous y êtes invité, testez la connexion aux Téléservices à partir de votre serveur.

Configuration d'une connexion universelle à partir de votre serveur qui fournit aux autres systèmes un accès via une connexion directe à Internet

Si vous vous connectez aux Téléservices via le serveur local qui agit en tant que point de connexion pour les autres serveurs, exécutez les étapes suivantes pour configurer la connexion universelle :

- | 1. Démarrez iSeries Navigator et sélectionnez l'assistant de connexion universelle.
- | 2. Sélectionnez une configuration de connexion principale ou secondaire. La configuration par défaut est la configuration de connexion principale.
- | 3. Cochez la case pour afficher et modifier les informations relatives aux points de contact.
- | 4. Indiquez les informations demandées (service, adresse et pays ou région) dans les écrans de cet assistant.

5. Connectez-vous à partir du système en cours avec une connexion directe à Internet comme type de connexion.
6. Cochez la case si vous choisissez de configurer un proxy et complétez les informations relatives au proxy.
7. Précisez que vous souhaitez que ce serveur iSeries fonctionne en tant que point de connexion par le biais duquel les autres serveurs et les autres partitions pourront se connecter aux Téléservices.
8. Sélectionnez une ou plusieurs interfaces via lesquelles les autres serveurs ou les autres partitions pourront se connecter aux Téléservices.
9. Créez ou sélectionnez un profil de réponse L2TP. Ce profil est nécessaire pour la reconnaissance des autres systèmes ou serveurs qui se connectent aux Téléservices via votre serveur.
10. Configurez un serveur proxy de maintenance et de support.
11. Passez en revue la fenêtre Récapitulatif afin de vérifier que la configuration répond aux conditions requises et cliquez sur **Terminer** pour enregistrer la configuration.
12. Lorsque vous y êtes invité, testez la connexion aux Téléservices IBM via votre serveur.

Configuration d'une connexion PPP via un fournisseur d'accès Internet

Utilisez l'assistant de connexion universelle de la façon indiquée ci-après pour créer une connexion universelle à l'un des services suivants via une connexion ISP (fournisseur d'accès Internet) point à point :

- Téléservices
- Electronic Service Agent
- Mise à jour de l'Information Center

Remarque : Consultez le «Scénario : Configuration d'une connexion PPP via un fournisseur d'accès Internet», à la page 40 et le «Scénario : Configuration d'une connexion commutée point à point à partir d'un serveur fournissant une connectivité à d'autres systèmes via un fournisseur d'accès Internet», à la page 46 pour consulter des exemples de configuration spécifique.

Conditions requises

Les conditions requises pour pouvoir activer les Téléservices via une connexion directe à Internet sont les suivantes :

- Vérifiez qu'iSeries Access for Windows et iSeries Navigator sont installés sur votre ordinateur personnel (voir iSeries Access for Windows - Installation et configuration).
- Assurez-vous d'avoir installé tous les Service Packs les plus récents pour iSeries Navigator. Les scénarios présentés utilisent la version 5.4 du logiciel.
- Vérifiez que TCP/IP est actif. Vous pouvez démarrer TCP/IP via la commande STRTCP (Démarrer TCP/IP).
- Pour pouvoir configurer la connexion à partir de l'assistant de connexion universelle, vous devez disposer du droit de responsable de la sécurité (*SECOFR) associé aux droits spéciaux *ALLOBJ, *IOSYSCFG et *SECADM dans votre profil utilisateur i5/OS et du droit *USE sur WRKCNTINF.
- Vous devez installer les utilitaires de connectivité TCP/IP (5722-TC1).
- Vous devez installer Digital Certificate Manager (DCM) (5722-SS1 option 34).
- Assurez-vous que la valeur système QRETSVRSEC a pour valeur 1. Pour cela, utilisez la commande DSPSYSVAL (Afficher une valeur système). Si cette valeur n'est pas fixée à 1, entrez la commande CHGSYSVAL (Modifier une valeur système). L'ID utilisateur et le mot de passe du compte peuvent ainsi être stockés sur le serveur iSeries.
- Si vous utilisez un modem interne tel que le modem 56 Kbps fourni avec la carte 9793, vérifiez que l'attribut de réseau MDMCOUNTRYID est correctement défini. Pour cela, utilisez la commande DSPNETA

- | (Afficher les attributs du réseau). Si cet attribut n'est pas correctement défini, modifiez sa valeur à l'aide de la commande CHGNETA (Modifier les attributs du réseau).
- | • Le profil utilisé pour se connecter à votre fournisseur d'accès Internet doit avoir déjà été configuré.
- | • Vérifiez qu'une route TCP/IP est associée à votre profil ISP afin qu'elle achemine le trafic de la connexion universelle vers votre fournisseur d'accès Internet. Dans la plupart des cas, la route par défaut fonctionne.

