IBM SecureWay Policy Director

Guide de configuration et d'utilisation

Version 3 Edition 0

IBM SecureWay Policy Director

Guide de configuration et d'utilisation

Version 3 Edition 0

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Annexe. Remarques» à la page 95.

Première édition – octobre 1999

Réf. US : CT63KNA

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

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

Vous pouvez également consulter les serveurs Internet suivants :

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

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

Table des matières

Avis aux lecteurs canadiens

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

Illustrations

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

Terminologie

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

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

Claviers

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

OS/2 - Paramètres canadiens

Au Canada, on utilise :

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

Nomenclature

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

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

A propos de ce manuel

Ce manuel couvre les procédures d'installation et de configuration du produit IBM SecureWay Policy Director (Policy Director). Les serveurs Policy Director peuvent être installés sur les systèmes d'exploitation suivants :

- Microsoft Windows NT
- AIX
- Solaris

Le client NetSEAT peut être installé sur les systèmes d'exploitation suivants :

- Windows 95
- Windows 98
- Windows NT

A qui ce manuel s'adresse-t-il ?

Ce manuel est destiné à l'administrateur en charge de la planification et de l'installation de Policy Director.

L'administrateur doit être familiarisé avec l'installation et la configuration de l'environnement IBM DCE (Distributed Computing Environment) et du protocole LDAP (Lightweight Directory Access Protocol) d'IBM SecureWay Directory. Les serveurs IBM SecureWay Directory et IBM DCE sont utilisés par Policy Director et sont fournis avec ce produit.

Organisation du manuel

Ce manuel comprend les chapitres suivants :

- Le «Chapitre 1. Principes de Policy Director» à la page 1 fournit une présentation générale de Policy Director et de ses composants.
- Le «Chapitre 2. Configuration système requise» à la page 15 indique les conditions que votre environnement d'exploitation doit satisfaire en matière de logiciels et de configuration matérielle.
- Le «Chapitre 3. Planification de l'installation de Policy Director» à la page 19 indique comment planifier, organiser et gérer Policy Director.
- Le «Chapitre 4. Installation et configuration d'IBM SecureWay Directory» à la page 29 indique comment réaliser l'installation et la configuration du client SDK et du serveur de SecureWay Directory version 3.1.1 (LDAP) si vous voulez utiliser le registre des utilisateurs LDAP. Vous devez installer et

configurer le serveur LDAP avant d'installer Policy Director. Notez que le serveur LDAP doit également être activé avant l'installation de Policy Director.

- Le «Chapitre 5. Installation de Policy Director pour Windows» à la page 45 décrit l'installation et la configuration de Policy Director sur le système d'exploitation Windows NT.
- Le «Chapitre 6. Installation de Policy Director pour AIX» à la page 59 décrit l'installation et la configuration de Policy Director sur le système d'exploitation IBM AIX.
- Le «Chapitre 7. Installation de Policy Director pour Solaris» à la page 75 décrit l'installation et la configuration de Policy Director sur le système d'exploitation Sun Solaris.
- Le «Chapitre 8. Documentation annexe» à la page 89 indique où trouver les autres documents liés à Policy Director et aux produits associés.

Nouveautés de cette édition

Cette nouvelle édition de Policy Director comprend les innovations suivantes :

- Prise en charge d'IBM SecureWay Directory pour le stockage des données de droit d'accès des utilisateurs et des groupes.
- Dernières mises à jour de la spécification de l'API d'autorisation développée par le Open Group.
- Possibilité de définir et de modifier les droits d'accès des utilisateurs relais d'IBM Firewall à l'aide de la console de gestion de Policy Director.
- Service d'acquisition de droits d'accès (SAD) permettant d'utiliser des services d'authentification externes.
- Prise en charge de l'authentification par certificat de côté client à l'aide du nouveau service d'acquisition de droits d'accès.
- Possibilité d'élaborer un service d'acquisition de droits d'accès personnalisé à l'aide de l'interface IDL (Interface Definition Language) qui permet d'utiliser WebSEAL en association avec le SAD de Policy Director. Policy Director apporte également des fonctions de serveur standard qui permettent de gérer les fonctions du serveur SAD telles que le démarrage, l'enregistrement du serveur et la gestion des signaux.
- Possibilité d'utiliser la transmission par tunnel SSL en plus de la transmission par tunnel GSS.
- Gestion des règles de connexion et de mot de passe à l'aide de l'interface de ligne de commande de Policy Director.
- Gestion des utilisateurs, des groupes et des ressources SSO (destinations) à l'aide de la console de gestion ou de l'interface de ligne de commande de Policy Director.

- Utilitaire Web de gestion des mots de passe des ressources SSO.
- Procédure d'installation intégrée.

Compatibilité avec l'an 2000

Ces produits sont conçus pour passer l'an 2000 sans incident. Utilisés conformément aux recommandations données, ils peuvent accepter, traiter et générer des données comportant des dates comprises dans et entre le vingtième et le vingt-et-unième siècle dans la mesure où toutes les ressources (matériels, logiciels tiers et applications propriétaires) utilisées simultanément peuvent gérer ces dates sans incident.

Service et prise en charge

Contactez IBM pour obtenir des services et une prise en charge pour tous les produits de l'offre IBM SecureWay FirstSecure. La documentation de certains de ces produits peut mentionner une assistance fournie par une société tiers. Si vous avez acquis ces produits dans le cadre de l'offre FirstSecure, contactez IBM pour bénéficier d'une assistance.

Conventions

Ce manuel utilise les conventions typographiques suivantes :

Convention	Signification
gras	Eléments d'interface utilisateur tels que cases à cocher, boutons et éléments de listes.
`espacement fixe`	Syntaxe, exemple de code et texte à saisir par l'utilisateur.
italique	Mise en relief et première occurrence de termes spécifiques à Policy Director.
→	Série de sélections dans un menu. Par exemple : Cliquez sur **Fichier → Exécuter** signifie : Cliquez sur **Fichier**, puis cliquez sur **Exécuter**.

Informations disponibles sur le Web

Des informations relatives aux dernières mises à jour de Policy Director sont disponibles à l'adresse suivante :

`http://www.ibm.com/software/security/policy/library`

Des informations relatives aux mises à jour des autres produits IBM SecureWay FirstSecure sont disponibles à l'adresse suivante :

`http://www.ibm.com/software/security/firstsecure/library`

Chapitre 1. Principes de Policy Director

IBM SecureWay Policy Director (Policy Director) est disponible comme composant du progiciel IBM SecureWay FirstSecure et comme produit autonome.

Présentation d'IBM SecureWay FirstSecure

IBM SecureWay FirstSecure (FirstSecure) fait partie des solutions intégrées de sécurité proposées par IBM. FirstSecure comprend un ensemble de produits intégrés permettant de :

- créer un environnement sécurisé pour le e-business ;
- simplifier la planification de la sécurité pour réduire son coût ;
- mettre en application des règles de sécurité ;
- créer un environnement performant pour le e-business.

Les produits IBM SecureWay sont les suivants :

Policy Director
IBM SecureWay Policy Director (Policy Director) fournit des fonctions d'authentification, d'autorisation, de sécurisation des données et de gestion des ressources Web.

Boundary Server
IBM SecureWay Boundary Server (Boundary Server) propose les fonctions suivantes :

- Fonctions de pare-feu telles que filtrage, serveur relais et passerelle de circuit
- Connexion d'un réseau privé virtuel au pare-feu IBM Firewall
- Composants dédiés à la sécurité Internet
- Solution de sécurité des codes mobiles

Une interface utilisateur graphique de configuration permet de relier la fonction d'utilisateur relais de Policy Director au produit Firewall.

Intrusion Immunity
Intrusion Immunity offre des fonctions de détection d'intrusions et de protection antivirus.

Trust Authority

IBM SecureWay Trust Authority (Trust Authority) permet la prise en charge des normes de cryptographie et d'interdépendance fonctionnelle PKI. Trust Authority permet la délivrance, le renouvellement et la révocation des certificats numériques. Ces certificats permettent d'authentifier les utilisateurs et de sécuriser les communications.

Toolbox

Le produit IBM SecureWay Toolbox (Toolbox) regroupe des interfaces de programme d'application permettant d'incorporer des fonctions de sécurité aux logiciels développés. Le produit Toolbox fait partie du progiciel FirstSecure. Policy Director comme Toolbox comprennent la bibliothèque d'API de Policy Director et la documentation associée.

Dans la mesure où chacun des produits d'IBM SecureWay FirstSecure peut être installé séparément, vous pouvez planifier la sécurisation de votre environnement de façon contrôlée. Cette faculté réduit la complexité et le coût de cette sécurisation en même temps qu'elle permet d'accélérer la mise en place des applications et des ressources Web.

Pour plus d'informations sur les composants de FirstSecure et pour connaître les différents documents liés aux produits de la famille IBM SecureWay, reportez-vous au manuel *Guide de planification et d'intégration* de FirstSecure.

Présentation d'IBM SecureWay Policy Director

Policy Director est une solution autonome de gestion des autorisations et de la sécurité qui permet d'assurer une sécurité totale des ressources dans des réseaux internes et externes géographiquement distants. Un *extranet* est un réseau privé virtuel (RPV) qui utilise des fonctions de contrôle d'accès et de sécurité pour limiter à quelques personnes choisies l'usage d'un ou plusieurs intranets reliés à l'Internet.

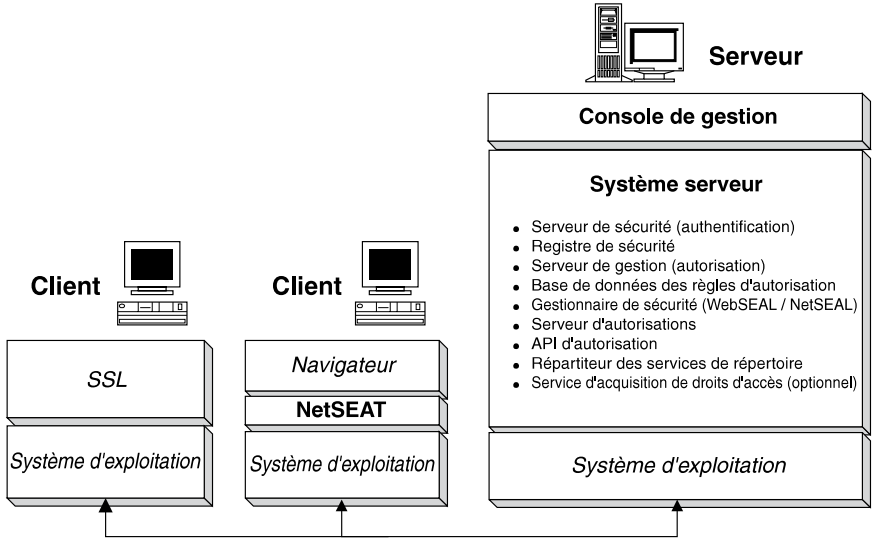
Policy Director propose des services d'authentification, d'autorisation, de sécurisation des données et de gestion des ressources. Vous pouvez utiliser Policy Director en relation avec des applications Internet standard pour concevoir des intranets et des extranets sécurisés et optimisés.

Policy Director est conçu pour les systèmes d'exploitation Windows NT, AIX et Solaris.

Composants de Policy Director

Policy Director comprend les composants suivants :

- Protocole LDAP d'IBM SecureWay Directory, clients et serveurs de DCE IBM
- Module de base de Policy Director
- Serveur de gestion
- Gestionnaire de sécurité, composé de WebSEAL et de NetSEAL
- Service d'acquisition de droits d'accès (SAD)
- Serveur d'autorisations
- API d'autorisation
- Client NetSEAT
- Console de gestion
- Répartiteur des services de répertoire (RSR)



Vous devez déterminer les fonctions de gestion et de sécurité dont votre réseau a besoin avant d'installer Policy Director. Utilisez les sections qui suivent pour identifier les composants de Policy Director qui vous sont nécessaires.

IBM SecureWay Directory et serveurs DCE

Les serveurs IBM SecureWay Directory et IBM DCE sont utilisés par Policy Director et sont fournis avec ce produit.

Policy Director peut utiliser au choix un registre des utilisateurs LDAP ou DCE. Vous devez choisir le registre des utilisateurs qu'utilisera Policy Director au cours de l'installation.

Si vous prévoyez d'utiliser le registre des utilisateurs LDAP, vous devez installer un client LDAP et configurer un serveur LDAP avant d'installer Policy Director. Reportez-vous aux instructions du «Chapitre 4. Installation et configuration d'IBM SecureWay Directory» à la page 29. Si vous prévoyez d'utiliser un registre des utilisateurs DCE, vous pouvez ignorer ce chapitre consacré à l'installation et la configuration de LDAP.

Serveur IBM SecureWay Directory

SecureWay Directory utilise le protocole LDAP pour gérer les informations des annuaires à partir d'une position centrale (enregistrement, mises à jour, extraction et échange de données). Si vous utilisez LDAP pour gérer votre registre des utilisateurs, Policy Director utilisera aussi LDAP pour accorder les autorisations aux utilisateurs.

Serveur DCE IBM

La solution d'environnement informatique partagé IBM DCE (Distributed Computing Environment) intègre des services et des utilitaires de création, d'utilisation et de gestion des applications partagées dans un environnement informatique hétérogène. Le DCE constitue le domaine sécurisé dans lequel les serveurs Policy Director peuvent authentifier les utilisateurs et communiquer en toute sécurité. Sur le système d'exploitation Windows NT, le client NetSEAT a le rôle du client DCE.

Module de base de Policy Director

Le module IVBase de Policy Director est le logiciel de référence utilisé par tous les composants de Policy Director. Il s'installe automatiquement lorsque vous installez d'autres composants de Policy Director, sauf dans le cas particulier de la console de gestion pour Windows.

Pour la version AIX, le composant SMIT Setup (IV.Smit) est intégré au module IV.Base. Ce module contient des données de configuration utilisées par SMIT et doit être installé sur tous les serveurs AIX.

Serveur de gestion

Le serveur de gestion (IVMgr) est le serveur d'autorisations principal pour l'ensemble du domaine sécurisé. Il contrôle et administre la base de données des autorisations principale. Tous les flux de données transitent par le serveur de gestion.

Vous devez installer le serveur de gestion sur une machine du domaine sécurisé avant d'installer les gestionnaires de sécurité ou les serveurs d'autorisations mais pas nécessairement sur le même ordinateur que ces derniers composants. Chaque domaine sécurisé ne doit contenir qu'une seule instance du serveur de gestion.

Chaque instance du serveur de gestion installée sur une machine donnée nécessite d'installer les composants suivants sur la même machine :

- Client DCE
- Client LDAP (si vous utilisez un registre des utilisateurs LDAP)
- Module de base de Policy Director
- Serveur de gestion

Gestionnaire de sécurité

Le gestionnaire de sécurité (IVNet) applique les règles de contrôle d'accès d'après les données d'une instance (copie) de la base de données des règles d'autorisation. Le gestionnaire de sécurité comprend les composants suivants :

- WebSEAL pour le contrôle d'accès avancé des transactions HTTP et HTTPS
- NetSEAL pour le contrôle d'accès standard des transactions TCP/IP

Vous devez obligatoirement installer NetSEAL et WebSEAL pour configurer et activer ces fonctions (qui sont désactivées par défaut).

WebSEAL

WebSEAL (IVWeb) est le serveur HTTP attaché au gestionnaire de sécurité. Il s'agit d'un serveur Web sécurisé pouvant accepter les transactions des clients HTTP, HTTPS et NetSEAT. Couplé au service d'acquisition de droits d'accès de Policy Director, WebSEAL permet l'authentification des utilisateurs Policy Director par le biais de certificats X.509.

NetSEAL

NetSEAL (IVTrap) réalise un contrôle d'accès standard pour les serveurs TCP/IP. Ce composant contrôle les accès sur une série de ports configurés sur un serveur TCP/IP.

La suite de produits Policy Director constitue une solution de sécurisation des échanges de données entre clients et serveurs, dans le cadre de l'Internet comme dans celui des intranets privés. Policy Director NetSEAL et Policy Director WebSEAL sont des programmes de côté serveur qui contrôlent et gèrent les données des réseaux à l'intérieur des domaines sécurisés définis dans l'environnement informatique partagé (DCE).

Serveur d'autorisations

Le serveur d'autorisations (IVAcld) répond aux requêtes d'autorisation des applications tiers qui utilisent l'API d'autorisation de Policy Director en mode

distant. Le serveur d'autorisations doit être installé sur au moins une machine du domaine sécurisé contenant les applications tiers.

API d'autorisation

Le module IVAuthADK de Policy Director comprend des API (interface de programme d'application) d'autorisation. Ces API permettent de concevoir des applications utilisant les services d'autorisation de Policy Director.

Le kit de développement d'applications ADK (Application Development Kit) de Policy Director comprend un serveur d'API d'autorisation (AuthAPI) qui permet au développeur d'intégrer des règles de sécurité et d'autorisation Policy Director directement dans ses applications. Les API d'autorisation de Policy Director offrent un accès direct au service d'autorisation de Policy Director. Cette possibilité signifie que le développeur n'a désormais plus besoin de créer un code d'autorisation pour chaque application.

Le kit de développement d'applications comprend des échantillons de programme en langage C.

Il contient également le code source du serveur SAD de démonstration et celui du serveur de service d'autorisation externe de démonstration.

Client NetSEAT

Le client Policy Director NetSEAT est un client sommaire conçu pour Windows 95, Windows 98 ou Windows NT. Son rôle est d'établir des canaux de communication sécurisés pour les besoins des serveurs de Policy Director.

Le client NetSEAT permet aux autres clients d'accéder aux domaines sécurisés et d'utiliser les services de sécurité avancés proposés par les serveurs NetSEAL et WebSEAL. NetSEAT sécurise toutes les communications de réseau d'un client en codant l'ensemble des données de ses transactions client-serveur et Web.

NetSEAT peut également sécuriser les transactions TCP/IP d'un client notamment celles générées par des services tels que Telnet et POP3. Le client NetSEAT permet à l'administrateur système d'exercer un contrôle d'accès standard sur les activités de réseau d'un poste de travail. Ce contrôle repose sur l'utilisation des fonctions du domaine sécurisé, notamment sur ses fonctions d'authentification et d'affectation de privilèges aux utilisateurs et aux ressources.

Console de gestion

La console de gestion (IVConsole) est une application graphique Java qui permet d'administrer les règles de sécurité du domaine sécurisé de Policy Director. A partir de cette console, vous pouvez exécuter diverses taches d'administration sur le registre des comptes et sur la base de données primaire des règles d'autorisation. La console de gestion nécessite qu'un client

DCE se connecte au domaine sécurisé et contacte les serveurs de gestion de Policy Director au moyen d'appels RPC sécurisés. La console de gestion utilise des services de DCE de base (services d'exploitation) fournis par le client NetSEAT (pour Windows 95, Windows 98 ou Windows NT).

Répartiteur des services de répertoire

Le répartiteur des services de répertoire fait partie du module du serveur de gestion. La console de gestion et les clients NetSEAT nécessitent l'installation d'un répartiteur des services de répertoire dans le domaine sécurisé si vous utilisez des stations de travail Windows NT, Windows 95, ou Windows 98. En général, le répartiteur des services de répertoire ne requiert plus aucune tâche d'administration ou de configuration après son installation initiale.

Service d'acquisition de droits d'accès (en option)

Le service d'acquisition de droits d'accès (SAD) de Policy Director est un composant proposé en option.

L'*acquisition de droits d'accès* est un processus consistant à transformer ou convertir des données d'identité, fournies par un système d'authentification, en une représentation standard de l'identité du client utilisable à l'échelle du domaine. C'est cette représentation standard que l'on appelle les *droits d'accès du client*.

Lorsque vous avez besoin d'acquérir des droits d'accès, vous devez configurer le SAD de Policy Director à utiliser avec le serveur WebSEAL Policy Director. Les utilisateurs de Policy Director sont automatiquement associés aux droits d'accès par WebSEAL.

Les données de *certificat* des clients utilisant des certificats X.509 de côté client peuvent être associées à des identités Policy Director par le biais du SAD Policy Director ou par celui d'un service d'acquisition de droits d'accès créé par vous même.

Si des utilisateurs sont définis dans un registre externe, leurs noms d'utilisateur peuvent être mappés (rattachés) à des identités reconnues par Policy Director par le biais d'un serveur SAD personnalisé. Vous pouvez concevoir et personnaliser un serveur SAD adapté à votre domaine sécurisé pour traiter des données d'authentification telles que des certificats de client, des noms d'utilisateur ou des jetons. La personne chargée de concevoir ou de créer le SAD détermine tous les aspects de ce service d'authentification et de mappage. Policy Director stocke les règles de mappage dans une base de données externe. Policy Director assure l'interface IDL entre WebSEAL et le service d'acquisition de droits d'accès de Policy Director et apporte des fonctions de serveur standard qui permettent de gérer les fonctions du serveur SAD telles que le démarrage, l'enregistrement du serveur et la gestion

des signaux. Il revient au développeur du SAD d'étendre ses capacités pour exécuter les fonctions de mappage d'identités demandées par chaque application.

Pour plus d'informations sur chacun des composants de Policy Director, reportez-vous au manuel *Policy Director - Guide d'administration*.

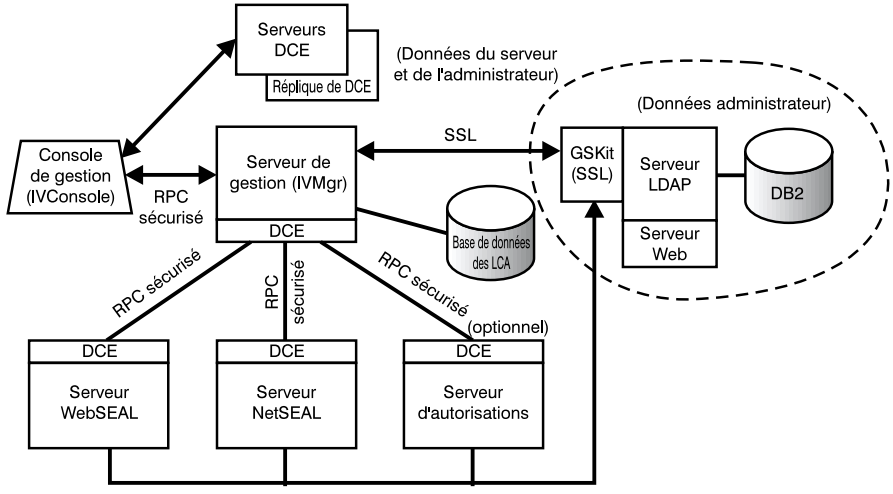
Fonctionnement de Policy Director

Les sections qui suivent détaillent quatre types d'utilisation ordinaire de Policy Director :

- Utilisation de la console de gestion par l'administrateur
- Utilisateur accédant à des ressources Web protégées à partir d'un navigateur Web
- Utilisateur accédant à un serveur TCP/IP protégé via un client NetSEAT
- Utilisateur accédant à un serveur tiers protégé

Utilisation de la console de gestion par l'administrateur

Le schéma suivant illustre les flux de données intervenant lorsque l'administrateur gère Policy Director au moyen de la console de gestion. Les composants LDAP (ligne en pointillés) n'interviennent que si vous utilisez le registre des utilisateurs LDAP.



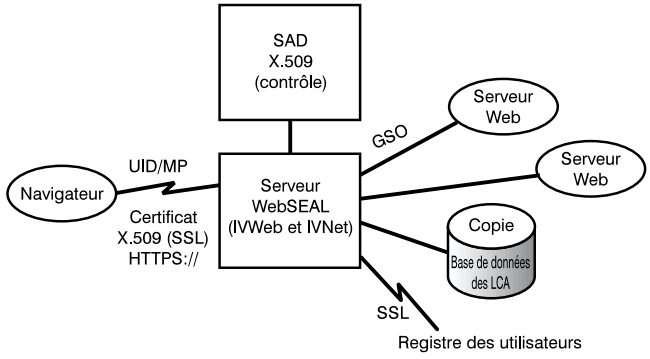
A partir de la console de gestion, l'administrateur s'authentifie et reçoit des droits d'accès.

S'il gère des utilisateurs et des groupes, la console de gestion envoie des requêtes au serveur de gestion par le biais d'un appel RPC sécurisé. Le serveur de gestion transmet les informations reçues au serveur LDAP via une connexion SSL précédemment établie sur la base du DN et du mot de passe du serveur de gestion.

Si l'administrateur ajoute, modifie ou applique une liste de contrôle d'accès (LCA), la console de gestion envoie ces données au serveur de gestion par le biais d'un appel RPC sécurisé. Le serveur de gestion enregistre ensuite les modifications dans l'instance locale de la base de données des LCA. Une fois la base de données modifiée, le serveur de gestion notifie cette mise à jour à tous les autres serveurs au moyen d'un appel RPC sécurisé. Les serveurs WebSEAL, NetSEAL et le serveur d'autorisations vérifient périodiquement auprès du serveur de gestion l'existence de mises à jour de la base de données des LCA.

Utilisateur accédant à des ressources Web protégées à partir d'un navigateur Web

Le schéma suivant illustre les flux de données intervenant lorsqu'un utilisateur accède à des ressources Web protégées à partir d'un navigateur Web.



Lorsque l'utilisateur tente d'accéder à une page Web protégée, le navigateur SSL contacte le serveur WebSEAL. Si le serveur WebSEAL a été configuré pour pratiquer l'authentification sur la base de certificats de client, il demande un certificat X.509 au navigateur. Une fois ce certificat réceptionné, il le transmet au serveur du SAD. Le SAD tente alors de mapper ce certificat à une identité d'utilisateur reconnue par Policy Director. Dans le fichier de configuration du SAD, l'administrateur de Policy Director peut créer une table associant le DN d'un certificat à celui d'un utilisateur Policy Director. Lorsque WebSEAL soumet un certificat au SAD, celui-ci extrait d'abord son DN puis recherche son occurrence dans la table. S'il en trouve une, le SAD renvoie à WebSEAL le DN d'utilisateur Policy Director associé. WebSEAL utilise ensuite ce DN pour identifier l'utilisateur Policy Director. En l'absence d'occurrence, le SAD renvoie à WebSEAL le DN extrait du certificat. Dans cette situation, l'utilisateur Policy Director est identifié au moyen de ce DN de certificat. Le serveur WebSEAL utilise le DN renvoyé pour extraire les droits d'accès de l'utilisateur.

Pour plus d'informations sur les certificats X.509, consultez le site Web suivant :

`http://www.ietf.org`

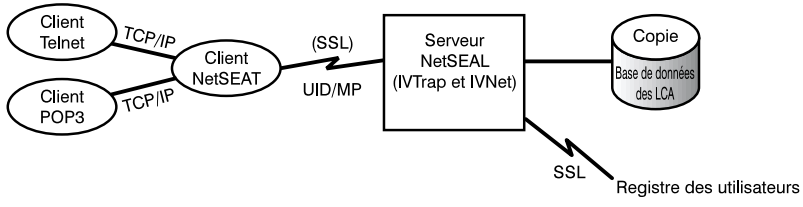
Une fois l'utilisateur authentifié, WebSEAL consulte l'instance locale de la base de données des LCA pour décider si cet utilisateur est autorisé ou non à accéder à l'objet Web comme il le demande.

Si la connexion entre le serveur WebSEAL et le serveur d'arrière-plan contenant la ressource Web demandée passe par une jonction GSO, WebSEAL recherche les droits d'accès GSO attachés à cette jonction dans LDAP et communique le nom de l'utilisateur et son mot de passe au serveur Web.

Pour plus d'informations sur la gestion des ressources GSO et des groupes de ressources GSO, reportez-vous aux sections du manuel *Policy Director - Guide d'administration* consacrées à la console de gestion.

Utilisateur accédant à un serveur TCP/IP protégé via un client NetSEAT

Le schéma suivant illustre les flux de données intervenant lorsqu'un utilisateur accède à un serveur TCP/IP protégé via un client NetSEAT.



A partir d'un client Telnet, l'utilisateur envoie une requête de connexion à un serveur protégé par NetSEAL. NetSEAL demande le nom de l'utilisateur et son mot de passe et vérifie cette identité en la comparant à celle contenue dans le registre des utilisateurs. NetSEAL vérifie que l'utilisateur peut accéder à la machine via le port spécifié.

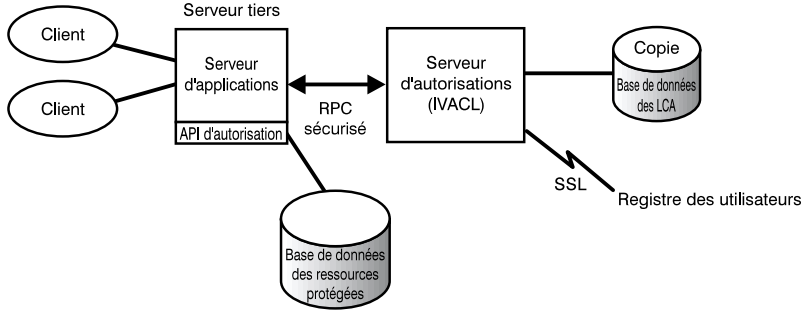
NetSEAT réoriente de manière transparente les requêtes vers les serveurs Policy Director sécurisés au moyen d'un tunnel SSL sécurisé. NetSEAT utilise ses données de configuration pour reconnaître les requêtes adressées à un serveur sécurisé à partir d'applications TCP/IP génériques telles que Telnet, POP3 ou HTTP. NetSEAT utilise l'authentification de base, en plus du protocole SSL, pour déterminer l'identité et les droits d'accès de l'utilisateur de NetSEAT. Une fois l'autorisation établie, NetSEAT imbrique les données de la transaction dans un tunnel SSL sécurisé et l'exécute conformément aux règles de sécurité définies.

Par exemple, lorsqu'un navigateur Web demande à accéder à un service, ou à une ressource, sécurisé par le gestionnaire de sécurité de Policy Director, NetSEAT intercepte la requête de manière transparente et la transmet au serveur approprié. S'il s'agit de la première requête adressée à Policy Director et qu'une authentification est nécessaire, NetSEAT affiche une boîte de dialogue contenant une invite de connexion. Une fois l'utilisateur authentifié, Policy Director attache de manière transparente les droits d'accès appropriés aux requêtes suivantes. Ce processus permet d'établir un environnement de connexion unique (SSO) pour toutes les applications Winsock gérées par

Policy Director. En outre, Policy Director se base sur ces droits d'accès pour déterminer si un utilisateur peut ou non accéder à une ressource qu'il protège.

Utilisateur accédant à un serveur tiers protégé

Le schéma suivant illustre les flux de données intervenant lorsqu'un utilisateur accède à un serveur tiers protégé.



Lorsqu'un client tente d'accéder aux données d'un serveur tiers protégé, ce serveur l'authentifie et mappe son identité à un nom d'utilisateur Policy Director. Le serveur d'applications communique cette identité d'utilisateur Policy Director au serveur d'autorisations qui, à son tour, consulte le registre des utilisateurs LDAP (ou DCE selon les cas) et extrait les droits d'accès correspondants. Le serveur d'applications communique ensuite les droits d'accès de l'utilisateur, le nom de l'objet et l'opération demandée au serveur d'autorisations, qui renvoie une recommandation d'autoriser ou d'interdire cette opération. Sur cette base, le serveur d'applications autorise ou interdit l'accès.

Contenu du progiciel Policy Director

Les programmes du produit IBM SecureWay Policy Director version 3.0 sont contenus dans cinq CD-ROM. Le titre et le contenu de chaque CD-ROM sont présentés dans le tableau suivant.

Titre du CD-ROM	Contenu
IBM SecureWay Policy Director version 3.0	• IBM Policy Director version 3.0
IBM SecureWay Policy Director Security Services	• IBM DCE pour AIX version 2.2 • IBM DCE pour Windows NT version 2.2 • Transarc DCE pour Solaris version 2.0
IBM SecureWay Directory version 3.1.1 pour AIX	• IBM SecureWay Directory version 3.1.1 • IBM DB2 version 5.2 avec Fix Pack 7 • IBM Global Security Kit SSL Runtime Toolkit version 3.0.1 (GSKit)
IBM SecureWay Directory version 3.1.1 pour Windows NT	• IBM SecureWay Directory version 3.1.1 • IBM DB2 version 5.2 avec Fix Pack 7 • IBM Global Security Kit SSL Runtime Toolkit version 3.0.1 (GSKit)
IBM SecureWay Directory version 3.1.1 pour Solaris	• IBM SecureWay Directory version 3.1.1 • IBM DB2 version 5.2 avec Fix Pack 8 • IBM Global Security Kit SSL Runtime Toolkit version 3.0.1 (GSKit)

Chapitre 2. Configuration système requise

Les sections suivantes indiquent les conditions que votre environnement d'exploitation doit satisfaire en matière de logiciels et de configuration matérielle. Des informations de dernière minute sur la configuration système requise sont disponibles dans le fichier README du CD-ROM de Policy Director. Les informations contenues dans ce fichier README remplacent celles des documents imprimés.

Pour obtenir le dernier fichier README disponible, contactez le site WEB d'IBM SecureWay Policy Director, à l'adresse suivante :

`http://www.ibm.com/software/security/policy/library`

Avant d'installer les serveurs de Policy Director et les composants DCE, LDAP et NetSEAT, vérifiez que vous disposez bien des équipements et logiciels indiqués dans les sections qui suivent.

Configuration matérielle

L'utilisation de la mémoire, de la mémoire tampon et de la mémoire cache ainsi que les structures de contrôle sont adaptables. En revanche, les exigences concernant le système d'exploitation de base, les clients DCE et LDAP et les besoins des applications client déterminent des conditions minimales en matière d'espace disque et de mémoire.

La configuration matérielle requise pour installer le serveur Policy Director est la suivante :

Plate-forme	Espace disque minimum	RAM minimum
Serveur Windows NT avec processeur Intel (ou compatible) 80486 133 MHz ou supérieur	16 Mo	64 Mo
Serveur AIX avec matériel sur AIX 4.3.1	16 Mo	64 Mo
Serveur Solaris avec matériel sur Solaris 2.6	16 Mo	64 Mo

La configuration matérielle requise pour installer le client Policy Director est la suivante :

Plate-forme	Espace disque minimum	RAM minimum
Client Windows NT avec processeur Intel (ou compatible) 80486 133 MHz ou supérieur	16 Mo	32 Mo

Serveur AIX avec matériel sur AIX 4.3.1	16 Mo	32 Mo
Serveur Solaris avec matériel sur Solaris 2.6	16 Mo	24 Mo

Configuration logicielle

Pendant la planification de l'installation de Policy Director, vérifiez que vous disposez des versions requises des systèmes d'exploitation et des autres logiciels nécessaires mentionnés dans les sections qui suivent. S'agissant des systèmes d'exploitation, les conditions requises pour installer les serveurs Policy Director, le client NetSEAT et la console de gestion sont les suivantes :

Serveurs Policy Director

Les serveurs Policy Director peuvent être installés sur les systèmes d'exploitation suivants :

- Windows NT Server version 4.0 avec Service Pack 4 ou version ultérieure
- AIX version 4.3.1 ou version ultérieure
- Sun Solaris version 2.6

Clients NetSEAT

Les clients NetSEAT Policy Dirtector peuvent être installés sur les systèmes d'exploitation suivants :

- Windows NT version 4.0 avec Service Pack 4 ou version ultérieure
- Windows 98
- Windows 95

Console de gestion

La console de gestion de Policy Director peut être installée sur les systèmes d'exploitation suivants :

- Windows NT Server version 4.0 avec Service Pack 4, ou version ultérieure
- Windows NT, Windows 95 ou Windows 98
- AIX version 4.3.1 ou version ultérieure, avec Java Runtime 1.1.6 ou version ultérieure
- Sun Solaris version 2.6

Autres logiciels requis

Policy Director nécessite d'installer un serveur DCE et, si vous comptez utiliser le registre des utilisateurs LDAP, un serveur LDAP. Un serveur (DCE ou LDAP) doit être installé sur au moins une machine du domaine sécurisé. Les clients et les serveurs DCE et LDAP sont fournis avec Policy Director. Vous pouvez les installer avant Policy Director ou utiliser ceux déjà installés s'ils sont au niveau requis.

Windows NT et AIX

Sur les plates-formes Windows NT et AIX, les serveurs Policy Director nécessitent les logiciels suivants :

- IBM DCE pour Windows NT version 2.2 ou ultérieure, pour les serveurs Windows NT, ou IBM DCE pour AIX version 2.2 ou ultérieure, pour les serveurs AIX
- IBM SecureWay Directory version 3.1.1 (LDAP), comprenant DB2 version 5.2, Fix Pack 7 (LDAP doit être installé uniquement si vous comptez utiliser le registre des utilisateurs LDAP)
- Secure Sockets Layer (SSL) version 3.0 ou ultérieure
- Le SAD de Policy Director et WebSEAL nécessitent l'un des navigateurs Web suivants :
  - Microsoft Internet Explorer version 4 ou ultérieure
  - Netscape Communicator version 4.5 ou ultérieure
  - Netscape Navigator version 4.5 ou ultérieure
- Winsock version 2.0 ou ultérieure (pour les clients Policy Director sur Windows 95 uniquement)

Solaris

Sur les plates-formes Solaris, les serveurs Policy Director nécessitent les logiciels suivants :

- Transarc DCE version 2.0
- IBM SecureWay Directory version 3.1.1 (LDAP), comprenant DB2 version 5.2, Fix Pack 8 (LDAP doit être installé uniquement si vous comptez utiliser le registre des utilisateurs LDAP)
- Secure Sockets Layer version 3.0 ou ultérieure
- Le SAD de Policy Director et WebSEAL nécessitent l'un des navigateurs Web suivants :
  - Microsoft Internet Explorer version 4 ou ultérieure
  - Netscape Communicator version 4.5 ou ultérieure
  - Netscape Navigator version 4.5 ou ultérieure

Chapitre 3. Planification de l'installation de Policy Director

Les sections qui suivent indiquent comment préparer et planifier l'installation et la configuration de Policy Director. Lisez impérativement le «Chapitre 1. Principes de Policy Director» à la page 1 et déterminez quels composants de Policy Director vous sont nécessaires avant de planifier l'installation.