Configuration d'une connexion universelle à partir de votre serveur via une connexion ISP (fournisseur d'accès Internet)

Si la configuration TCP/IP existe déjà et est fonctionnelle, exécutez les étapes suivantes pour configurer la connexion universelle si vous vous connectez aux Téléservices via le serveur local :

- | 1. Démarrez iSeries Navigator et sélectionnez l'assistant de connexion universelle.
- | 2. Sélectionnez une configuration de connexion principale ou secondaire. La configuration par défaut est la configuration de connexion principale.
- | 3. Cochez la case pour afficher et modifier les informations relatives aux points de contact.
- | 4. Indiquez les informations demandées (service, adresse et pays ou région) dans les boîtes de dialogue de cet assistant.
- | 5. Connectez-vous à partir du système en cours en utilisant un fournisseur d'accès Internet comme type de connexion.
- | 6. Sélectionnez un profil de connexion existant pour votre fournisseur d'accès Internet à partir de la boîte de dialogue Sélection de profil.
- | 7. Indiquez que ce serveur ne fournit pas de connexion aux autres serveurs ou partitions.
- | 8. Passez en revue la fenêtre Récapitulatif afin de vérifier que la configuration répond aux conditions requises et cliquez sur **Terminer** pour enregistrer la configuration.
- | 9. Lorsque vous y êtes invité, testez la connexion aux Téléservices IBM via votre serveur.

Configuration d'une connexion universelle à partir de votre serveur qui fournit aux autres serveurs un accès via une connexion ISP (fournisseur d'accès Internet) point à point

Si vous vous connectez aux Téléservices via un serveur éloigné ou si votre serveur local agit en tant que point de connexion pour les autres serveurs, exécutez les étapes suivantes pour configurer la connexion universelle :

1. Démarrez iSeries Navigator et sélectionnez l'assistant de connexion universelle.
2. Sélectionnez une configuration de connexion principale ou secondaire. La configuration par défaut est la configuration de connexion principale.
3. Cochez la case pour afficher et modifier les informations relatives aux points de contact.
4. Indiquez les informations demandées (service, adresse et pays ou région) dans les écrans de cet assistant.
5. Connectez-vous à partir du système en cours en utilisant un fournisseur d'accès Internet comme type de connexion.
6. Sélectionnez un profil de connexion existant pour votre fournisseur d'accès Internet à partir de la boîte de dialogue Sélection de profil.
7. Précisez que vous souhaitez que ce serveur iSeries fonctionne en tant que point de connexion par le biais duquel les autres serveurs ou les autres partitions pourront se connecter aux Téléservices IBM.
8. Sélectionnez une ou plusieurs interfaces via lesquelles les autres serveurs ou les autres partitions pourront se connecter aux Téléservices.
9. Créez ou sélectionnez un profil de réponse L2TP. Ce profil est nécessaire pour la reconnaissance des autres systèmes ou serveurs qui se connectent aux Téléservices IBM via votre serveur.
10. Configurez un serveur proxy de maintenance et de support.

11. Passez en revue la fenêtre Récapitulatif afin de vérifier que la configuration répond aux conditions requises et cliquez sur **Terminer** pour enregistrer la configuration.
12. Lorsque vous y êtes invité, testez la connexion aux Téléservices IBM via votre serveur.

Configuration d'une connexion multiple entre noeuds

Utilisez l'assistant de connexion universelle de la façon indiquée ci-après pour créer une connexion universelle à l'un des services suivants via une connexion multiple entre noeuds distante via Internet.