Configurations standard

Les configurations détaillées dans cette section peuvent vous aider à déterminer la mieux adaptée à votre réseau. Utilisez le tableau de la section «Composants requis pour les configurations courantes» à la page 20 pour identifier les composants que vous devez installer. Sélectionnez ensuite ces composants pendant la procédure d'installation de Policy Director. Notez que WebSEAL et NetSEAL peuvent s'installer sur n'importe quel ordinateur du réseau. Les configurations les plus courantes pour l'installation des composants de Policy Director sont détaillées ci-après.

Serveur de gestion uniquement
Dans cette première situation, on dispose d'une seule instance du serveur de gestion pour l'ensemble du domaine sécurisé. Le serveur de gestion réside seul sur une machine dédiée. Il administre la base de données primaire des autorisations du domaine sécurisé, la duplique à travers le domaine sécurisé et gère les données d'emplacement des autres modules de Policy Director définis dans le domaine sécurisé.

Gestionnaire de sécurité avec serveur WebSEAL
Le module WebSEAL comprend deux composants : le gestionnaire de sécurité (IVNet) et WebSEAL (IVWeb) proprement dit. Un serveur WebSEAL a pour rôle de protéger un espace Web. WebSEAL prend en charge des serveurs d'arrière-plan, pour permettre une accessibilité avancée et offrir un recours en cas de panne d'un serveur, par le biais de *jonctions intelligentes*, ou jonctions.

Gestionnaire de sécurité avec serveur NetSEAL
Le module NetSEAL comprend deux composants : le gestionnaire de sécurité (IVNet) et NetSEAL (IVTrap) proprement dit. Un serveur NetSEAL a pour mission de sécuriser un réseau privé virtuel (RPV) et d'assurer le contrôle d'accès aux services des réseaux existants et des réseaux tiers.

Gestionnaire de sécurité avec serveur WebSEAL et serveur NetSEAL
Combinaison d'un serveur WebSEAL et d'un serveur NetSEAL.

Serveur d'autorisations
Un serveur permet aux applications tiers d'appeler le service d'autorisation de Policy Director par le biais de l'API d'autorisation de Policy Director.

Serveur d'autorisations et ADK
Un serveur offre un environnement de développement pour créer des applications tiers utilisant l'API d'autorisation afin d'appeler le service d'autorisation.

Console de gestion
Application graphique Java qui permet d'administrer les règles de sécurité du domaine sécurisé de Policy Director. Il n'est pas impératif d'installer IVBase pour utiliser la console de gestion sur Windows.

Tous les composants
Un serveur propose l'ensemble des services mentionnés dans les configurations précédentes.

Composants requis pour les configurations courantes

Les configurations de Policy Director décrites dans la section «Configurations standard» à la page 19 sont répertoriées dans le tableau qui suit. Ce tableau indique les composants que vous devez installer pour chaque configuration. Ces composants apparaissent dans le tableau selon l'ordre à respecter pour leur installation (de gauche à droite).

Notez que WebSEAL et NetSEAL comprennent chacun deux composants :

WebSEAL Gestionnaire de sécurité (IVNet) et WebSEAL (IVWeb)

NetSEAL Gestionnaire de sécurité (IVNet) et NetSEAL (IVTrap)

Remarques sur IVBase :

- Il n'est pas impératif d'installer IVBase pour utiliser la console de gestion sur Windows.
- IV.Smit s'installe automatiquement avec IV.Base pour AIX.

Situations	Composants à installer							
	IVBase	**IVMgr**	**IVNet**	**IVWeb**	**IVTrap**	**IVAcld**	**IVAuthADK**	**IVConsole**
Une instance du serveur de gestion seul	X	X						
Gestionnaire de sécurité avec WebSEAL	X	X***	X	X				
Gestionnaire de sécurité avec NetSEAL	X	X***	X		X			
Gestionnaire de sécurité avec WebSEAL et NetSEAL	X	X***	X	X	X			
Serveur d'autorisations	X	X***				X		
Serveur d'autorisations et ADK	X	X***				X	X	
Console de gestion	X							X
Tous les composants	X	X***	X	X	X	X	X	X

*** S'il s'agit du premier ou du seul ordinateur du domaine sécurisé, vous devez y installer le serveur de gestion (IVMgr). Dans le cas contraire et si le domaine sécurisé contient déjà un serveur de gestion, vous ne devez pas en installer un autre. Un domaine sécurisé ne doit contenir qu'un seul serveur de gestion.

Informations requises avant l'installation

Avant de lancer l'installation de Policy Director, notez les informations système dont vous avez besoin.

Serveurs Policy Director

- Nom d'utilisateur de l'administrateur de cellule (cell_admin)
- Mot de passe de l'administrateur de cellule (cell_admin)
- WebSEAL : port HTTP (par défaut)
- WebSEAL : répertoire racine des documents Web

Client NetSEAT (Windows uniquement)

- Nom de la cellule
- Nom d'hôte du serveur de sécurité
- Nom d'hôte du serveur calendaire
- Nom d'hôte du répartiteur des services de répertoire

Processus de transmission par tunnel

Policy Director prend en charge les protocoles suivants pour la transmission des données codées :

- Transmission par tunnel SSL (Secure Sockets Layer)
- Transmission par tunnel GSS (Generic Security Service)

WebSEAL prend en charge les systèmes de protection d'intégrité et de confidentialité des données par tunnel chiffré SSL. WebSEAL et NetSEAL prennent en charge les appels de processus à distance (RPC). L'utilisation des systèmes d'intégrité et des horodates avec RPC offre une protection contre les *tentatives de lecture non autorisées*. Lors de ces tentatives de détournement par relecture, les données d'un utilisateur sont interceptées entre le client de l'utilisateur et le serveur. Le fraudeur va ensuite relire ces données ou les retransmettre au serveur afin de se substituer à l'utilisateur légitime.

Transmission par tunnel SSL : Le protocole SSL permet l'échange de signaux visant à établir une communication entre deux stations de travail. Ce protocole assure la sécurité et la confidentialité des données échangées sur l'Internet. SSL fonctionne avec une clé publique pour l'authentification et une clé secrète pour le chiffrement des données transmises via la connexion SSL.

Activez SSL pour utiliser la transmission par tunnel SSL avec les modules de Policy Director NetSEAL. Cette configuration s'applique lorsque le client NetSEAT sert de client SSL à un serveur Policy Director NetSEAL protégeant des ports définis, tel que celui utilisé par Telnet.

Policy Director WebSEAL gère SSL version 2 et 3.

Transmission par tunnel GSS : L'interface GSS (API GSS) est un moyen conventionnel pour permettre aux applications d'accéder aux services de sécurité. La transmission par tunnel GSS s'utilise en lieu et place des appels RPC sécurisés. Activez cette option si vous installez le client NetSEAT comme module de support pour Policy Director pour Windows NT ou pour la console de gestion de Policy Director.

La transmission par tunnel GSS apporte des services de sécurité génériques aux programmes appelants. Ce système repose sur un certain nombre de technologies et de mécanismes sous-jacents. Il permet de migrer des

applications vers différents environnements. La transmission par tunnel GSS permet de contrôler le niveau de protection des transactions dans les deux sens de la communication, indépendamment de ce sens. Par exemple, les données circulant du client vers le serveur peuvent être totalement protégées par un chiffrement global tandis que celles transitant dans l'autre sens peuvent ne pas être protégées.

Composants à installer pour le domaine sécurisé

Policy Director est un système de sécurité distribuée dont les composants peuvent être installés selon diverses configurations, sur un ou plusieurs ordinateurs. La liste qui suit indique les composants qui doivent être installés dans le domaine sécurisé.

- Services DCE
- Registre des utilisateurs (installez IBM SecureWay Directory uniquement si vous voulez utiliser le registre des utilisateurs LDAP)
- Serveurs Policy Director
- Console de gestion de Policy Director
- Kit de développement Authorization ADK

Si vous partez d'une configuration DCE ou LDAP existante, vérifiez qu'elle est au niveau requis. Reportez-vous à la section «Autres logiciels requis» à la page 16 pour plus d'informations sur ce sujet. Prenez connaissance des interdépendances existantes avant d'installer Policy Director.

Services DCE

Chaque domaine (cellule du DCE) sécurisé par Policy Director nécessite une installation complète des services de DCE, sur au moins une machine, pour assurer la sécurité des communications entre les serveurs Policy Director. Les services du DCE peuvent résider sur le même hôte que les serveurs Policy Director ou sur un système hôte distant relié au réseau.

Pour plus d'informations sur l'installation du DCE, reportez-vous aux manuels couvrant l'installation et l'administration de votre plate-forme ainsi qu'aux ressources de support technique disponibles. Reportez-vous à la section «Documentation sur IBM Distributed Computing Environment (DCE)» à la page 90 pour obtenir la liste des documents relatifs au DCE.

Respectez les recommandations suivantes lors de l'installation du DCE :

- Si vous créez un nouveau domaine sécurisé Policy Director sur un unique système hôte, faites une installation complète du serveur DCE.
- Si les serveurs DCE résident sur un système hôte distant, créez un nouveau domaine sécurisé en installant Policy Director sur un hôte local.
- Si vous installez Policy Director pour Windows NT dans un domaine sécurisé Policy Director existant, utilisez le client NetSEAT pour l'accès aux

services DCE. Installez le client NetSEAT sur le même système hôte que les serveurs Policy Director pour Windows NT.

Registre des utilisateurs

Policy Director peut utiliser au choix le registre des utilisateurs d'IBM SecureWay Directory (LDAP) ou celui de l'environnement informatique partagé (DCE).

Pour utiliser le registre des utilisateurs LDAP, vous devez installer et configurer un serveur LDAP avant d'installer Policy Director. Vous devez également installer un client LDAP sur chaque machine où réside Policy Director.

Reportez-vous au manuel *IBM SecureWay Directory version 3.1.1 - Installation et configuration* pour plus d'informations sur l'installation de LDAP. Reportez-vous à la section «Documentation du produit IBM SecureWay Directory» à la page 92 pour connaître l'emplacement de ce document.

Pour plus d'informations sur l'installation du DCE, reportez-vous aux documents indiqués dans la section «Documentation sur IBM Distributed Computing Environment (DCE)» à la page 90.

Serveurs Policy Director

L'installation des serveurs de Policy Director requiert les conditions suivantes :

- Pour communiquer correctement tous les serveurs Policy Director pour Windows NT ont besoin du client Policy Director NetSEAT.
- Toute installation d'un serveur Policy Director déclenche l'installation automatique du module de base.
- S'il s'agit du *premier* ou du *seul* ordinateur du domaine sécurisé, vous devez y installer le serveur de gestion.
- Dans le cas contraire et si le domaine sécurisé contient déjà un serveur de gestion, vous ne devez pas en installer un autre. Un domaine sécurisé ne doit contenir qu'une seule instance du serveur de gestion.
- WebSEAL, NetSEAL et le serveur d'autorisations tiers sont des composants optionnels.
- Le gestionnaire de sécurité s'associe à WebSEAL pour gérer le composant serveur HTTP WebSEAL et le contrôle d'accès avancé, et à NetSEAL pour gérer le contrôle d'accès TCP/IP standard.
- Tous les serveurs Policy Director pour AIX et Solaris nécessitent d'installer un client DCE complet et, si vous comptez utiliser le registre des utilisateurs LDAP, un client LDAP.

Console de gestion

La console de gestion nécessite d'installer et de configurer le domaine sécurisé et le serveur de gestion. La console de gestion a également besoin d'un client DCE et, dans le cas d'une machine Windows, du client NetSEAT.

Kit de développement Authorization ADK

Le kit de développement d'applications d'autorisation de Policy Director doit être installé sur la machine dédiée au développement d'applications. Ce kit de développement permet de créer des applications servant à autoriser les utilisateurs à accéder à des serveurs tiers protégés. Le module de base de Policy Director s'installe automatiquement en même temps que le kit de développement Authorization ADK.

Le domaine sécurisé dans lequel l'application est exécutée doit contenir au moins un serveur d'autorisations. Un environnement de développement standard comprend le serveur d'autorisations et, sur le même système, le kit de développement Authorization ADK.

Etapes de l'installation de Policy Director

L'installation de Policy Director se décompose de la manière suivante :

1. Si vous disposez d'une version antérieure d'IBM SecureWay Policy Director que vous voulez mettre à niveau, reportez-vous aux informations relatives à la migration dans la page Web consacrée à ce sujet (voir la section «Informations disponibles sur le Web» à la page x).
2. Vérifiez que votre système d'exploitation est adapté à Policy Director.

   Reportez-vous à la section «Serveurs Policy Director» à la page 16 pour plus d'informations sur les systèmes d'exploitation pris en charge.
3. Déterminez les composants correspondant à vos besoins et identifiez les ordinateurs que vous utiliserez pour les installer.

   Reportez-vous à la section «Configurations standard» à la page 19 pour obtenir une aide.
4. Choisissez si votre domaine sécurisé utilisera la transmission par tunnel SSL ou GSS.

   Reportez-vous à la section «Processus de transmission par tunnel» à la page 22 pour plus d'informations.
5. Installez et configurez une infrastructure de DCE s'il n'en existe pas déjà une.

   Reportez-vous à la section «Services DCE» à la page 23 pour plus d'informations sur les services de DCE obligatoires.
6. Choisissez si votre domaine sécurisé utilisera un registre des utilisateurs LDAP ou DCE. Dans le cas du registre des utilisateurs d'IBM SecureWay Directory (LDAP), installez et configurez LDAP s'il n'est pas déjà présent.

Reportez-vous au «Chapitre 4. Installation et configuration d'IBM SecureWay Directory» à la page 29 pour plus d'informations sur l'installation de LDAP.

7. Installez les clients DCE et LDAP sur les ordinateurs devant héberger les serveurs de Policy Director.

   Pour plus d'informations sur l'installation du DCE, reportez-vous aux documents indiqués dans la section «Documentation sur IBM Distributed Computing Environment (DCE)» à la page 90.

8. Installez les composants des serveurs Policy Director.

   Selon la plate-forme et le système d'exploitation utilisés, reportez-vous au chapitre approprié pour la procédure d'installation. Ces chapitres sont les suivants :

   - «Chapitre 5. Installation de Policy Director pour Windows» à la page 45
   - «Chapitre 6. Installation de Policy Director pour AIX» à la page 59
   - «Chapitre 7. Installation de Policy Director pour Solaris» à la page 75

9. Configurez le service d'acquisition de droits d'accès (SAD) de Policy Director si vous prévoyez d'utiliser ce service pour l'authentification des certificats des clients.

   Reportez-vous à la section «Configuration du Service d'acquisition de droits d'accès» à la page 27 pour plus d'informations sur le SAD de Policy Director.

10. Installez la console de gestion.

    Selon la plate-forme et le système d'exploitation utilisés, reportez-vous au chapitre approprié pour la procédure d'installation. Ces chapitres sont les suivants :

    - Pour Windows NT, voir «Installation de la console de gestion sur Windows» à la page 53.
    - Pour AIX, voir la section «Installation de la console de gestion» à la page 71, si vous voulez utiliser le registre des utilisateurs du DCE, et la section «Configuration et démarrage de la console de gestion» à la page 63 pour utiliser le registre des utilisateurs LDAP.
    - Pour Solaris, voir «Installation de la console de gestion» à la page 86.

Mise à niveau de Policy Director

Si vous désirez réinstaller un module quelconque, supprimez préalablement l'ancien module avant d'installer le nouveau. Reportez-vous à la section «Suppression de Policy Director» à la page 72.

Configuration du Service d'acquisition de droits d'accès

Le service d'acquisition de droits d'accès (SAD) de Policy Director est un composant adaptable qui permet d'étendre les méthodes d'authentification prises en charge par WebSEAL.

Le SAD de Policy Director s'installe automatiquement. Pour utiliser ce SAD comme seul et unique service d'acquisition de droits d'accès, vous devez le configurer comme tel. Reportez-vous aux chapitres 2 et 13 du manuel *Policy Director - Guide d'administration* pour plus d'informations sur les principes et la configuration du SAD de Policy Director.

Chapitre 4. Installation et configuration d'IBM SecureWay Directory

Si vous prévoyez d'utiliser un registre des utilisateurs DCE, vous pouvez ignorer ce chapitre consacré à l'installation et la configuration d'BM SecureWay Directory (LDAP).

Au cours de l'installation de Policy Director, vous devez choisir si votre domaine sécurisé utilisera un registre des utilisateurs LDAP ou DCE.

- Si vous choisissez le registre LDAP, vous devez installer un client et un serveur IBM SecureWay Directory version 3.1.1 (LDAP), puis configurer le serveur LDAP avant d'installer Policy Director.
- Si vous utilisez SSL pour accéder au serveur LDAP, le client LDAP doit également être configuré.

Installation du serveur et du client LDAP

Policy Director nécessite d'installer un serveur LDAP si vous comptez utiliser le registre des utilisateurs LDAP.

Un serveur LDAP doit être installé sur au moins une machine du domaine sécurisé. Le client et le serveur LDAP sont fournis avec Policy Director. Vous pouvez les installer avant Policy Director ou utiliser ceux déjà installés s'ils sont au niveau requis.

Pendant l'installation de LDAP, sélectionnez l'option **SecureWay Directory et Client SDK**.

Reportez-vous au manuel *IBM SecureWay Directory version 3.1.1 - Installation et configuration* pour plus d'informations sur l'installation et la configuration de LDAP. Il existe une version de ce manuel au format HTML, pour chaque système d'exploitation pris en charge, dans le CD-ROM approprié. Reportez-vous à la section «Documentation du produit IBM SecureWay Directory» à la page 92 pour plus d'informations sur la documentation disponible.

Installation du client LDAP uniquement

Si vous comptez utiliser le registre des utilisateurs LDAP, vous devez installer un serveur LDAP sur chaque système qui contiendra Policy Director. Le client LDAP est fourni avec Policy Director. Installez le client LDAP avant d'installer Policy Director.

Pendant l'installation de LDAP, sélectionnez l'option **SecureWay Client SDK** dans le cas où le serveur LDAP a déjà été installé et configuré pour Policy Director.

Configuration du serveur LDAP

Si vous comptez utiliser le registre des utilisateurs LDAP, vous devez configurer le serveur LDAP avant d'installer le premier serveur Policy Director. Une fois le serveur LDAP configuré pour le premier système Policy Director, il n'est pas nécessaire de le reconfigurer si vous ajoutez des serveurs Policy Director supplémentaires.

Si vous activez l'accès SSL au niveau du serveur LDAP au cours de la configuration de celui-ci, vous devez copier une paire de clés de serveur et de client sur chaque nouveau système utilisant l'accès SSL. Reportez-vous à la section «Activation de l'accès SSL (optionnel)» à la page 34 pour plus d'informations.