- Téléservices
- Electronic Service Agent
- Mise à jour de l'Information Center

Remarque : Pour un exemple de configuration spécifique, consultez la rubrique «Scénario : Configuration d'une connexion multiple entre noeuds via un serveur distant», à la page 53.

Conditions requises et préalables

Les conditions requises pour pouvoir activer les Téléservices via une connexion multiple entre noeuds distante sont les suivantes :

- Le serveur iSeries doit disposer d'une connexion IP à la passerelle multiple entre noeuds VPN.
- Vérifiez qu'iSeries Access for Windows et iSeries Navigator sont installés sur votre ordinateur personnel (voir iSeries Access for Windows - Installation et configuration).
- Assurez-vous d'avoir installé tous les Service Packs les plus récents pour iSeries Navigator. Les scénarios présentés utilisent la version 5.4 du logiciel.
- Vérifiez que TCP/IP est actif. Vous pouvez démarrer TCP/IP via la commande STRTCP (Démarrer TCP/IP).
- Pour pouvoir configurer la connexion à partir de l'assistant de connexion universelle, vous devez disposer du droit de responsable de la sécurité (*SECOFR) associé aux droits spéciaux *ALLOBJ, *IOSYSCFG et *SECADM dans votre profil utilisateur i5/OS et du droit *USE sur WRKCNTINF.
- Vous devez installer les utilitaires de connectivité TCP/IP (5722-TC1).
- Vous devez installer Digital Certificate Manager (DCM) (5722-SS1 option 34).
- Assurez-vous que la valeur système QRETSVRSEC a pour valeur 1. Pour cela, utilisez la commande DSPSYSVAL (Afficher une valeur système). Si cette valeur n'est pas fixée à 1, entrez la commande CHGSYSVAL (Modifier une valeur système).
- Vérifiez que la route TCP/IP par défaut ou qu'une route hôte achemine le trafic en provenance de l'interface TCP/IP appropriée vers Internet afin que la connexion VPN puisse être établie avec IBM. Pour des informations supplémentaires, consultez les rubriques «Détermination des adresses de passerelle VPN IBM», à la page 69 et «Détermination des adresses de destination de services IBM», à la page 69.

Configuration d'une connexion multiple entre noeuds via un serveur distant

Si la configuration TCP/IP existe déjà et est fonctionnelle, exécutez les étapes suivantes pour configurer la connexion universelle si vous vous connectez aux Téléservices via un autre serveur ou une autre partition :

1. Démarrez iSeries Navigator et sélectionnez l'assistant de connexion universelle.
2. Sélectionnez une configuration de connexion principale ou secondaire. La configuration par défaut est la configuration de connexion principale.
3. Cochez la case pour afficher et modifier les informations relatives aux points de contact.
4. Indiquez les informations demandées (service, adresse et pays ou région) dans les boîtes de dialogue de cet assistant.

5. Connectez-vous à partir d'un autre système ou d'une autre partition utilisant une connexion multiple entre noeuds VPN à Internet comme type de connexion.
6. Cochez la case si vous souhaitez configurer un proxy.
7. Indiquez une adresse de passerelle VPN ou un nom d'hôte qui permettra d'établir la connexion multiple entre noeuds VPN à IBM.
8. Si vous choisissez de configurer un proxy, complétez les informations relatives au proxy. Le cas échéant, passez à l'étape suivante.
9. Indiquez que ce système ne fournit pas de connexion aux autres serveurs ou partitions.
10. Passez en revue la fenêtre Récapitulatif afin de vérifier que la configuration répond aux conditions requises et cliquez sur **Terminer** pour enregistrer la configuration.
11. Lorsque vous y êtes invité, testez la connexion aux Téléservices à partir de votre serveur.

Configuration d'une connexion multiple entre noeuds à partir d'un serveur qui agit en tant que point de connexion pour les autres serveurs

Si vous vous connectez aux Téléservices via un autre serveur ou une autre partition, exécutez les étapes suivantes pour configurer la connexion universelle :

1. Démarrez iSeries Navigator et sélectionnez l'assistant de connexion universelle.
2. Sélectionnez une configuration de connexion principale ou secondaire. La configuration par défaut est la configuration de connexion principale.
3. Cochez la case pour afficher et modifier les informations relatives aux points de contact.
4. Indiquez les informations demandées (service, adresse et pays ou région) dans les écrans de cet assistant.
5. Connectez-vous à partir d'un autre système ou d'une autre partition utilisant une connexion multiple entre noeuds VPN à Internet comme type de connexion.
6. Cochez la case si vous souhaitez configurer un proxy.
7. Indiquez une adresse de passerelle VPN ou un nom d'hôte qui permettra d'établir la connexion multiple entre noeuds VPN à IBM.
8. Si vous choisissez de configurer un proxy, complétez les informations relatives au proxy. Le cas échéant, passez à l'étape suivante.
9. Précisez que vous souhaitez que ce serveur iSeries fonctionne en tant que point de connexion par le biais duquel les autres serveurs ou les autres partitions pourront se connecter aux Téléservices IBM.
10. Sélectionnez une ou plusieurs interfaces via lesquelles les autres serveurs ou les autres partitions pourront se connecter aux Téléservices.
11. Créez ou sélectionnez un profil de réponse L2TP. Ce profil est nécessaire pour la reconnaissance des autres systèmes ou serveurs qui se connectent aux Téléservices IBM via votre serveur.
12. Configurez un serveur proxy de maintenance et de support.
13. Passez en revue la fenêtre Récapitulatif afin de vérifier que la configuration répond aux conditions requises et cliquez sur **Terminer** pour enregistrer la configuration.
14. Lorsque vous y êtes invité, testez la connexion aux Téléservices IBM via votre serveur.

Procédures supplémentaires de configuration de la connexion universelle

Les procédures suivantes permettent de configurer les informations sur le fournisseur de services, de tester la connexion aux Téléservices, de vérifier la compatibilité avec SOCKS et de localiser l'adresse des passerelles VPN IBM et les destinations de service.

Configuration des informations relatives au fournisseur de services

Apprenez à configurer les informations relatives au fournisseur de services.

Test de la connexion avec les Téléservices

Apprenez à tester votre connexion afin de vérifier le bon fonctionnement de la connexion universelle avec les Téléservices.

Vérification de la compatibilité avec SOCKS

Apprenez à localiser les adresses que vous devez traiter directement.

Détermination des adresses de passerelle VPN IBM

Apprenez à déterminer l'adresse des connexions passerelle VPN IBM.

Détermination des adresses de destinations de services IBM

Apprenez à déterminer les adresses de destinations de services IBM utilisées par les applications de service.

Configuration des informations relatives au fournisseur de services

Il peut arriver que vous ayez besoin de prendre contact directement par téléphone avec un fournisseur de services. Pour configurer les échanges téléphoniques relatifs à une demande de maintenance, procédez comme indiqué ci-après :

1. Sur la ligne de commande du menu principal, tapez WRKCNTINF et appuyez sur Entrée. La boîte de dialogue Gestion des points de contact assistance s'affiche.
2. Sur la ligne de commande, tapez 6 (Gestion des prestataires de maintenance) et appuyez sur Entrée.
3. Sélectionnez l'option 2 pour modifier l'entrée du point de contrôle *IBMSRV et appuyez sur Entrée. La boîte de dialogue Modification d'un prestataire de maintenance s'affiche.
4. Si vous installez ce serveur aux Etats-Unis, tapez les informations suivantes dans l'écran Modification d'un prestataire de maintenance :
Maintenance du matériel : **1-800-426-7378**
Maintenance du logiciel : **1-800-237-5511**
Si vous n'installez pas ce serveur aux Etats-Unis, prenez contact avec votre technicien de maintenance pour connaître les numéros de téléphone des services de maintenance :
5. Appuyez sur Entrée.
6. Appuyez sur F3 (Exit) pour revenir à l'écran Gestion des points de contact assistance.

Test de la connexion avec les Téléservices

Pour vous assurer du bon fonctionnement de la connexion universelle avec les Téléservices, effectuez le test suivant :

Pour tester la connexion universelle, procédez comme suit :

1. Localisez la boîte de dialogue Envoi d'une demande de test :
 - a. Affichez le menu principal.
 - b. Sur la ligne de commande, tapez SNDSVRQS *TEST.
 - c. Appuyez sur Entrée. La boîte de dialogue Envoi d'une demande de test s'affiche.
2. Appuyez sur Entrée pour lancer le test.
3. La phrase Demande de test achevée s'affiche au bas de l'écran pour indiquer que le test a abouti. Si le test ne fonctionne pas, notez le message d'erreur et prenez contact avec votre technicien de maintenance.