Pour configurer le serveur LDAP, vous devez accomplir la procédure suivante pour chaque domaine sécurisé :

1. Ajoutez les suffixes nécessaires. Reportez-vous à la section «Ajout de suffixes » à la page 31.
2. Installez les objets et les attributs du système de sécurité. Reportez-vous à la section «Installation des objets et des attributs du système de sécurité» à la page 31.
3. Activez le contrôle d'accès au niveau du serveur LDAP. Reportez-vous à la section «Activation du contrôle d'accès sur le système LDAP» à la page 42.
4. Activez l'accès par SSL. Reportez-vous à la section «Activation de l'accès SSL (optionnel)» à la page 34.

Si vous avez activé l'accès par SSL, répétez la procédure de la section «Activation de l'accès SSL sur le client LDAP» à la page 39 chaque fois que vous ajoutez un nouveau client LDAP (serveur Policy Director) utilisant SSL pour accéder au serveur LDAP.

Remarque : L'administrateur du système LDAP peut spécifier les paramètres de codage des mots de passe dans la base de données de LDAP. LDAP permet de stocker les mots de passe sans codage, ce qui

peut induire des risques pour la sécurité. Reportez-vous à la documentation de votre système LDAP pour plus d'informations sur la définition des attributs des mots de passe et leur niveau de codage.

Ajout de suffixes

Dans le programme IBM SecureWay Directory, créez un nouveau suffixe de la manière suivante :

1. A l'aide d'un navigateur Web, accédez à l'utilitaire d'administration Web d'IBM SecureWay Directory à l'adresse suivante :

   `http://nom_serveur/ldap`

   Connectez-vous au site via l'interface Web, sous l'ID de l'administrateur LDAP (par exemple, `cn=root`).
2. Cliquez sur **Suffixes → Ajout d'un suffixe**.
3. Dans le champ **DN du suffixe**, entrez le suffixe choisi :

   `secAuthority=Default`

   L'objet correspondant à `secAuthority=Default` est créé durant la configuration du serveur de gestion.
4. Cliquez sur le bouton **Ajout d'un suffixe**.
5. Pour ajouter un autre suffixe, cliquez sur le lien **Ajout d'un suffixe** pour revenir à la fenêtre précédente.
6. Le cas échéant, ajoutez un suffixe pour vos utilisateurs Policy Director et pour les données GSO (Global Sign-On). Par exemple :

   `o=IBM,c=FR`

   Définissez des suffixes adaptés à votre installation. `o=` indique le nom abrégé de votre organisation et `c=` désigne son pays.

   Cette procédure génère les suffixes associés aux données GSO ainsi qu'aux utilisateurs et aux groupes de votre réseau. Ils sont créés par l'utilitaire d'administration Web de LDAP.
7. Cliquez sur le bouton **Ajout d'un suffixe**.
8. Répétez cette procédure pour chaque suffixe à ajouter.
9. Une fois l'ajout des suffixes terminé, cliquez sur le lien de **redémarrage du serveur**, dans la page Web de l'utilitaire d'administration de LDAP, pour redémarrer le serveur LDAP.

Installation des objets et des attributs du système de sécurité

Policy Director gère les droits d'accès des utilisateurs au niveau du serveur LDAP au moyen d'une série d'attributs et d'objets LDAP.

L'utilitaire IBM SecureWay Directory Management Tool (DMT) permet de déterminer si les objets et les attributs de sécurité sont installés ou non. Vous pouvez ensuite les installer dans le deuxième cas. L'utilitaire DMT s'installe en même temps que SecureWay Directory.

Pour déterminer si les objets et les attributs de sécurité de Policy Director sont installés ou non, procédez de la manière suivante :

1. Démarrez l'utilitaire Directory Management Tool sur un client LDAP.

   Remarque : Si un message vous indique qu'il n'existe aucune entrée pour le suffixe secAuthority=Default, vous pouvez continuer sans risque. L'objet correspondant au suffixe `secAuthority=Default` est créé durant la configuration du serveur de gestion.
2. Cliquez sur **Schéma → Classes d'objet → Affichage des classes d'objet**.
3. Vérifiez la présence de tous les objets et attributs de Policy Director suivants :

   Classes d'objets
   secAuthorityInfo
   secGroup
   secMap
   secPolicy
   secPolicyData
   secUser
4. Cliquez sur **Schéma → Attributs → Affichage des attributs**
5. Vérifiez la présence de tous les objets et attributs de Policy Director suivants :

   Attributs
   secUUID
   secLoginType
   secAuthority
   secAcctValid
   secPwdValid
   secDN
   secPwdMgmtBind
   secAcctExpires
   secAcctInactivity
   secAcctLife
   secPwdAlpha
   secPwdSpaces
   secPwdFailures
   secPwdLastChanged
   secPwdLastUsed

6. Exécutez l'une des opérations suivantes selon les résultats obtenus dans les étapes 3 à la page 32 et 5 à la page 32.
   - Si tous les objets requis sont présents, aucune autre action n'est nécessaire. Passez à la section «Activation de l'accès SSL (optionnel)» à la page 34.
   - Si *certains* objets sont présents et d'autres absents, passez à l'étape 7.
   - Si *aucun* objet n'est présent, passez à l'étape 8.
7. Si certains objets et attributs de Policy Director sont présents et d'autres absents, supprimez les objets et attributs existants.

   Dans l'utilitaire DMT, cliquez sur :

   Schéma → Classes d'objets → Suppression de classes d'objets et supprimez les classes d'objets.

   Ensuite, cliquez sur **Schéma → Attributs → Suppression d'attributs** et supprimez les attributs.
8. Si aucun des objets et attributs de Policy Director n'est présent, insérez le CD-ROM *IBM SecureWay Policy Director version 3.0* dans le lecteur approprié.
9. Entrez la commande **ldapmodify** sur une ligne de commande pour charger le fichier de la structure. Par exemple, tapez :

   UNIX :

   ```
   ldapmodify -h nom d'hôte -p 389 -D cn=root -w
   mot de passe -f /schema/secschema.def
   ```

   Windows :

   ```
   ldapmodify -h nom d'hôte -p 389 -D cn=root -w mot de passe -f
   x:\schema\secschema.def
   ```

   où *x:* désigne le lecteur de CD-ROM du système Windows.
10. Si vous prévoyez d'utiliser Policy Director pour gérer les utilisateurs de SecureWay Boundary Server, vous devez également ajouter les objets et les attributs contenus dans le fichier de la structure de Policy Director.

    Entrez la commande **ldapmodify** sur une ligne de commande pour charger le fichier de la structure. Par exemple, tapez :

    Windows :

    ```
    ldapmodify -h
    nom d'hôte -p 389 -D cn=root -w mot de passe -f x:\schema\puschema.def
    ```

    UNIX :

    ```
    ldapmodify -h
    nom d'hôte -p 389 -D cn=root -w mot de passe -f /schema/puschema.def
    ```

    où *x:* désigne le lecteur de CD-ROM du système.

Activation de l'accès SSL (optionnel)

Si vous n'avez pas besoin d'accéder au serveur LDAP par tunnel SSL, ignorez cette section. Passez à la section «Activation du contrôle d'accès sur le système LDAP» à la page 42.

Si votre serveur LDAP nécessite l'accès par SSL, lisez cette section. Cette procédure doit être accomplie lors de l'établissement de la première communication SSL entre le serveur LDAP et le client LDAP.

Vous pouvez, si vous le désirez, activer l'utilisation du protocole SSL pour protéger les communications entre les serveurs de Policy Director et le serveur LDAP.

Le produit IBM Global Security Kit (GSKit) SSL Runtime Toolkit version 3.0.1 s'installe en même temps que le système LDAP. GSKit propose deux versions de l'utilitaire de gestion des clés KMT (Key Management Tool) : une version avec fenêtres, **ikmguiw**, et l'autre sans, **ikmgui**. Vous pouvez utiliser l'une ou l'autre de ces versions lorsque **ikmguiw** est appelé par les procédures suivantes.

Les instructions d'emploi de cet utilitaire se trouvent dans la documentation du système LDAP. Reportez-vous à la section «Documentation du produit IBM SecureWay Directory» à la page 92.

Vous pouvez également suivre ces procédures pour activer l'accès SSL au niveau de Policy Director.

Création du fichier de la base de données des clés et du certificat

Pour activer le support du protocole SSL sur le serveur LDAP, celui-ci doit posséder un certificat attestant de son identité et utilisable comme *certificat personnel*. Le serveur envoie ce certificat personnel au client pour permettre à celui-ci de se faire authentifier par le serveur. Les certificats comme la paire de clés publique/privée sont stockés dans un fichier de base de données des clés. Généralement, un utilisateur se procure un *certificat signé* auprès d'une autorité de certification (AC) telle que VeriSign.

Vous pouvez également utiliser un *certificat auto-signé*. Dans ce cas, la machine sur laquelle ce certificat est créé joue le rôle de l'autorité de certification.

Utilisez l'utilitaire de gestion des clés de GSKit (**ikmguiw**) pour créer le fichier de la base de données des clés et le certificat. Procédez de la manière suivante (certificat signé ou auto-signé) :

1. Vérifiez que le produit IBM Global Security Kit (GSKit) SSL Runtime Toolkit version 3.0.1 et l'utilitaire Java Key Management Tool sont installés à la fois sur le serveur LDAP et sur tous les clients LDAP devant utiliser SSL.

Windows : `C:\Program Files\IBM\GSK\bin\ikmguiw.exe`

Solaris : `/opt/IBM/GSK/bin/ikmguiw`

AIX : `/usr/lpp/ibm/gsk/bin/ikmguiw`

2. Démarrez IBM Key Management Tool (**ikmguiw**).
3. Sélectionnez l'option de fichier de base de données clé, puis **Nouveau**.
4. Vérifiez que le type de base de données sélectionné est un fichier de base de données clé CMS.
5. Entrez les renseignements requis dans les champs correspondant au nom de fichier et à l'emplacement pour définir le nom et l'emplacement du fichier de la base de données des clés. L'extension d'un fichier de base de données des clés est *.kdb*.
6. Cliquez sur **OK**.
7. Entrez le mot de passe du fichier de la base de données des clés et confirmez-le.

   N'oubliez ce mot de passe, qui vous sera demandé chaque fois que vous voudrez modifier le fichier de la base de données des clés.
8. Acceptez ou modifiez le délai d'expiration par défaut selon les besoins de votre organisation.
9. Si vous désirez masquer le mot de passe et le stocker dans un fichier caché, sélectionnez l'option permettant de cacher le mot de passe dans un fichier.

   L'utilisation d'un fichier caché dispense les applications d'avoir à connaître le mot de passe du fichier de la base de données des clés pour l'utiliser. Le fichier caché réside au même emplacement que le fichier de la base de données des clés et possède l'extension *.sth*.
10. Cliquez sur **OK**.

Le fichier de la base de données des clés a été créé. Vous possédez également un jeu de certificats d'AC par défaut. Ces certificats d'AC définissent les autorités de certification reconnues par défaut.

Création d'un certificat personnel

Si vous désirez utiliser un certificat délivré par une autorité de certification (par exemple, VeriSign), vous devez le lui demander pour le recevoir. Exécutez la procédure détaillée dans la section «Réception du certificat ».

Réception du certificat : Si vous utilisez un certificat délivré par une autorité de certification (par exemple, par VeriSign) au lieu d'un certificat auto-signé, exécutez la procédure suivante :

1. Utilisez la commande **ikmguiw** pour demander un certificat à une autorité de certification. Une fois reçu, ce certificat sera stocké dans le fichier de la base de données des clés.
2. Cliquez sur l'option de demandes de certificats personnels.

3. Sélectionnez **Nouveau**.
4. Entrez tous les renseignements dans la requête à adresser à l'autorité de certification.
5. Cliquez sur **OK**.
6. Une fois le certificat renvoyé par l'AC, pour le copier dans le fichier de la base de données des clés, cliquez sur les certificats personnels, puis sur l'option de réception.
7. Lorsque le certificat du serveur LDAP a été copié dans le fichier de la base de données des clés, vous pouvez configurer ce serveur de manière à activer les communications SSL.

Si le certificat du serveur LDAP n'est pas reconnu, copiez le certificat de l'autorité de certification sur la machine du client.

Si le certificat est délivré par une AC reconnue (par exemple VeriSign), aucune autre action n'est nécessaire. Passez à la section «Activation de SSL sur le serveur LDAP» à la page 38.

Création d'un certificat auto-signé : Si vous désirez utiliser un certificat délivré par une autorité de certification (par exemple, VeriSign), au lieu d'un certificat auto-signé, reportez-vous à la section «Réception du certificat » à la page 35.

Pour créer un certificat auto-signé et le stocker dans le fichier de la base de données des clés :

1. Sélectionnez l'option de création, puis l'option correspondant au nouveau certificat auto-signé.
2. Entrez un nom dans le champ de libellé de clé. GSKit s'en servira pour identifier le nouveau certificat dans la base de données des clés.

   Par exemple, cette étiquette peut refléter le nom de la machine du serveur LDAP.
3. Acceptez les valeurs par défaut contenues dans les champs correspondant à la version (X.509 V3) et à la taille de la clé.
4. Validez le nom de machine par défaut ou entrez un autre DN dans le champ de nom commun.
5. Entrez le nom de votre société dans le champ de l'entreprise.
6. Renseignez les champs optionnels ou laissez-les vides.
7. Acceptez les valeurs par défaut des champs relatifs au pays et à la période de validité (365 jours) ou entrez des valeurs correspondant à votre situation.
8. Cliquez sur **OK**.

   GSKit crée une paire de clés publique/privée et le certificat associé.

Si le fichier de la base de données des clés contient plusieurs certificats personnels, GSKit vous demande si vous voulez faire de cette clé le certificat par défaut. Vous pouvez ainsi choisir l'un des certificats comme certificat par défaut. Ce certificat par défaut sera utilisé au moment de l'exécution si vous n'en spécifiez pas un autre.

Le certificat personnel du serveur LDAP a été créé. Il doit apparaître dans la section des certificats personnels du fichier de la base de données des clés. Utilisez la barre centrale de l'utilitaire KMT pour sélectionner un type de certificat parmi ceux contenus dans le fichier de la base de données des clés.

Vous devez ensuite convertir le certificat du serveur LDAP en un fichier de données ASCII codé en base 64.

Extraction du certificat auto-signé

Si vous utilisez un certificat auto-signé, vous devez extraire le certificat du signataire du fichier de la base de données des clés. Passez à la procédure d'extraction.

Cette extraction permet de configurer la machine du client. Si vous avez créé un certificat auto-signé comme décrit dans la section «Création d'un certificat auto-signé » à la page 36, ce certificat apparaît aussi dans la section des certificats du signataire du fichier de la base de données des clés. Vérifiez que ce nouveau certificat apparaît bien dans cette section.

Pour extraire le certificat du signataire :

1. Utilisez la commande **ikmguiw** pour convertir le certificat du serveur LDAP en un fichier de données ASCII codé en base 64. Ce fichier sera utilisé au cours de la procédure décrite dans la section «Activation de l'accès SSL sur le client LDAP» à la page 39.
2. Mettez en évidence le certificat auto-signé créé au cours de la section «Création d'un certificat auto-signé » à la page 36.
3. Cliquez sur l'option d'extraction de certificat.
4. Sélectionnez le type de données ASCII codées en base 64.
5. Entrez le nom du certificat que vous venez d'extraire. L'extension du fichier du certificat est *.arm*.
6. Entrez l'emplacement où vous voulez stocker le certificat extrait.
7. Cliquez sur **OK**.
8. Copiez ce certificat sur la machine du client LDAP.
9. Vous pouvez maintenant activer les communications SSL au niveau du serveur LDAP.

Activation de SSL sur le serveur LDAP

Pour activer les communications SSL au niveau du serveur LDAP :

1. Vérifiez que le serveur LDAP est installé et actif si vous prévoyez d'utiliser le registre des utilisateurs LDAP. Reportez-vous au «Chapitre 4. Installation et configuration d'IBM SecureWay Directory» à la page 29.
2. Utilisez l'utilitaire Web d'administration de LDAP. Entrez l'adresse URL suivante :

   ```
   http://nom_serveur/ldap
   ```

   La valeur de *nom_serveur* désigne le nom de la machine du serveur LDAP.
3. Connectez-vous au site sous l'ID de l'administrateur de LDAP (par exemple, cn=root) si vous ne l'êtes pas déjà.
4. Cliquez sur **Serveur → SSL**.
5. Selon l'état que vous voulez définir pour SSL, cliquez au choix sur **SSL activé** (activation des transmissions SSL et non SSL) ou sur **SSL uniquement**.
6. Cliquez sur **Authentification de serveur** pour choisir la méthode d'authentification utilisée.
7. Entrez un numéro de port ou acceptez le numéro de port par défaut (636).
8. Entrez le nom et le chemin du fichier de la base de données des clés créé à l'étape 5 de la section Création du fichier de la base de données des clés et du certificat.

   L'extension du fichier de base de données des clés est *.kdb*.
9. Entrez dans le champ relatif au libellé de la clé l'étiquette utilisée pour identifier le certificat du serveur LDAP dans la base de données des clés. Par exemple, cette étiquette peut refléter le nom de la machine du serveur LDAP.
10. Entrez le mot de passe du fichier de la base de données des clés et confirmez-le. Laissez vide le champ du mot de passe si vous voulez que le serveur LDAP utilise le fichier caché.
11. Cliquez sur le bouton d'application.
12. Cliquez sur le lien de **redémarrage du serveur** pour relancer le serveur LDAP et activer les modifications.

Test de l'accès SSL : Pour vérifier que le protocole SSL a bien été activé, entrez la commande suivante sur la ligne de commande du serveur LDAP :

```
ldapsearch -h nom du serveur -Z -K fichier des
clés -P mot de passe -b "" -s base \
objectclass=*
```

Entrez une barre oblique inversée (\) si la commande occupe plus d'une ligne.

Où :

Option	Description
nom du serveur	Nom d'hôte DNS du serveur LDAP.
fichier des clés	Nom de chemin complet du fichier de l'anneau de clés généré.
mot de passe	Mot de passe du fichier de l'anneau de clés généré.

Cette commande renvoie les données de base du serveur LDAP, notamment ses suffixes.

Le protocole SSL est à présent activé au niveau du serveur LDAP. Vous devez à présent l'activer sur le client LDAP.

Activation de l'accès SSL sur le client LDAP

Une fois le protocole SSL activé sur le serveur LDAP, vous devez faire de même au niveau du client LDAP.

Création d'un fichier de base de données des clés : Vérifiez que GSKit est installé sur le client, puis créez le fichier de la base de données des clés à l'aide de l'utilitaire de gestion des clés IBM KMT, comme indiqué dans la section «Création du fichier de la base de données des clés et du certificat» à la page 34.

Pour que le client puisse authentifier le serveur LDAP, il doit reconnaître l'autorité de certification (le signataire) ayant créé le certificat de ce serveur. Si le serveur LDAP utilise un certificat auto-signé, le client doit être configuré de manière à pouvoir reconnaître la machine ayant généré le certificat de ce serveur comme une autorité racine sécurisée (une autorité de certification).