Vérification de la compatibilité avec SOCKS

Pour trouver l'adresse IP des passerelles VPN, voir «Détermination des adresses de passerelle VPN IBM», à la page 69. Le trafic provenant de ces adresses IP doit être acheminé vers le serveur SOCKS. Ces acheminements doivent s'effectuer directement.

| En outre, des routes hôte sont créées pour toutes les destinations de service car l'application tente de se connecter à cette destination. Pour rechercher les hôtes de maintenance devant être traités directement, consultez la section «Détermination des adresses de destination de services IBM».


Détermination des adresses de passerelle VPN IBM

Pour trouver les adresses de passerelle VPN IBM après avoir exécuté l'assistant de connexion universelle (lorsque vous utilisez iSeries Navigator), procédez comme suit :

1. Localisez le profil de connexion de l'expéditeur L2TP en cliquant sur les options suivantes : **Réseau > Services d'accès distant > Profils de connexion de l'expéditeur**.
2. Cliquez à l'aide du bouton droit de la souris sur le profil **QVPN01IBM1** et sélectionnez Propriétés.
3. Sélectionnez l'onglet **Connexion** pour afficher l'adresse de passerelle VPN IBM présentée comme le nom hôte ou l'adresse IP du noeud final du tunnel distant.
4. Cliquez à l'aide du bouton droit de la souris sur le profil **QVPN01IBM2** et sélectionnez Propriétés.
5. Sélectionnez l'onglet **Connexion** pour afficher l'adresse de passerelle VPN IBM présentée comme le nom hôte ou l'adresse IP du noeud final du tunnel distant.
6. Répétez les étapes 2 à 5 pour les profils **QVPN02IBM1** et **QVPN02IBM2** (s'ils existent).

Pour trouver les adresses de passerelle VPN IBM si vous utilisez une passerelle VPN Cisco pour une connexion multiple entre noeuds, procédez comme suit :

Pour trouver l'adresse de la passerelle VPN IBM, procédez comme suit :

1. Accédez au site Web Support for iSeries family
(<http://www-1.ibm.com/servers/eserver/support/iseres/index.html>) .
2. Sélectionnez **Technical Databases**.
3. Sélectionnez **Registered Software Knowledge Base**. Vous devez disposer d'un mot de passe correct pour pouvoir accéder à cette page et d'un contrat d'assistance en ligne valable pour accéder à ces rubriques.
4. Une fois que vous avez tapé le mot de passe, effectuez une recherche sur **VPN Cisco multi-hop Connection Configuration** ou **23300444**. Cette page vous fournira l'adresse IP GWA sous forme d'adresse de passerelle IBM.

Détermination des adresses de destination de services IBM

| Pour rechercher les adresses de destination de services IBM pouvant être utilisées pour le trafic HTTP et HTTPS, vous pouvez parcourir le fichier de définition de localisation du fournisseur de services. Le fichier se trouve dans

| `'/qibm/userdata/os400/universalconnection/serviceProviderIBMLocationDefinition.xml'`

| Les éléments <Adresse-IP> et <Port> définissent des informations relatives à l'adresse nécessaires pour le filtrage des règles et/ou configurations SOCKS.

| Si vous ne trouvez pas le fichier susmentionné, le fichier principal (contenant les adresses de tous les emplacements mondiaux) se trouve dans

| `'/qibm/userdata/os400/universalconnection/serviceProviderIBM.xml'` ou

| `'/qibm/proddata/os400/universalconnection/serviceProviderIBM.xml'`.


| Vous pouvez parcourir n'importe lequel de ces fichiers à l'aide de la commande CL DSPF.

Identification et résolution des incidents liés à l'assistant de connexion universelle

Si vous ne parvenez pas à exécuter l'assistant de connexion universelle, répondez aux questions suivantes et relancez l'assistant.

1. L'assistant de connexion universelle est-il indisponible ?

Vérifiez que les critères suivants sont bien remplis :

- iSeries Access for Windows doit être installé. Pour plus d'informations, consultez le site Web iSeries Access (<http://www-1.ibm.com/servers/eserver/series/access/>) .