Ajout d'un certificat d'AC : Pour ajouter un certificat d'AC dans le fichier de la base de données des clés :

1. Vérifiez que le certificat extrait du fichier de la base de données des clés dans la section «Extraction du certificat auto-signé» à la page 37 a été copié sur la machine du client. Copiez-le si besoin.
2. Sélectionnez la section des certificats du signataire du fichier de la base de données des clés CMS du client.
3. Cliquez sur le bouton d'ajout.
4. Sélectionnez le type de données ASCII codées en base 64.
5. Indiquez le nom et l'emplacement du fichier du certificat. L'extension du fichier du certificat est *.arm*.
6. Cliquez sur **OK**.

7. Entrez l'étiquette du certificat d'AC que vous êtes en train d'ajouter. Par exemple, cette étiquette peut refléter le nom de la machine du serveur LDAP.
8. Cliquez sur **OK**.

   Le certificat auto-signé apparaît dans la base de données des clés du client sous la forme d'un certificat d'AC.
9. Mettez en évidence le certificat d'AC que vous venez d'ajouter, puis cliquez sur l'option de visualisation et d'édition.
10. Pour valider sa qualité de certificat d'AC, vérifiez que l'option de définition du certificat en tant que racine sécurisée est sélectionnée.

    Si le certificat du serveur LDAP a été créé par une autorité de certification conventionnelle, vérifiez que cette AC est associée à un certificat d'AC et qu'elle est répertoriée comme racine sécurisée. Dans le cas contraire, ajoutez le certificat de l'autorité de certification en qualité de certificat d'AC et indiquez qu'il s'agit d'une autorité racine sécurisée.

A ce stade, le client doit pouvoir établir une connexion SSL avec le serveur LDAP.

Test de l'activation de SSL : Pour vérifier que le protocole SSL a bien été activé, entrez la commande suivante sur la ligne de commande du client LDAP :

```
ldapsearch -h nom de serveur -Z -K fichier des clés
du client -P mot de passe -b "" \
-s base objectclass=*
```

Entrez une barre oblique inversée (\) si la commande occupe plus d'une ligne.

Où :

Option	Description
nom du serveur	Nom d'hôte DNS du serveur LDAP.
fichier des clés du client	Nom de chemin complet du fichier de l'anneau de clés généré.
mot de passe	Mot de passe du fichier de l'anneau de clés généré.

Cette commande renvoie les données de base du serveur LDAP, notamment ses suffixes.

Le protocole SSL est à présent activé au niveau du client LDAP.

Configuration de la méthode d'authentification du client et du serveur LDAP (optionnel)

Cette procédure de configuration est facultative.

1. Exécutez la procédure décrite dans la section «Activation de SSL sur le serveur LDAP» à la page 38. Toutefois, pour le serveur LDAP, au lieu de l'option **Authentification de serveur**, choisissez **Authentification du serveur et du client**.

   Dans ce cas de figure, lorsque le serveur a envoyé au client son certificat et s'est fait authentifier, il demande en retour le certificat du client. Si le serveur LDAP a été configuré dans ce sens, un certificat doit être créé pour la machine du client.
2. La création d'un certificat pour la machine du client se fait selon les procédures décrites dans les sections suivantes :
   - «Création du fichier de la base de données des clés et du certificat» à la page 34
   - «Création d'un certificat auto-signé » à la page 36 dans le cas d'un certificat auto-signé, ou «Réception du certificat » à la page 35 s'il s'agit d'un certificat d'AC.
   - «Extraction du certificat auto-signé» à la page 37
   - «Activation de SSL sur le serveur LDAP» à la page 38
3. Au niveau du serveur LDAP, une fois le certificat personnel du client créé et ajouté au fichier de la base de données des clés de celui-ci, l'autorité de certification ayant créé ce certificat doit être reconnue comme une autorité racine sécurisée. Le certificat de l'autorité de certification est ajouté à la base de données des clés du serveur LDAP comme décrit dans la section «Ajout d'un certificat d'AC » à la page 39.

Test de l'accès SSL : A présent que l'autorité de certification ayant créé le certificat personnel du client est reconnue par le serveur LDAP, la configuration peut être testée à l'aide de la commande suivante :

```
ldapsearch -h nom de serveur -Z -K fichier des clés du client
-P mot de passe -N étiquette du client \
-b "" \ -s base objectclass=*
```

Entrez une barre oblique inversée (\) si la commande occupe plus d'une ligne.

Où :

Option	Description
nom du serveur	Nom d'hôte DNS du serveur LDAP.
fichier des clés du client	Nom de chemin complet du fichier de l'anneau de clés généré pour le client.
mot de passe	Mot de passe du fichier de l'anneau de clés généré.

étiquette du client	Etiquette associée à la clé, le cas échéant. Ce champ ne doit être renseigné que dans le cas où le serveur LDAP a été configuré pour l'authentification du client et du serveur.

Cette commande renvoie les données de base du serveur LDAP, notamment ses suffixes. Notez que le paramètre **-N** indique l'étiquette spécifiée lors de l'ajout du certificat personnel du client dans sa base de données des clés.

Ne spécifiez pas l'étiquette du certificat d'AC du serveur LDAP. Le paramètre **-N** indique à GSKit quel certificat le client enverra au serveur lorsque celui-ci le demandera. Faute d'étiquette spécifiée, lorsque le serveur demande son certificat au client, celui-ci lui envoie son certificat personnel par défaut.

La configuration du protocole SSL est à présent terminée.

Activation du contrôle d'accès sur le système LDAP

Pour terminer l'intégration de la solution de sécurité Policy Director avec le registre des utilisateurs LDAP, vous devez mettre à jour les listes de contrôle d'accès de LDAP. Procédez de la manière suivante :

1. Lancez l'utilitaire Directory Management Tool (DMT) à partir du client LDAP ou du serveur LDAP. Cliquez sur **Démarrer → Programmes → IBM SecureWay Directory → Directory Management Tool**.
2. Reconnectez le serveur :
   a. Cliquez sur **Serveur → Reconnexion**.
   b. Cliquez sur **Authentifié**.
   c. Tapez le DN de l'utilisateur (par exemple, cn=root).
   d. Tapez votre mot de passe.
   e. Cliquez sur **OK**.
3. Cliquez sur **OK** ou fermez la fenêtre chaque fois qu'un message d'avertissement apparaît.
4. Donnez au groupe des démons de sécurité de Policy Director le contrôle total des suffixes créés dans la section «Ajout de suffixes » à la page 31.
   a. Cliquez sur **Entrées → Ajout d'une entrée**.
   b. Entrez le suffixe de la base de données des utilisateurs Policy Director et des utilisateurs GSO dans le champ **Nom distinctif relatif de l'entrée**. Par exemple :

      ```
      o=IBM,c=FR
      ```

   c. Cliquez sur **Organisation**.
   d. Cliquez sur **Suivant**.

      La fenêtre de création des entrées LDAP apparaît.

e. Ajoutez les renseignements décrivant votre société, puis cliquez sur le bouton **Création**.

f. Cliquez sur **Arborescence → Régénération de l'arborescence**. La nouvelle entrée doit apparaître dans l'arborescence des répertoires.

5. Donnez au groupe des démons de sécurité de Policy Director le contrôle total du système LDAP. Pour cela ajoutez la ligne suivante à la liste des propriétaires de chaque LCA contrôlant LDAP :

   ```
   cn=SecurityGroup,secAuthority=Default
   ```

   après avoir cliqué sur l'onglet **LCA**.

   La fenêtre d'édition des LCA de LDAP apparaît.

   a. Tapez `cn=SecurityGroup,secAuthority=Default` dans le champ DN, puis cliquez sur **group** dans la liste déroulante.

   b. Cliquez sur le bouton **Ajout**.

   c. Sélectionnez toutes les cases à cocher placées sous Droits accordés pour les options Ajout, Suppression et Classe.

   d. Cela fait, cliquez sur **Modification**. La ligne `cn=SecurityGroup,secAuthority=Default` doit apparaître dans la liste des LCA appliquées au DN de votre suffixe.

   e. Répétez cette procédure pour chaque nouveau suffixe à ajouter à la liste des propriétaires.

La configuration de LDAP est à présent terminée.

Chapitre 5. Installation de Policy Director pour Windows

Ce chapitre décrit comment installer et configurer Policy Director sur les plates-formes Windows et Windows NT.

Avant de lancer l'installation de Policy Director, lisez attentivement les informations contenues dans la section «Avant d'installer Policy Director pour Windows».

Avant d'installer Policy Director pour Windows

Avant de lancer l'installation de NetSEAT et de Policy Director, lisez les informations suivantes :

- Avant d'installer NetSEAT et Policy Director, vous devez installer et configurer le serveur Windows NT.
- Vous devez connaître les mots de passe de l'administrateur du domaine Windows NT et de l'administrateur du domaine sécurisé (par exemple, cell_admin). Prenez soin d'obtenir les privilèges d'administrateur nécessaires.
- Si vous créez une nouvelle cellule de DCE à l'occasion de l'installation des serveurs de Policy Director sur le système d'exploitation Windows NT :
  - Vous devez également installer et configurer un serveur DCE.
  - Si vous comptez utiliser le registre des utilisateurs LDAP, vous devez installer et configurer un serveur LDAP.
- Lisez toutes les informations relatives à la mise en oeuvre de Policy Director, contenues dans la section «Composants à installer pour le domaine sécurisé» à la page 23.

Installation de NetSEAT et de Policy Director

Avant de lancer l'installation de Policy Director, fermez toutes les applications actives. Vous devrez arrêter puis redémarrer le système une fois Policy Director installé.

Inventaire du domaine sécurisé

Au cours de l'installation, vous devez fournir les renseignements suivants sur la configuration de votre domaine sécurisé :

- Le nom de votre domaine sécurisé (cellule de DCE), par exemple cell_admin
- Le nom des ordinateurs fournissant les services suivants :
  - Sécurité
  - Heure
  - Services des répertoires de cellule (SRC)
  - Répartiteur des services de répertoire (RSR)

Installation de NetSEAT

Le fichier de configuration de Policy Director NetSEAT copie les fichiers de NetSEAT sur votre disque dur, puis démarre automatiquement l'assistant de configuration de NetSEAT.

Pour installer NetSEAT :

1. Connectez-vous au système sous un ID avec privilèges d'administrateur.
2. Insérez le CD-ROM intitulé *IBM SecureWay Policy Director version 3.0* dans le lecteur de CD-ROM.
3. Passez dans le répertoire \win32\client.
4. Cliquez deux fois sur le fichier setup.exe pour lancer le programme InstallShield.
5. Sélectionnez la langue de travail désirée dans la fenêtre de sélection des langues.
6. Cliquez sur **Suivant** dans la fenêtre d'accueil de Policy Director.
7. Cliquez sur **Suivant**.
8. Dans la fenêtre de sélection des composants à installer, cliquez sur **Client des applications serveur Policy Director**.
9. Cliquez sur **Suivant**.
10. Dans la fenêtre de sélection du type d'installation, cliquez sur **Standard**.

    L'emplacement défini par défaut pour une installation standard est :

    ```
    c:\Program Files\ibm\netseat\
    ```

    Si vous cliquez sur **Personnalisée**, indiquez l'unité sur laquelle vous voulez installer NetSEAT.

    La fenêtre de sélection des emplacements apparaît.
11. Cliquez sur **Suivant**.

    Les fichiers de NetSEAT se copient à l'emplacement défini par défaut sur votre disque dur. La fenêtre de configuration de NetSEAT apparaît.

Configuration de NetSEAT

Les tâches de configuration fournissent à NetSEAT des informations sur le domaine sécurisé, par exemple le nom des serveurs du DCE, leurs emplacements et les services qu'ils dispensent.

Une fois tous les fichiers de NetSEAT copiés sur votre disque dur, la fenêtre de configuration de NetSEAT apparaît (onglet **Domaines sécurisés**).

Pour configurer NetSEAT :

1. Pour ajouter l'entrée d'un nouveau domaine sécurisé, cliquez sur **Ajout**.

   La fenêtre Nouveau domaine sécurisé apparaît.
2. Tapez le nom du domaine sécurisé (cellule de DCE) auquel NetSEAT va appartenir (par exemple, cell_admin).
3. Sélectionnez au choix la case à cocher **Activer GSS** ou **Activer SSL**.
4. Cliquez sur **OK**.

   La fenêtre Propriétés du domaine sécurisé apparaît à l'écran.
5. Pour ajouter un serveur DCE et ses services, cliquez sur **Ajout**.

   La fenêtre Ajout d'un serveur DCE apparaît.

   Cette fenêtre permet d'indiquer à NetSEAT les serveurs DCE existant dans le domaine sécurisé et les services qu'ils dispensent. Vous pouvez être amené à ajouter ainsi plusieurs serveurs DCE. Tous les services peuvent résider sur une seule machine ou sur plusieurs.

   Les situations possibles sont les suivantes :

   - **Nouveau domaine sécurisé (un seul système hôte)**

     Si vous créez un domaine sécurisé ne comportant qu'un seul système hôte, celui-ci doit héberger tous les services du DCE. Entrez le nom de ce système hôte dans le champ **Nom de la machine**. Sélectionnez un ou plusieurs services. Sélectionnez le répartiteur des services de répertoire même si vous ne l'avez pas encore installé.
   - **Nouveau domaine sécurisé (plusieurs systèmes hôtes)**

     Si vous créez un domaine sécurisé et que les services du DCE sont localisés sur un autre système hôte, l'hôte local n'hébergera que les services du répartiteur des services de répertoire. Dans ce cas, ajoutez d'abord le serveur DCE chargé des services de DCE (Sécurité, Heure et SRC). Ajoutez ensuite un autre serveur DCE (nommé `hôte_local`) pour représenter le système local, puis sélectionnez la case à cocher du RSR. Vous pouvez sélectionner le répartiteur des services de répertoire même si vous ne l'avez pas encore installé.
   - **Domaine sécurisé existant**

     Si vous installez Policy Director dans un domaine sécurisé existant, ajoutez le nom du serveur DCE chargé des services Sécurité, Heure et SRC. Ajoutez ensuite le nom du serveur DCE hébergeant le serveur de

gestion de Policy Director qui installe automatiquement le répartiteur des services de répertoire. Sélectionnez la case à cocher du RSR pour ce système. Dans cette situation, tous les services, le RSR compris, doivent être localisés sur le même système hôte.

6. Pour chaque serveur, entrez le DN complet de la machine d'un serveur existant dans le domaine sécurisé (par exemple, SFF98732.austin.ibm.com).
7. Pour chaque serveur, sélectionnez un ou plusieurs de ces services :
   - Sécurité
   - RSR
   - Heure
   - SRC
8. Cliquez sur **OK**.

   La fenêtre Propriétés du domaine sécurisé affiche la nouvelle entrée.
9. Répétez les étapes 5 à la page 47 à 8 pour ajouter des serveurs et des services supplémentaires.
10. Dans la fenêtre Propriétés du domaine sécurisé, acceptez la configuration de connexion avancée par défaut représentée par l'option **ID DCE uniquement**.

    La zone de la connexion intégrée dans la fenêtre Propriétés du domaine sécurisé n'est pas utilisée pour l'installation de NetSEAT.
11. Cliquez sur **OK**.

    La fenêtre de configuration de NetSEAT apparaît.
12. Cliquez sur **OK**.

    La fenêtre de redémarrage du système apparaît.
13. Cliquez sur **Oui** pour redémarrer l'ordinateur.
14. Cliquez sur **OK**.

    NetSEAT redémarre automatiquement en même temps que l'ordinateur. Une icône NetSEAT apparaît dans la barre des tâches de Windows.

    L'installation et la configuration de NetSEAT sont à présent terminées.

Vérification de la configuration du client NetSEAT

Avant d'installer le serveur Policy Director, vérifiez que le client NetSEAT est configuré comme il convient dans le domaine sécurisé spécifié. Vous pouvez utiliser **netseat_ping** pour savoir si les services suivants sont disponibles :

- Service de sécurité
- Service horaire
- Service de répertoire de cellules
- Répartiteur des services de répertoire

Pour vérifier que le client NetSEAT peut communiquer avec ces services, procédez de la manière suivante :

1. Cliquez sur **Démarrer → Programmes → NetSEAT → Connexion NetSEAT**, puis connectez-vous sous l'ID de cell_admin.

   Vous pouvez aussi entrer la commande **netseat_login** sur la ligne de commande pour vous connecter.
2. Ne sélectionnez pas l'option ID PKI, sauf si votre configuration le nécessite.
3. Entrez le nom d'utilisateur et le mot de passe de l'administrateur de Policy Director.
4. Cliquez sur **OK**.
5. Sur la ligne de commande, entrez la commande **netseat_ping** pour afficher l'état de la configuration.

   Par exemple, dans le cas d'un client NetSEAT configuré dans un domaine sécurisé appelé "redback", entrez la commande suivante à l'invite de commande DOS :

   ```
   netseat_ping -C redback
   ```

   La sortie ressemble à ceci :

   ```
   /.../redback:
          SecurityServers:
                       ncacn_ip_tcp:redback[ ] est disponible
                       ncadg_ip_udp:redback[ ] est disponible
          CdsServers:
                       ncacn_ip_tcp:redback[ ] est disponible
                       ncadg_ip_udp:redback[ ] est disponible
          TimeServers:
                       ncacn_ip_tcp:redback[ ] est disponible
                       ncadg_ip_udp:redback[ ] est disponible
          DsbServers:
                       ncacn_ip_tcp:redback[ ] non disponible
                       ncacn_ip_udp:redback[ ] non disponible
   ```

   Notez que le RSR ne sera pas encore actif si vous prévoyez de créer un nouveau domaine sécurisé. Dans ce cas, la sortie de la commande **netseat_ping** indiquera la mention `non disponible` pour le RSR. Ce résultat est celui attendu dans cette situation. Vous pouvez continuer sans risque l'installation de Policy Director, puis le processus d'installation du serveur de gestion installera, configurera et initialisera automatiquement le répartiteur des services de répertoire. Si le RSR est déjà actif, la sortie de la commande indiquera `est disponible (v3.1)` pour ce service.
6. Si d'autres services sont indisponibles, hormis le RSR, corrigez le problème avant d'installer les serveurs de Policy Director.

Installation des serveurs de Policy Director

Avant de lancer l'installation des serveurs de Policy Director, vous devez connaître le nom d'utilisateur et le mot de passe d'un administrateur.

Pour installer les serveurs de Policy Director :

1. Vérifiez que le serveur LDAP est installé et actif si vous prévoyez d'utiliser le registre des utilisateurs LDAP. Reportez-vous au «Chapitre 4. Installation et configuration d'IBM SecureWay Directory» à la page 29.
2. Insérez le CD-ROM intitulé *IBM SecureWay Policy Director version 3.0* dans le lecteur de CD-ROM.
3. Passez dans le répertoire \win32\server.
4. Cliquez sur le fichier setup.exe pour lancer le programme InstallShield.
5. Sélectionnez la langue de travail désirée dans la fenêtre de sélection des langues.
6. Cliquez sur **Suivant** dans la fenêtre d'accueil de Policy Director.
7. Cliquez sur **Suivant**.

   La fenêtre de sélection des emplacements apparaît.
8. Acceptez le répertoire par défaut proposé pour installer les fichiers des programmes ou cliquez sur le bouton **Parcourir** pour créer ou sélectionner un autre répertoire.

   L'emplacement par défaut est `C:\Program Files\IBM\`

   Si vous avez installé NetSEAT dans un emplacement autre que le répertoire par défaut, installez les serveurs de Policy Director au même emplacement.
9. Cliquez sur **Suivant**.

   La fenêtre de sélection des composants à installer apparaît.
10. Sélectionnez les serveurs Policy Director appropriés. Pour obtenir une aide sur la sélection, reportez-vous à la section «Configurations standard» à la page 19.

    Il ne doit exister qu'une seule instance du serveur de gestion de Policy Director (IVMgr) dans le domaine sécurisé.
11. Cliquez sur **Suivant**.
12. Si vous n'avez pas sélectionné WebSEAL, passez à l'étape 14 à la page 51.

    Si vous avez sélectionné le composant WebSEAL (IVWeb), la fenêtre de sélection du répertoire racine des documents Web apparaît. Cette fenêtre permet de spécifier le répertoire racine de l'espace Web. Toutes les ressources dédiées au site WEB résideront dans ce répertoire.
13. Acceptez le répertoire racine proposé par défaut ou cliquez sur le bouton **Parcourir** pour créer ou sélectionner un autre répertoire. L'emplacement par défaut est :

    ```
    C:\...\IBM\Policy Director\www\docs
    ```

    Les fichiers de Policy Director se copient sur le disque dur. La fenêtre de connexion de l'administrateur apparaît. Cette étape permet de créer les droits d'accès pour terminer le processus de configuration.

14. Entrez le nom et le mot de passe de l'administrateur de la cellule DCE.
15. Si vous avez sélectionné le serveur de gestion (IVMgr), vous devez sélectionner **Registre LDAP** ou **Registre DCE**.

    Dans le cas contraire, le type de registre des utilisateurs utilisé pour le domaine sécurisé est automatiquement détecté.

    - Si un registre des utilisateurs LDAP est détecté, le processus d'installation se poursuit comme indiqué dans la section «Utilisation d'un registre des utilisateurs LDAP».
    - Si un registre des utilisateurs DCE est détecté, le processus d'installation se poursuit comme indiqué dans la section «Utilisation d'un registre des utilisateurs DCE» à la page 52.
16. Cliquez sur l'une des options suivantes pour choisir le registre des utilisateurs :
    - Si vous avez sélectionné **Registre LDAP**, passez à la section «Utilisation d'un registre des utilisateurs LDAP».
    - Si vous avez sélectionné **Registre DCE**, passez à la section «Utilisation d'un registre des utilisateurs DCE» à la page 52.

Utilisation d'un registre des utilisateurs LDAP

Si votre domaine sécurisé Policy Director utilise un registre des utilisateurs LDAP, ou si vous installez IVMgr et que vous avez choisi **Registre LDAP**, la fenêtre du serveur LDAP apparaît.

1. Entrez les données de configuration du serveur LDAP :
    - Nom d'hôte LDAP
    - Numéro de port
    - Numéro du port SSL (uniquement si vous utilisez SSL pour accéder au serveur LDAP).
    - DN LDAP pour la base de données GSO (par exemple, o=ibm,c=us)
2. Cliquez sur **Suivant**.

    La fenêtre de configuration des communications avec le serveur LDAP apparaît.
3. Activez ou désactivez les communications SSL entre Policy Director et le serveur LDAP. Cliquez sur **Oui** pour les activer, ou sur **Non** pour les désactiver.

    Sur Windows NT, les communications SSL ne sont activées qu'une seule fois entre tous les serveurs de Policy Director résidant sur le système hôte et le serveur LDAP.

    Si vous avez activé les communications SSL, passez à l'étape 4 à la page 52.

    Dans le cas contraire, passez à l'étape 5 à la page 52.

4. Renseignez les options suivantes :
   - Emplacement du fichier des clés SSL
   - DN du fichier SSL (étiquette de la clé)
   - Mot de passe du fichier des clés SSL

   Pour plus d'informations, reportez-vous à la section «Création du fichier de la base de données des clés et du certificat» à la page 34.
5. Cliquez sur **Suivant**.

   La fenêtre de connexion de l'administrateur LDAP apparaît.
6. Entrez le nom de l'administrateur LDAP (par exemple, cn=root) et son mot de passe, puis cliquez sur **OK**.

   Les serveurs sont configurés et s'initialisent. Ceci peut prendre quelques minutes. La fenêtre des informations système apparaît et indique l'état des serveurs, notamment s'agissant de leur enregistrement.
7. Cliquez sur **Suivant**.

   La fenêtre de fin de configuration de Policy Director apparaît.
8. Cliquez sur **Oui** pour redémarrer le système.

   Si vous avez répondu par **Non** à l'option de redémarrage, vous devrez relancer Windows NT plus tard pour terminer le processus de configuration. Cela fait, l'installation de Policy Director sera achevée.
9. Cliquez sur **Terminer**.

   Un message vous demande de redémarrer votre système.

Utilisation d'un registre des utilisateurs DCE

Si votre domaine sécurisé Policy Director utilise un registre des utilisateurs DCE, ou si vous installez IVMgr et que vous avez choisi **Registre DCE**, le processus d'installation se poursuit de la manière suivante :

1. Si vous avez sélectionné le composant WebSEAL (IVWeb), la fenêtre de sélection du répertoire racine des documents Web apparaît. Cette fenêtre permet de spécifier le répertoire racine de l'espace Web. Toutes les ressources dédiées au site WEB résideront dans ce répertoire.

   Si vous n'avez pas sélectionné WebSEAL, passez à l'étape 3.
2. Acceptez le répertoire racine proposé par défaut ou cliquez sur le bouton **Parcourir** pour créer ou sélectionner un autre répertoire. L'emplacement par défaut est :

   `C:\Program Files\IBM\Policy Director\www\docs`
3. Cliquez sur **Suivant**.

   Les fichiers de Policy Director se copient sur le disque dur. La fenêtre de connexion de l'administrateur apparaît.

4. Entrez le nom de l'administrateur LDAP et son mot de passe, puis cliquez sur **OK**.

   Les serveurs sont configurés et s'initialisent. Ceci peut prendre quelques minutes. La fenêtre des informations système apparaît et indique l'état des serveurs, notamment s'agissant de leur enregistrement.

5. Cliquez sur **Suivant**.

   La fenêtre de fin de configuration de Policy Director apparaît.

6. Cliquez sur **Terminer**.

   Un message vous demande de redémarrer votre système.

7. Cliquez sur **Oui** pour redémarrer le système.

   Si vous avez répondu par **Non** à l'option de redémarrage, vous devrez relancer Windows NT plus tard pour terminer le processus de configuration. Cela fait, l'installation de Policy Director sera achevée.

Configuration du Service d'acquisition de droits d'accès

Le SAD de Policy Director s'installe automatiquement. Pour utiliser ce SAD comme seul et unique service d'acquisition de droits d'accès, vous devez le configurer comme tel. Pour plus d'informations sur la configuration d'un service d'acquisition de droits d'accès, reportez-vous au manuel *Policy Director - Guide d'administration*.

Utilisation de la fonction d'interception de NetSEAL sur Windows NT

Policy Director NetSEAL (IVTrap) peut intercepter les requêtes au niveau de ports spécifiquement définis. Pour utiliser la fonction d'interception de NetSEAL, vous devez arrêter, puis redémarrer toutes les applications utilisant les ports spécifiés.

Pour plus d'informations sur la configuration de la fonction d'interception de Policy Director NetSEAL avec des ports spécifiques, reportez-vous à la présentation générale de NetSEAL fournie dans le manuel *Policy Director - Guide d'administration*.

Installation de la console de gestion sur Windows

Policy Director comporte une console de gestion qui permet de gérer plusieurs de ses composants à partir d'un client Windows. Cette console de gestion peut être installée sur les systèmes d'exploitation suivants :

- Windows 95
- Windows 98
- Windows NT version 4.0 avec Service Pack 4 ou version ultérieure

Chaque système d'exploitation Windows acceptant Policy Director nécessite le client NetSEAT.

Ce client NetSEAT peut être configuré comme client DCE ou comme client d'un serveur Policy Director. Bien que la console de gestion accepte les deux types de configuration, les serveurs de Policy Director demandent qu'elle soit installée comme client de serveur Policy Director.

Si vous devez réinstaller un composant, vous devez préalablement supprimer l'ancien avant d'installer le nouveau.

Installation de la console de gestion avec les serveurs

Une fois les modules de Policy Director installés et configurés, comme décrit dans la section «Installation des serveurs de Policy Director» à la page 49, passez aux étapes suivantes :

1. Insérez le CD-ROM intitulé *IBM SecureWay Policy Director version 3.0* dans le lecteur de CD-ROM.
2. Passez dans le répertoire \win32\Console.
3. Cliquez deux fois sur le fichier setup.exe pour lancer le programme InstallShield.
4. Sélectionnez la langue de travail désirée dans la fenêtre de sélection des langues.
5. Cliquez sur **Suivant** dans la fenêtre d'accueil de Policy Director.
6. Cliquez sur **Suivant**. La fenêtre de sélection des emplacements apparaît.
7. Indiquez l'emplacement où vous voulez installer les fichiers.

   Les fichiers se copient aux emplacements appropriés sur l'ordinateur. Une fenêtre d'informations vous informe que l'installation a réussi.
8. Si un message vous propose de redémarrer Windows, cliquez sur **Oui**.
9. Cliquez sur **OK**.
10. Passez à la section «Démarrage de la console de gestion» à la page 55.

Installation de la console de gestion sans les serveurs

Pour permettre l'administration de la solution de sécurité Policy Director à partir d'autres systèmes Windows, vous pouvez installer la console de gestion sur des ordinateurs sans y installer les serveurs de Policy Director. Lorsque vous installez la console de gestion de cette manière, le client NetSEAT peut être configuré comme client DCE ou comme client d'un serveur Policy Director.

Pour installer la console de gestion sans les serveurs, ouvrez le bureau de Windows et effectuez les opérations suivantes :

1. Vérifiez que le système d'exploitation Windows est pris en charge. Reportez-vous à la section «Serveurs Policy Director» à la page 16.

2. Installez le client Policy Director NetSEAT. Reportez-vous aux instructions de la section «Installation de NetSEAT» à la page 46.
3. Vérifiez que le client NetSEAT est configuré comme il convient dans le domaine sécurisé qui accueillera la console de gestion. Reportez-vous à la section «Vérification de la configuration du client NetSEAT» à la page 48.
4. Insérez le CD-ROM intitulé *IBM SecureWay Policy Director version 3.0* dans le lecteur de CD-ROM.
5. Passez dans le répertoire \win32\Console.
6. Cliquez deux fois sur le fichier setup.exe pour lancer le programme InstallShield.
7. Sélectionnez la langue de travail désirée dans la fenêtre de sélection des langues.
8. Cliquez sur **Suivant** dans la fenêtre d'accueil de Policy Director.
9. Cliquez sur **Suivant**. La fenêtre de sélection des emplacements apparaît.
10. Indiquez l'emplacement où vous voulez installer les fichiers.

    Les fichiers se copient aux emplacements appropriés sur l'ordinateur. Une fenêtre d'informations vous informe que l'installation a réussi.
11. Cliquez sur **OK** pour terminer l'installation.
12. Pour démarrer la console de gestion, passez à la section «Démarrage de la console de gestion».

Démarrage de la console de gestion

Pour démarrer la console de gestion :

1. Vérifiez que les modules de Policy Director sont installés et actifs.
2. Cliquez sur **Démarrer→ Programmes → Policy Director → Console de gestion.**

   La fenêtre d'accueil de la console de gestion de Policy Director apparaît.
3. Connectez-vous à la console de gestion sous un ID doté de droits d'administrateur, tel que cell_admin.

Suppression de Policy Director

Pour supprimer les composants de Policy Director, connectez-vous en qualité d'administrateur. Connectez-vous au domaine Windows sous un ID doté de droits d'accès d'administrateur. Par exemple :

```
dce_login cell_admin mot de passe
```

Si vous tentez de supprimer un composant sans avoir les droits d'accès appropriés, un message d'échec d'autorisation apparaît.

Vous devez supprimer les composants de Policy Director dans l'ordre inverse de leur installation. Utilisez l'icône **Ajout/Suppression de programmes** du panneau de configuration de Windows pour supprimer les composants de Policy Director.

Pour désinstaller l'ensemble de Policy Director, procédez dans l'ordre suivant :

1. Supprimez la console de gestion.
2. Supprimez les serveurs.
3. Supprimez le client NetSEAT.

Suppression de la console de gestion

Pour supprimer la console de gestion :

1. Si la fenêtre de la console de gestion est ouverte, fermez-la.
2. Sélectionnez **Ajout/Suppression de programmes** dans le panneau de configuration de Windows, puis cliquez sur **Console de gestion de Policy Director**.
3. Cliquez sur le bouton **Ajouter/Supprimer**.
4. Cliquez sur **Oui** pour confirmer la suppression du programme.
5. Cliquez sur **OK**.

Suppression des serveurs

Pour supprimer les serveurs de Policy Director, vous devez préalablement obtenir les privilèges et les droits d'accès requis.

Pour supprimer les serveurs :

1. Vérifiez que les modules de Policy Director sont installés et actifs.
2. Sélectionnez **Ajout/Suppression de programmes** dans le panneau de configuration de Windows, puis sélectionnez le premier serveur de Policy Director à supprimer.
3. Supprimez les serveurs de Policy Director dans l'ordre inverse de leur installation.

   Par exemple, si vous avez installé tous les serveurs, supprimez-les dans l'ordre suivant :

   - Authorization ADK (IVAuthADK)
   - Serveur d'autorisations (IVAcld)
   - NetSEAL (IVTrap).
   - WebSEAL (IVWeb).
   - Gestionnaire de sécurité (IVNet)
   - Serveur de gestion (IVMgr).
   - Base (IVBase). Ce composant est automatiquement installé.

La console de gestion de Policy Director peut être supprimée à n'importe quel instant. Pour plus d'informations sur l'ordre d'installation des composants, reportez-vous à la section «Etapes de l'installation de Policy Director» à la page 25.

4. Cliquez sur le bouton **Ajouter/Supprimer**.
5. Entrez le nom d'utilisateur et le mot de passe de l'administrateur LDAP à l'invite.
6. Répétez les étapes 2 à la page 56 à 5 pour chaque serveur de Policy Director.
7. Cliquez sur **OK** une fois les suppressions terminées.

Suppression du client NetSEAT

Vous devez posséder les privilèges de l'administrateur Windows NT pour supprimer les composants du client Policy Director NetSEAT.

1. Sélectionnez **Ajout/Suppression de programmes** dans le panneau de configuration de Windows, puis cliquez sur l'onglet **Installation/Désinstallation**.
2. Dans la liste de l'onglet, sélectionnez **Client Policy Director NetSEAT**.
3. Cliquez sur **Ajouter/Supprimer**.
4. Cliquez sur **OK**.

Chapitre 6. Installation de Policy Director pour AIX

Ce chapitre décrit comment installer et configurer Policy Director sur le système d'exploitation AIX.

Avant de lancer l'installation de Policy Director, lisez attentivement les informations contenues dans la section «Avant d'installer Policy Director pour AIX».

Avant d'installer Policy Director pour AIX

Avant de lancer l'installation de NetSEAT et de Policy Director, lisez les informations suivantes :

- Si vous créez une nouvelle cellule de DCE à l'occasion de l'installation des serveurs de Policy Director :
  - Vous devez également installer et configurer un serveur DCE.
  - Si vous comptez utiliser le registre des utilisateurs LDAP, vous devez installer et configurer un serveur LDAP.
- Lisez toutes les informations relatives à la mise en oeuvre de Policy Director, contenues dans la section «Composants à installer pour le domaine sécurisé» à la page 23.

Installation de la console de gestion

Policy Director comporte une console de gestion qui permet de gérer tous ses composants. Cette console de gestion peut être installée sur un système AIX, sur un système Windows, ou sur les deux.

La console de gestion pour AIX est vendue sous la forme d'un module appelé IV.Console. L'installation et la configuration de ce module se fait avec SMIT.

Installation de Policy Director

Pour installer Policy Director sur AIX :

1. Vérifiez que le serveur LDAP est installé et actif si vous prévoyez d'utiliser le registre des utilisateurs LDAP. Reportez-vous au «Chapitre 4. Installation et configuration d'IBM SecureWay Directory» à la page 29.
2. Connectez-vous en qualité d'utilisateur racine.
3. Insérez le CD-ROM intitulé *IBM SecureWay Policy Director version 3.0* dans le lecteur de CD-ROM.
4. Démarrez SMIT.
5. Cliquez sur **Installation et maintenance de logiciels**.

   Le menu Installation et maintenance de logiciels apparaît.
6. Cliquez sur **Installation et mise à jour de logiciels**.

   Le menu Installation et mise à jour de logiciels apparaît.
7. Cliquez sur **Installation et mise à jour de logiciels par nom de progiciel**.

   La fenêtre Installation et mise à jour de logiciels par nom de progiciel apparaît.
8. Indiquez l'unité contenant les fichiers à installer.

   Par exemple :

   - Si l'installation se fait à partir d'un lecteur de CD-ROM, entrez : `/dev/cd0`
   - Si l'installation se fait à partir d'un répertoire, ou d'un serveur, entrez : `/mnt/user/lpp/IV`

     Une fois l'unité indiquée, une fenêtre de sélection multiple apparaît.
9. Cliquez sur **IV**.

   Une fenêtre de sélection multiple affiche la liste des modules de Policy Director.
10. Sélectionnez les modules à installer.
    - Pour installer tous les modules de Policy Director, cliquez sur **IV**.
    - Si vous n'installez que certains des modules de Policy Director, respectez les indications fournies dans la section «Composants à installer pour le domaine sécurisé» à la page 23.
11. Cliquez sur **OK**.

    La fenêtre du menu SMIT Installation et mise à jour de logiciels par nom de progiciel apparaît.
12. Cliquez sur **Oui** à côté du champ :

    `Installation automatique des logiciels requis ?`

    Cette option entraîne l'installation automatique des modules de Policy Director IV.Base et IV.smit. Ces modules doivent obligatoirement être installés pour les besoins des autres composants de Policy Director. Si

vous sélectionnez **Non**, revenez au menu de sélection des modules. Vérifiez que vous avez bien sélectionné IV.Base et IV.Smit.