- Le composant réseau en option doit être installé.

- Pour pouvoir configurer la connexion à partir de l'assistant de connexion universelle, vous devez disposer du droit de responsable de la sécurité (*SECOFR) associé aux droits spéciaux *ALLOBJ, *IOSYSCFG et *SECADM dans votre profil utilisateur i5/OS et du droit *USE sur WRKCNTINF.

2. Si vous utilisez un modem interne, votre attribut réseau Code pays ou région du modem correspond-il à l'emplacement de votre serveur iSeries ?

Pour vérifier que la valeur de cet attribut est correcte :

- A partir d'une ligne de commande i5/OS, entrez la commande DSPNETA (Afficher les attributs du réseau).
- Appuyez sur Entrée.
- Si la valeur est correcte, passez à la question suivante.
- Si la valeur est incorrecte, modifiez-la en tapant CHGNETA MDMCOUNTRYID(XX), où XX représente le code pays ou région adéquat.

3. La valeur système QRETSVRSEC est-elle correcte ?

Pour que les informations d'authentification nécessaires à la connexion à IBM soient correctement renvoyées, vérifiez que cette valeur système est fixée à 1 (Conserver les données). Pour effectuer cette modification, procédez comme suit : A partir d'une ligne de commande i5/OS, entrez CHGSYSVAL SYSVAL(QRETSVRSEC) VALUE('1')

4. TCP est-il démarré ?

Vous devez démarrer TCP pour que l'assistant de connexion universelle puisse fonctionner correctement. En outre, TCP doit être actif chaque fois que vous accédez à la connexion universelle. Pour démarrer TCP :

- A partir d'une ligne de commande i5/OS, entrez STRTCP (Démarrer TCP).
- Appuyez sur Entrée.


5. Votre réseau privé virtuel (VPN) fonctionne-t-il correctement ?

Pour obtenir de l'aide, voir Troubleshoot VPN.

6. Le modem que vous utilisez existe-t-il dans la liste de sélection ou est-il nécessaire de modifier certains paramètres par défaut ?

Pour modifier la liste des modems, choisissez l'une des options suivantes :

- Pour modifier la liste des modems avec iSeries Navigator, procédez comme suit :
 - Sélectionnez le serveur approprié.
 - Développez l'arborescence de **Réseau**.
 - Sélectionnez **Services d'accès distant**.
 - Sélectionnez Modems.
 - Pour plus d'informations, voir Configure your modem for PPP. Pour connaître les paramètres adéquats, consultez le manuel fourni avec le modem.
- Pour modifier la liste des modems à partir de la ligne de commande, procédez comme suit :
 - A partir d'une ligne de commande i5/OS, entrez CFGTCPPTP.

- b. Appuyez sur Entrée.
 - c. Sélectionnez l'option 11 (Work with modem information).
 - d. Sélectionnez les options permettant d'ajouter ou de modifier les modems. Pour plus d'informations, voir Configure your modem for PPP. Pour connaître les paramètres adéquats, consultez le manuel fourni avec le modem.
7. Votre modem est-il configuré avec un type de trame asynchrone (paramètre FRAMING) ?
- Si tel n'est pas le cas, il peut s'avérer nécessaire de modifier les paramètres du commutateur DIP et d'autres éléments matériels. Pour des informations supplémentaires, reportez-vous au manuel fourni avec le modem. Si vous utilisez un modem interne ou un IBM 7852-400, aucune modification n'est nécessaire.
8. Des incidents se sont-ils produits lorsque vous avez tenté de tester la connexion ?
- Voir Troubleshoot PPP.
9. Tentez-vous actuellement d'utiliser une connexion commutée SNA existante aux Téléservices pour la sauvegarde ?
- Vérifiez que la description de ligne QESLINE mentionne un nom de ressource correct (DSPLIND QESLINE) et est connectée à un modem compatible avec le mode synchrone. Vous pouvez utiliser le même modem IBM 7852-400 pour la connexion universelle et pour une sauvegarde SNA. Pour plus d'informations, voir Configure an SNA connection. Il est également possible d'utiliser deux modems distincts.
10. Etes-vous en train d'établir une connexion à l'assistant de connexion universelle via AT&T Global Network Services ?
- Si vous utilisez AT&T pour établir la connexion aux Téléservices, tenez compte des informations suivantes :
- a. Tous les 30 jours (ou chaque fois que vous utilisez la connexion universelle au-delà de cette période de 30 jours), votre serveur télécharge une liste téléphonique AT&T mise à jour. Cela permet de conserver une liste téléphonique à jour pour la connexion universelle.
 - b. Lors de ce téléchargement, un message est envoyé dans la file d'attente de messages de l'opérateur système.
 - c. Si vos profils de connexion universelle contiennent un ou plusieurs numéros de téléphone qui ne figurent plus dans la liste téléphonique AT&T à jour, le système envoie un message de diagnostic. Ce message a pour but de vous demander d'exécuter à nouveau l'assistant de connexion universelle afin de mettre à jour les numéros de téléphone. Lorsque vous exécutez de nouveau cet assistant, les numéros de téléphone mis à jour vous sont présentés afin que vous puissiez les sélectionner. Pour visualiser les numéros de téléphone les plus récents, consultez le site Web AT&T Business Internet Services (www.attbusiness.net)  .