13. Choisissez des valeurs appropriées à votre situation pour les autres champs.
14. Cliquez sur **OK**.

    SMIT affiche des informations d'état, concernant notamment :

    - la vérification de la préinstallation des modules de Policy Director ;
    - le nom de chaque module pendant l'extraction de ses fichiers ;
    - la création de menus de configuration pour chaque module ;
    - un message d'état indiquant la réussite de l'extraction des fichiers.
15. Une fois l'extraction des fichiers terminée, configurez les modules de Policy Director, conformément aux instructions de la section «Configuration de Policy Director avec un registre des utilisateurs LDAP». Si vous utilisez le registre DCE, reportez-vous à la section «Configuration de Policy Director avec un registre des utilisateurs DCE» à la page 68.

Configuration de Policy Director avec un registre des utilisateurs LDAP

Vous devez installer les modules de Policy Director avant de pouvoir les configurer. Si vous ne les avez pas installés, reportez-vous à la section «Installation de Policy Director» à la page 60.

Si vous avez installé Policy Director avec un registre des utilisateurs DCE, reportez-vous à la section «Configuration de Policy Director avec un registre des utilisateurs DCE» à la page 68.

Vous devez configurer chaque module de Policy Director installé, hormis SMIT Setup. Configurez ces modules l'un après l'autre. Certains des modules de Policy Director nécessitent de répondre à des questions au cours de la configuration.

Pour configurer les modules de Policy Director :

1. Démarrez SMIT.

   Le menu de gestion de système apparaît.
2. Cliquez sur **Applications de communication et services**.

   La liste des logiciels installés apparaît. Par exemple :

   - TCP/IP
   - NFS
   - DCE
   - Policy Director
3. Cliquez sur **Policy Director**.

Le menu de Policy Director s'affiche avec les options suivantes :

- Configuration de Policy Director
- Annulation de la configuration de Policy Director

4. Cliquez sur **Configuration de Policy Director**.

   La liste des modules de Policy Director installés apparaît :

   - Configuration du module de base de Policy Director
   - Configuration du serveur de gestion de Policy Director
   - Configuration de la console de gestion de Policy Director
   - Configuration du gestionnaire de sécurité de Policy Director
   - Configuration de Policy Director WebSEAL
   - Configuration du serveur d'autorisations de Policy Director
   - Configuration de Policy Director NetSEAL
   - Configuration du serveur d'autorisation ADK de Policy Director

5. Cliquez sur chaque module à configurer, l'un après l'autre.

   Vous devez configurer les modules de Policy Director dans l'ordre de leur apparition dans la liste de configuration. Sélectionnez tour à tour chaque module, du premier jusqu'au dernier.

Vous devez à présent configurer chacun des modules de Policy Director que vous avez sélectionnés, à l'aide des instructions de configuration contenues dans la section correspondante.

Configuration du module de base

Le module IVBase s'installe sur l'ordinateur en même temps que n'importe lequel des autres modules. Pour configurer ce module, cliquez sur **Policy Director - Module de base** dans la liste de configuration de Policy Director.

La configuration du module de base de Policy Director se fait sans intervention de l'utilisateur.

Configuration du serveur de gestion

Pour configurer le serveur de gestion :

1. Cliquez sur **Policy Director - Serveur de gestion** dans la liste de configuration de Policy Director.

   Un message vous demande de choisir un type de registre des utilisateurs.

2. Si vous comptez utiliser le registre des utilisateurs LDAP, tapez 2.

   Un message vous demandera d'entrer le nom et le mot de passe de l'administrateur de la cellule du DCE.

3. Entrez le nom et le mot de passe de l'administrateur de la cellule du DCE à l'invite.

Si vous utilisez le registre des utilisateurs LDAP, une succession de messages apparaît pour configurer les communications entre le serveur de gestion et le serveur LDAP.

4. Entrez les données de configuration du serveur LDAP :
   - Nom d'hôte du serveur LDAP
   - Numéro de port du serveur LDAP
   - Numéro de port SSL du serveur LDAP (optionnel)
5. Entrez le nom d'utilisateur et le mot de passe de l'administrateur du système LDAP (par exemple, `cn=root`). Les données de sécurité de Policy Director sont à présent enregistrées sur le serveur LDAP.
6. Activez ou désactivez les communications SSL entre le serveur de gestion et le serveur LDAP.

   Remarque : Vous pouvez activer ou désactiver les communications SSL avec le serveur LDAP, individuellement pour chaque serveur concerné. Dans le cas présent, il s'agit des communications entre le serveur de gestion (IVMgr) et le serveur LDAP.
7. Si vous avez désactivé les communications SSL, passez à l'étape 8. Si vous avez activé les communications SSL, renseignez les paramètres suivants :
   - Emplacement du fichier de l'anneau de clés SSL
   - Etiquette de la clé SSL
   - Mot de passe de la clé SSL
8. Pour activer l'accès à la base de données GSO, indiquez le DN du suffixe de cette base de données (vous l'avez ajouté dans la section «Ajout de suffixes » à la page 31).

   Par exemple :

   ```
   o=IBM,c=FR
   ```

   Une fois configuré l'accès à la base de données GSO, le gestionnaire de configuration de Policy Director configure automatiquement un répartiteur des services de répertoire (RSR). Une série de messages indique chaque étape à mesure qu'elle s'accomplit.

   Un message annonce la fin de l'installation du module IVMgr.

   La liste des modules disponibles réapparaît.

Configuration et démarrage de la console de gestion

Pour configurer la console de gestion, cliquez sur **Policy Director - Console de gestion** dans la liste de configuration de Policy Director.

La configuration de la console de gestion de Policy Director se fait sans intervention de l'utilisateur.

Pour démarrer la console de gestion AIX :

1. Vérifiez que les modules de Policy Director sont installés et actifs.
2. Entrez la commande suivante :

```
$ /opt/intraverse/bin/ivconsole
```

Si vous utilisez la version client Windows de la console de gestion, suivez les instructions données dans la section «Démarrage de la console de gestion» à la page 55.

Configuration du gestionnaire de sécurité

Pour configurer le gestionnaire de sécurité (IVNet) :

1. Cliquez sur **Policy Director - Gestionnaire de sécurité** dans la liste de configuration de Policy Director.

   Une succession de messages apparaît pour intégrer le gestionnaire de sécurité au serveur LDAP.
2. Si un message le demande, entrez les données de configuration du serveur LDAP :
   - Nom d'hôte du serveur LDAP
   - Numéro de port du serveur LDAP
   - Numéro de port SSL du serveur LDAP (optionnel)

   Ces invites n'apparaissent pas si le serveur de gestion ou le serveur d'autorisations de Policy Director ont déjà été configurés.
3. Entrez le nom d'utilisateur et le mot de passe de l'administrateur du système LDAP. Les données de sécurité de Policy Director sont à présent enregistrées sur le serveur LDAP.
4. Activez ou désactivez les communications SSL entre le gestionnaire de sécurité et le serveur LDAP.

   Remarque : Vous pouvez activer ou désactiver les communications SSL avec le serveur LDAP, individuellement pour chaque serveur Policy Director concerné. Dans le cas présent, il s'agit des communications entre le gestionnaire de sécurité (module IVNet, qui comprend WebSEAL et NetSEAL) et le serveur LDAP.
5. Si vous avez désactivé les communications SSL, passez à l'étape 6 à la page 65. Si vous avez activé les communications SSL, renseignez les paramètres suivants :
   - Emplacement du fichier de l'anneau de clés SSL

- Etiquette de la clé SSL
- Mot de passe de la clé SSL

6. Pour activer l'accès à la base de données GSO, indiquez le DN du suffixe de cette base de données (vous l'avez ajouté dans la section «Ajout de suffixes » à la page 31).

   Par exemple :

   ```
   o=IBM,c=FR
   ```

   Cette invite n'apparaît pas si le serveur de gestion ou le serveur d'autorisations de Policy Director ont déjà été configurés.

   Un message vous demandera d'entrer le nom et le mot de passe de l'administrateur de la cellule du DCE.

7. Entrez le nom et le mot de passe de l'administrateur de la cellule du DCE à l'invite.

   Le gestionnaire de sécurité est à présent configuré et initialisé. Le serveur SAD est également lancé.

   Un message annonce la fin de l'installation du gestionnaire de sécurité.

Configuration de Policy Director WebSEAL

Pour configurer Policy Director WebSEAL (IVWeb) :

1. Cliquez sur **Policy Director - WebSEAL** dans la liste de configuration de Policy Director.

   Le menu de configuration de Policy Director WebSEAL s'affiche avec des valeurs qui définissent les paramètres suivants :

   - L'accès client HTTP et HTTPS
   - Les ports TCP nécessaires
   - Le répertoire racine par défaut des documents WEB

2. Confirmez les valeurs de configuration courantes :

   ```
   Vérifiez la configuration du serveur Web :
   1. Activer TCP HTTP ?                Oui
   2. Port HTTP                         80
   3. Activer HTTPS ?                   Oui
   4. Port HTTPS                        443
   5. Racine documents Web              /opt/Policy Director/www/docs
   a. Accepter la configuration et poursuivre l'installation
   x. Quitter l'installation

   Sélectionnez l'élément à modifier : a
   ```

3. Tapez a pour accepter cette configuration et continuer l'installation, ou entrez le numéro de la valeur à modifier.

   Le programme de configuration du gestionnaire de sécurité de Policy Director vous demande d'entrer le nom et le mot de passe de l'administrateur de la cellule du DCE.

4. Entrez le nom et le mot de passe de l'administrateur de la cellule du DCE à l'invite.

   Le gestionnaire de sécurité de Policy Director redémarre.

   Le programme d'installation configure et active Policy Director WebSEAL sur l'ordinateur.

Configuration du serveur d'autorisations de Policy Director

Pour configurer le serveur d'autorisations de Policy Director (IVAcld) :

1. Cliquez sur **Policy Director - Serveur d'autorisations** dans la liste de configuration de Policy Director.

   Une succession de messages apparaît pour intégrer le serveur d'autorisations au serveur LDAP.
2. Si un message le demande, entrez les données de configuration du serveur LDAP :
   - Nom d'hôte du serveur LDAP
   - Numéro de port du serveur LDAP
   - Numéro de port SSL du serveur LDAP (optionnel)

   Ces invites n'apparaissent pas si le serveur de gestion ou le serveur d'autorisations de Policy Director ont déjà été configurés.
3. Entrez le nom d'utilisateur et le mot de passe de l'administrateur du système LDAP. Les données de sécurité de Policy Director sont à présent enregistrées sur le serveur LDAP.
4. Activez ou désactivez les communications SSL entre le gestionnaire de sécurité et le serveur LDAP.

   Remarque : Vous pouvez activer ou désactiver les communications SSL avec le serveur LDAP, individuellement pour chaque serveur Policy Director concerné. Dans le cas présent, il s'agit des communications entre le serveur d'autorisations (IVAcld) et le serveur LDAP.
5. Si vous avez désactivé les communications SSL, passez à l'étape 6. Si vous avez activé les communications SSL, renseignez les paramètres suivants :
   - Emplacement du fichier de l'anneau de clés SSL
   - Etiquette de la clé SSL
   - Mot de passe de la clé SSL
6. Pour activer l'accès à la base de données GSO, indiquez le DN du suffixe de cette base de données (vous l'avez ajouté dans la section «Ajout de suffixes » à la page 31).

   Par exemple :

   ```
   o=IBM,c=FR
   ```

Cette invite n'apparaît pas si le serveur de gestion ou le serveur d'autorisations de Policy Director ont déjà été configurés.

Un message vous demandera d'entrer le nom et le mot de passe de l'administrateur de la cellule du DCE.

7. Entrez le nom et le mot de passe de l'administrateur de la cellule du DCE à l'invite.

   Le serveur d'autorisations est à présent configuré et initialisé.

   Un message annonce la fin de l'installation du serveur d'autorisations.

Configuration de Policy Director NetSEAL

Pour configurer Policy Director NetSEAL :

1. Cliquez sur **Policy Director - NetSEAL** dans la liste de configuration de Policy Director.

   Un message vous demandera d'entrer le nom et le mot de passe de l'administrateur de la cellule du DCE.

2. Entrez le nom d'utilisateur et le mot de passe de l'administrateur du système LDAP. Les données de sécurité de Policy Director sont à présent enregistrées sur le serveur LDAP.

   La configuration du module Policy Director NetSEAL se poursuit.

Policy Director NetSEAL peut intercepter les requêtes arrivant sur des ports définis. Pour utiliser la fonction d'interception de NetSEAL, vous devez arrêter, puis redémarrer toutes les applications utilisant les ports spécifiés. Pour plus d'informations sur l'utilisation de Policy Director NetSEAL, reportez-vous à la section «Utilisation de la fonction d'interception de NetSEAL sur AIX» à la page 72.

Configuration du kit de développement Authorization ADK de Policy Director

Pour configurer le kit de développement d'applications d'autorisation de Policy Director, cliquez sur **Policy Director - Authorization ADK** dans la liste de configuration de Policy Director.

La configuration du module Authorization ADK de Policy Director se fait sans intervention de l'utilisateur.

Configuration du service d'acquisition de droits d'accès de Policy Director

Le SAD de Policy Director s'installe automatiquement. Pour utiliser ce SAD comme seul et unique service d'acquisition de droits d'accès, vous devez le configurer comme tel. Pour plus d'informations sur le SAD de Policy Director et sur sa configuration avec le serveur WebSEAL, reportez-vous au manuel *Policy Director - Guide d'administration*.

Configuration de Policy Director avec un registre des utilisateurs DCE

Vous devez installer les modules de Policy Director avant de pouvoir les configurer. Si vous ne les avez pas installés, reportez-vous à la section «Installation de Policy Director» à la page 60.

Si vous avez installé Policy Director avec un registre des utilisateurs LDAP, reportez-vous à la section «Configuration de Policy Director avec un registre des utilisateurs LDAP» à la page 61.

Vous devez configurer chaque module de Policy Director installé, hormis SMIT Setup. Configurez ces modules l'un après l'autre. Certains des modules de Policy Director nécessitent de répondre à des questions au cours de la configuration.

Pour configurer les modules de Policy Director :

1. Démarrez SMIT.

   Le menu de gestion de système apparaît.
2. Cliquez sur **Applications de communication et services**.

   La liste des logiciels installés apparaît. Par exemple :
   - TCP/IP
   - NFS
   - DCE
   - Policy Director
3. Cliquez sur **Policy Director**.

   Le menu de Policy Director s'affiche avec les options suivantes :
   - Configuration de Policy Director
   - Annulation de la configuration de Policy Director
4. Cliquez sur **Configuration de Policy Director**.

   La liste des modules de Policy Director installés apparaît :
   - Configuration du module de base de Policy Director
   - Configuration du serveur de gestion de Policy Director
   - Configuration de la console de gestion de Policy Director
   - Configuration du gestionnaire de sécurité de Policy Director
   - Configuration de Policy Director WebSEAL
   - Configuration du serveur d'autorisations de Policy Director
   - Configuration de Policy Director NetSEAL
   - Configuration du serveur d'autorisation ADK de Policy Director
5. Cliquez sur chaque module à configurer, l'un après l'autre.

Vous devez configurer les modules de Policy Director dans l'ordre de leur apparition dans la liste de configuration. Sélectionnez tour à tour chaque module, du premier jusqu'au dernier.

Vous devez à présent configurer chacun des modules de Policy Director que vous avez sélectionnés, à l'aide des instructions de configuration contenues dans la section correspondante.

Configuration du module de base

Le module IVBase s'installe sur l'ordinateur en même temps que n'importe lequel des autres modules. Pour configurer ce module, cliquez sur **Policy Director - Module de base** dans la liste de configuration de Policy Director.

La configuration du module de base de Policy Director se fait sans intervention de l'utilisateur.

Configuration du serveur de gestion

Pour configurer le serveur de gestion :

1. Cliquez sur **Policy Director - Serveur de gestion** dans la liste de configuration de Policy Director.

   Un message vous demandera d'entrer le nom et le mot de passe de l'administrateur de la cellule du DCE.
2. Entrez le nom et le mot de passe de l'administrateur de la cellule du DCE à l'invite.

   Le programme d'installation configure et démarre le serveur de gestion.

Configuration et démarrage de la console de gestion

Pour configurer la console de gestion, cliquez sur **Policy Director - Console de gestion** dans la liste de configuration de Policy Director.

La configuration de la console de gestion de Policy Director se fait sans intervention de l'utilisateur.

Pour démarrer la console de gestion AIX :

1. Vérifiez que les modules de Policy Director sont installés et actifs.
2. Entrez la commande suivante :

```
$ /opt/intraverse/bin/ivconsole
```

Configuration du gestionnaire de sécurité

Pour configurer le gestionnaire de sécurité (IVNet) :

1. Cliquez sur **Policy Director - Gestionnaire de sécurité** dans la liste de configuration de Policy Director.
2. Entrez le nom et le mot de passe de l'administrateur de la cellule du DCE à l'invite.

Le programme d'installation configure et démarre le gestionnaire de sécurité.

Configuration de Policy Director WebSEAL

Pour configurer Policy Director WebSEAL (IVWeb) :

1. Cliquez sur **Policy Director - WebSEAL** dans la liste de configuration de Policy Director.

   Le menu de configuration de Policy Director WebSEAL s'affiche avec des valeurs qui définissent les paramètres suivants :

   - L'accès client HTTP et HTTPS
   - Les ports TCP nécessaires
   - Le répertoire racine par défaut des documents WEB

2. Confirmez les valeurs de configuration courantes :

```
Vérifiez la configuration du serveur Web :
1. Activer TCP HTTP ?                Oui
2. Port HTTP                         80
3. Activer HTTPS ?                   Oui
4. Port HTTPS                        443
5. Racine documents Web              /opt/Policy Director/www/docs
a. Accepter la configuration et poursuivre l'installation
x. Quitter l'installation

Sélectionnez l'élément à modifier : a
```

3. Tapez a pour accepter cette configuration et continuer l'installation, ou entrez le numéro de la valeur à modifier.

   Le programme de configuration du gestionnaire de sécurité de Policy Director vous demande d'entrer le nom et le mot de passe de l'administrateur de la cellule du DCE.

4. Entrez le nom et le mot de passe de l'administrateur de la cellule du DCE à l'invite.

   Le gestionnaire de sécurité de Policy Director redémarre.

   Le programme d'installation configure et active Policy Director WebSEAL sur l'ordinateur.

Configuration du serveur d'autorisations de Policy Director

Pour configurer le serveur d'autorisations de Policy Director (IVAcld) :

1. Cliquez sur **Policy Director - Serveur d'autorisations** dans la liste de configuration de Policy Director.

   Un message vous demandera d'entrer le nom et le mot de passe de l'administrateur de la cellule du DCE.

2. Entrez le nom et le mot de passe de l'administrateur de la cellule du DCE à l'invite.

   Le serveur d'autorisations est à présent configuré et initialisé.

Configuration de Policy Director NetSEAL

Pour configurer Policy Director NetSEAL :

1. Cliquez sur **Policy Director - NetSEAL** dans la liste de configuration de Policy Director.

   Un message vous demandera d'entrer le nom et le mot de passe de l'administrateur de la cellule du DCE.