Annexe. Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays.

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 106-0032, Japon

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales. LES PUBLICATIONS SONT LIVREES «EN L'ETAT» SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES PUBLICATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. 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 produits et logiciels décrits dans ce document.

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
| Software Interoperability Coordinator, Department YBWA
| 3605 Highway 52 N
| Rochester, MN 55901
| 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 dispositions de l'ICA, des Conditions Internationales d'Utilisation de Logiciels IBM, des Conditions d'Utilisation du Code Machine ou de tout autre contrat 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.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

Ces informations sont fournies uniquement à titre de planification. Elles sont susceptibles d'être modifiées avant la mise à disposition des produits décrits.

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.

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 entreprise) (année). Des segments de code sont dérivés des Programmes exemples d'IBM Corp. © Copyright IBM Corp. _entrez la ou les années_. All rights reserved.

Si vous visualisez ces informations en ligne, il se peut que les photographies et illustrations en couleur n'apparaissent pas à l'écran.

Marques

Les termes qui suivent sont des marques d'International Business Machines Corporation aux Etats-Unis et/ou dans certains autres pays :

- | AIX
- | AIX 5L
- | AS/400
- | Electronic Service Agent
- | e(logo)server
- | eServer
- | i5/OS
- | IBM
- | iSeries
- | Système d'exploitation OS/400
- | OS/400
- | pSeries
- | Windows
- | xSeries
- | zSeries

Microsoft, Windows, Windows NT 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.

Dispositions

Les droits d'utilisation relatifs à ces publications sont soumis aux dispositions suivantes.

Usage personnel : Vous pouvez reproduire ces publications pour votre usage personnel, non commercial, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez distribuer ou publier tout ou partie de ces informations ou en faire des oeuvres dérivées sans le consentement exprès d'IBM.

Usage commercial : Vous pouvez reproduire, distribuer et afficher ces publications uniquement au sein de votre entreprise, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez reproduire, distribuer, afficher ou publier tout ou partie de ces publications en dehors de votre entreprise, ou en faire des oeuvres dérivées, sans le consentement exprès d'IBM.

Excepté les droits d'utilisation expressément accordés dans ce document, aucun autre droit, licence ou autorisation, implicite ou explicite, n'est accordé pour ces publications ou autres informations, données, logiciels ou droits de propriété intellectuelle contenus dans ces publications.

IBM se réserve le droit de retirer les autorisations accordées ici si, à sa discrétion, l'utilisation des publications s'avère préjudiciable à ses intérêts ou que, selon son appréciation, les instructions susmentionnées n'ont pas été respectées.

Vous ne pouvez télécharger, exporter ou réexporter ces informations qu'en total accord avec toutes les lois et règlements applicables dans votre pays, y compris les lois et règlements américains relatifs à l'exportation.

IBM N'OCTROIE AUCUNE GARANTIE SUR LE CONTENU DE CES PUBLICATIONS. LES PUBLICATIONS SONT LIVREES EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES PUBLICATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

IBM