2. Entrez le nom d'utilisateur et le mot de passe de l'administrateur du système LDAP. Les données de sécurité de Policy Director sont à présent enregistrées sur le serveur LDAP.

   La configuration de Policy Director NetSEAL se poursuit.

Policy Director NetSEAL peut intercepter les requêtes arrivant sur des ports définis. Pour utiliser la fonction d'interception de NetSEAL, vous devez arrêter, puis redémarrer toutes les applications utilisant les ports spécifiés. Pour plus d'informations sur l'utilisation de Policy Director NetSEAL, reportez-vous à la section «Utilisation de la fonction d'interception de NetSEAL sur AIX» à la page 72.

Configuration du kit de développement Authorization ADK de Policy Director

Pour configurer le kit de développement d'applications d'autorisation de Policy Director, cliquez sur **Policy Director - Authorization ADK** dans la liste de configuration de Policy Director.

La configuration du module Authorization ADK de Policy Director se fait sans intervention de l'utilisateur.

Configuration du service d'acquisition de droits d'accès de Policy Director

Le SAD de Policy Director s'installe automatiquement. Pour utiliser ce SAD comme seul et unique service d'acquisition de droits d'accès, vous devez le configurer comme tel. Pour plus d'informations sur le SAD de Policy Director et sur sa configuration avec le serveur WebSEAL, reportez-vous au manuel *Policy Director - Guide d'administration*.

Installation de la console de gestion

Policy Director comporte une console de gestion qui permet de gérer plusieurs de ses composants à partir d'un client Windows. Cette console de gestion peut être installée sur les systèmes d'exploitation suivants :

- Windows 95
- Windows 98
- Windows NT version 4.0 avec Service Pack 4 ou version ultérieure
- AIX version 4.3.1.0 ou ultérieure

Chaque système d'exploitation Windows acceptant Policy Director nécessite le client NetSEAT.

Ce client NetSEAT peut être configuré comme client DCE ou comme client d'un serveur Policy Director. Bien que la console de gestion accepte les deux types de configuration, les serveurs de Policy Director demandent qu'elle soit installée comme client de serveur Policy Director.

Si vous devez réinstaller un composant, vous devez préalablement supprimer l'ancien avant d'installer le nouveau.

Utilisation de la fonction d'interception de NetSEAL sur AIX

Pour utiliser la fonction d'interception de Policy Director NetSEAL, le gestionnaire de sécurité du démon NetSEAL (secmgrd) doit s'initialiser avant les applications utilisant les ports sécurisés (avec demande d'alerte). Définissez comme il convient les entrées du fichier /etc/inittab pour que le processus secmgrd s'initialise avant les applications au démarrage du système.

La fonction d'interception de NetSEAL s'utilise avec des applications de réseau telles que Telnet, RLOGIN et POP3. Ces applications sont contrôlées par le démon **inetd**. Le script de démarrage de Policy Director, /etc/iv/iv, initialise secmgrd, puis arrête et relance le démon inetd. Cette procédure permet d'intercepter les événements liés à ces applications après le démarrage du système.

Si vous arrêtez Policy Director, puis que vous le relancez, vous devez également arrêter puis relancer les applications adressant des requêtes sur les ports avec demande d'alerte. Pour automatiser ce processus, vous pouvez modifier le script /etc/iv/iv de manière à arrêter puis réinitialiser les applications après le démarrage de secmgrd. Vous pouvez utiliser cette technique d'arrêt et de redémarrage de **inetd** comme modèle pour arrêter et relancer les autres applications.

Pour plus d'informations sur la configuration de la fonction d'interception de Policy Director NetSEAL avec des ports spécifiques, reportez-vous à la présentation générale de NetSEAL fournie dans le manuel *Policy Director - Guide d'administration*.

Suppression de Policy Director

La suppression de Policy Director pour AIX nécessite d'annuler préalablement sa configuration.

- Pour plus d'informations sur l'annulation de la configuration de Policy Director, reportez-vous à la section «Annulation de la configuration des modules de Policy Director» à la page 73.

- Pour plus d'informations sur la suppression de Policy Director, reportez-vous à la section «Suppression des modules de Policy Director» à la page 74.

Pour supprimer la version Windows de la console de gestion, reportez-vous à la section «Suppression de la console de gestion» à la page 56.

Annulation de la configuration des modules de Policy Director

Pour annuler la configuration des serveurs de Policy Director, procédez de la manière suivante :

1. Démarrez SMIT.
2. Cliquez sur **Applications de communication et services**.

   Le menu des services et des applications de communication apparaît.
3. Cliquez sur **Policy Director**.

   Le menu de Policy Director apparaît.
4. Dans le menu, cliquez sur **Annulation de la configuration de Policy Director**

   La liste des modules de Policy Director configurés apparaît.

   Sélectionnez les modules dont vous voulez annuler la configuration. Les modules susceptibles de figurer dans la liste sont les suivants :
   - Annulation de la configuration du serveur d'autorisations de Policy Director
   - Annulation de la configuration du kit de développement Authorization ADK de Policy Director
   - Annulation de la configuration de Policy Director NetSEAL
   - Annulation de la configuration de Policy Director WebSEAL
   - Annulation de la configuration du gestionnaire de sécurité de Policy Director
   - Annulation de la configuration du serveur de gestion de Policy Director
   - Annulation de la configuration de la console de gestion de Policy Director
   - Annulation de la configuration du module de base de Policy Director
   - Annulation de la configuration du menu IV Smit
5. La configuration de chacun de ces modules doit être annulée l'une après l'autre.

   Remarque : Cette opération doit se faire dans l'ordre inverse de leur installation. Pour respecter cet ordre, partez du premier module du menu vers le dernier.
6. Si vous annulez la configuration des modules de Policy Director dans le but de supprimer totalement Policy Director de votre système, cliquez sur

Annulation de la configuration du menu SMIT de Policy Director après avoir annulé la configuration de tous les autres modules de Policy Director.

Cette action supprime les données des modules de Policy Director de la base de données de SMIT.

7. Reportez-vous à la section «Suppression des modules de Policy Director» pour supprimer Policy Director.

Suppression des modules de Policy Director

Avant de supprimer Policy Director, vérifiez préalablement que vous avez bien annulé la configuration de tous les modules du produit. Pour plus d'informations sur cette procédure, reportez-vous à la section «Annulation de la configuration des modules de Policy Director» à la page 73.

Pour supprimer Policy Director :

1. Démarrez SMIT.
2. Cliquez sur **Installation et maintenance de logiciels**.

   Le menu Installation et maintenance de logiciels apparaît.
3. Cliquez sur **Maintenance des logiciels et utilitaires**.

   Le menu Maintenance des logiciels et utilitaires apparaît.
4. Cliquez sur **Retrait de logiciels installés**.

   La fenêtre Retrait de logiciels installés apparaît.
5. Sélectionnez les modules de Policy Director à supprimer. Vous pouvez sélectionner plusieurs modules simultanément.

   Pour supprimer tous les modules de Policy Director, entrez `IV`.

Les logiciels de Policy Director sont supprimés du système.

Suppression de la console de gestion et de NetSEAT

Vous pouvez supprimer la version Windows de la console de gestion et le client NetSEAT au moyen de la fonction de désinstallation d'InstallShield :

- Supprimez la console de gestion. Reportez-vous à la section «Suppression de la console de gestion» à la page 56.
- Supprimez le client NetSEAT. Reportez-vous à la section «Suppression du client NetSEAT» à la page 57.

Chapitre 7. Installation de Policy Director pour Solaris

Ce chapitre décrit comment installer et configurer Policy Director sur le système d'exploitation Solaris.

Avant de lancer l'installation de Policy Director, lisez attentivement les informations contenues dans la section «Avant d'installer Policy Director pour Solaris».

Avant d'installer Policy Director pour Solaris

Avant de lancer l'installation de Policy Director, lisez les informations suivantes :

La procédure d'installation de cette version de Policy Director nécessite l'emploi de la commande **pkgadd**. Pour exécuter la commande **pkgadd**, entrez la syntaxe suivante à l'invite de commande :

```
# pkgadd -d /cdrom/cdrom0/solaris
```

Utilisez la commande **pkgadd** pour installer Policy Director. La commande **pkgadd** affiche souvent des invites supplémentaires qui n'apparaissent pas dans la procédure standard. Ces invites répondent à des situations particulières qui dépendent des paramètres et de la configuration de votre système. Répondez toujours `Oui` à ces invites si elles échappent aux procédures standard.

Avant d'installer Policy Director :

- Vous devez installer un client DCE.
- Si vous utilisez le registre des utilisateurs LDAP, vous devez aussi installer un client LDAP.

Vous devez activer les fonctions d'administration à distance de Transarc DCE avant de lancer l'installation de Policy Director. Vous ne pourrez pas accomplir l'installation de Policy Director si ces fonctions ne sont pas activées.

L'utilisation de certaines de ces fonctions d'administration à distance donne à l'administrateur de la cellule des pouvoirs équivalents à celui de l'utilisateur racine local. En principe, Transarc DCE désactive ces fonctions d'administration à distance. Celles-ci sont toutefois nécessaires pour installer Policy Director.

Pour plus d'informations sur l'activation des fonctions d'administration à distance, reportez-vous à la section 4.2.1 du document *Transarc Release Notes, Release 1.1* (DCE-D1002-01).

Sortie de l'écran d'installation

Les procédures standard présentées dans ce document n'indiquent pas toutes les sorties possibles de la commande **pkgadd**. La plupart des sorties non répertoriées fournissent des informations supplémentaires sur les opérations réalisées. En général, les procédures standard présentées dans ce document ne mentionnent que les messages nécessitant une réponse de l'utilisateur.

Installation des serveurs de Policy Director avec un registre des utilisateurs LDAP

Si vous avez installé Policy Director avec un registre des utilisateurs DCE, reportez-vous à la section «Installation d'un serveur Policy Director avec un registre des utilisateurs DCE» à la page 82.

Les programmes des serveurs se trouvent dans le répertoire /solaris du CD-ROM *IBM SecureWay Policy Director version 3.0*.

L'installation des modules de Policy Director nécessite de se connecter sous l'ID de l'utilisateur racine.

Si vous désirez réinstaller un module quelconque, supprimez préalablement l'ancien module (**pkgrm**) avant d'installer le nouveau.

Pour installer le serveur de gestion :

1. Vérifiez que le serveur LDAP est installé et actif si vous prévoyez d'utiliser le registre des utilisateurs LDAP. Reportez-vous au «Chapitre 4. Installation et configuration d'IBM SecureWay Directory» à la page 29.
2. Entrez la commande **pkgadd** pour afficher la liste des modules contenus dans le CD-ROM :

   ```
   # pkgadd -d /cdrom/cdrom0/solaris
   ```

   La liste des modules disponibles apparaît.

   Si vous utilisez un autre point de montage pour le lecteur de CD-ROM, indiquez-le dans la commande précédente.
3. Pour installer les fichiers du module de base de Policy Director, tapez le numéro du module IVBase, puis appuyez sur Entrée.

   Cette commande extrait les fichiers du CD-ROM puis les installe sur le disque dur, à l'emplacement que vous avez indiqué.

   Un message annonce la fin de l'installation du module IVBase. La liste des modules disponibles réapparaît.

Avant de continuer, souvenez-vous qu'il ne doit exister qu'une seule instance du serveur de gestion (IVMgr) dans le domaine sécurisé. Si l'installation a lieu sur un système autonome, passez à l'étape suivante. Dans le cas d'un serveur secondaire, assurez-vous que vous avez lu la section «Composants à installer pour le domaine sécurisé» à la page 23.

4. Pour installer les fichiers du serveur de gestion de Policy Director, tapez le numéro du module IVMgr. Appuyez sur Entrée.

   Cette commande extrait les fichiers du CD-ROM puis les installe sur le disque dur, à l'emplacement que vous avez indiqué.

   Un message vous demande de choisir un type de registre des utilisateurs.

5. Si vous utilisez le registre des utilisateurs LDAP, tapez 2 pour le sélectionner.

   Un message vous demandera d'entrer le nom et le mot de passe de l'administrateur de la cellule du DCE.

6. Entrez les renseignements nécessaires pour accéder au compte de l'administrateur de la cellule DCE.

   ```
   Entrez le nom utilisateur de
   l'administrateur de cellule (cell_admin) :
   Entrez le mot de passe de l'administrateur de cellule :
   ```

   Une succession de messages apparaît pour configurer les communications entre le serveur de gestion et le serveur LDAP.

7. Entrez les données de configuration du serveur LDAP :
   - Nom d'hôte du serveur LDAP
   - Numéro de port du serveur LDAP
   - Numéro de port SSL du serveur LDAP

8. Entrez le DN et le mot de passe de l'administrateur du système LDAP (par exemple, `cn=root`). Le serveur LDAP contient à présent les données de sécurité de Policy Director.

9. Activez ou désactivez les communications SSL entre le serveur de gestion et le serveur LDAP.

   Vous pouvez activer ou désactiver les communications SSL avec le serveur LDAP, individuellement pour chaque serveur Policy Director concerné. Dans le cas présent, il s'agit des communications entre le serveur de gestion et le serveur LDAP.

10. Si vous avez désactivé les communications SSL, vous pouvez ignorer cette étape. Si vous avez activé les communications SSL, renseignez les paramètres suivants :
    - `Emplacement du fichier de l'anneau de clés SSL`
    - `Etiquette de la clé SSL`
    - `Mot de passe de la clé SSL`

11. Pour activer l'accès à la base de données GSO, indiquez le DN du suffixe de cette base de données (vous l'avez ajouté dans la section «Ajout de suffixes » à la page 31).

    Par exemple :

    ```
    o=IBM,c=FR
    ```

    Une fois configuré l'accès à la base de données GSO, le gestionnaire de configuration de Policy Director configure automatiquement un répartiteur de services de répertoire (RSR). Une série de messages indique chaque étape à mesure qu'elle s'accomplit.

    Un message annonce la fin de l'installation du serveur de gestion. La liste des modules disponibles réapparaît.

Installation du gestionnaire de sécurité pour WebSEAL et NetSEAL

Le gestionnaire de sécurité (module IVNet) nécessite des ressources fournies par le module de base. Vérifiez que ce module de base est installé avant d'installer IVNet.

1. Pour installer les fichiers du gestionnaire de sécurité de Policy Director, tapez le numéro du module IVNet, puis appuyez sur Entrée.

   Les fichiers sont extraits du CD-ROM puis installés sur le disque dur, dans le répertoire par défaut.

   Si vous utilisez le registre des utilisateurs LDAP, une succession de messages apparaît pour intégrer le gestionnaire de sécurité au serveur LDAP.
2. Si un message le demande, entrez les données de configuration du serveur LDAP :
   - Nom d'hôte du serveur LDAP
   - Numéro de port du serveur LDAP
   - Numéro de port SSL du serveur LDAP

   Les invites de configuration mentionnées ci-dessus n'apparaissent que si les communications avec le serveur LDAP n'ont été configurées pour aucun autre module de Policy Director sur le système. Si le serveur de gestion (IVMgr) ou le serveur d'autorisations (IVAcld) ont été configurés sur le système, ces invites n'apparaissent pas à ce stade.
3. Entrez le DN et le mot de passe de l'administrateur du système LDAP.

   Le serveur LDAP contient à présent les données de sécurité de Policy Director.
4. Activez ou désactivez les communications SSL entre le gestionnaire de sécurité et le serveur LDAP.

Vous pouvez activer ou désactiver les communications SSL avec le serveur LDAP, individuellement pour chaque serveur Policy Director concerné. Dans le cas présent, il s'agit des communications entre le gestionnaire de sécurité et le serveur LDAP.

5. Si vous avez désactivé les communications SSL, vous pouvez ignorer cette étape. Si vous avez activé les communications SSL, renseignez les paramètres suivants :
   - `Emplacement du fichier de l'anneau de clés SSL`
   - `Etiquette de la clé SSL`
   - `Mot de passe de la clé SSL`
6. Pour activer l'accès à la base de données GSO, indiquez le DN du suffixe de cette base de données (vous l'avez ajouté dans la section «Ajout de suffixes » à la page 31).

   Par exemple :

   ```
   o=IBM,c=FR
   ```

   Un message vous demandera d'entrer le nom et le mot de passe de l'administrateur de la cellule du DCE.
7. Entrez les renseignements nécessaires pour accéder au compte de l'administrateur de la cellule DCE.

   ```
   Entrez le nom utilisateur de
   l'administrateur de cellule (cell_admin) :
   Entrez le mot de passe de l'administrateur de cellule :
   ```

   Le gestionnaire de sécurité est à présent configuré et initialisé.

   Le serveur SAD est à présent configuré et initialisé.

   Un message annonce la fin de l'installation du module IVNet. La liste des modules disponibles réapparaît.

Activation de WebSEAL

Pour activer WebSEAL, vous devez préalablement installer le module correspondant (IVWeb).

1. Tapez le numéro désignant le module IVWeb pour installer les fichiers nécessaires à l'activation du serveur HTTP WebSEAL.
2. Appuyez sur Entrée pour continuer.

   Les fichiers sont extraits du CD-ROM puis installés sur le disque dur.

   Une liste de configuration apparaît, avec des valeurs confirmant l'accès des clients par HTTP et HTTPS, les ports TCP utilisés et le répertoire racine par défaut des documents Web.

3. Confirmez les valeurs de configuration courantes :

```
Vérifiez
la configuration du serveur Web :
1. Activer TCP HTTP ?                Oui
2. Port HTTP                         80
3. Activer HTTPS ?                   Oui
4. Port HTTPS                        443
5. Racine documents Web              /opt/Policy Director/www/docs

a. Accepter la configuration et poursuivre l'installation
x. Quitter l'installation

Sélectionnez l'élément à modifier : a
```

4. Tapez a pour accepter cette configuration et continuer l'installation, puis appuyez sur Entrée.
5. Entrez les renseignements nécessaires pour accéder au compte de l'administrateur de la cellule DCE.

```
Entrez le nom utilisateur de
l'administrateur de cellule (cell_admin) :
Entrez le mot de passe de l'administrateur de cellule :
```

Le programme d'installation configure et active WebSEAL sur l'ordinateur. Le gestionnaire de sécurité redémarre automatiquement.

Activation de NetSEAL

Pour activer NetSEAL, vous devez préalablement installer le module correspondant (IVTrap).

1. Tapez le numéro désignant le module IVTrap pour installer les fichiers nécessaires à l'activation du composant NetSEAL (contrôle d'accès TCP/IP standard).

   NetSEAL est à présent configuré et activé.

   Un message vous demandera d'entrer le nom et le mot de passe de l'administrateur de la cellule du DCE.
2. Entrez les renseignements nécessaires pour accéder au compte de l'administrateur de la cellule DCE.

   Un message vous informe que vous devez indiquer les ports protégés à l'aide de la commande **ivadmin**.

   Un nouveau message vous demande de réamorcer le système pour placer tous les ports protégés sous le contrôle de NetSEAL.

   Un message annonce la fin de l'installation du module IVTrap. La liste des modules disponibles réapparaît.

Policy Director NetSEAL peut intercepter les requêtes arrivant sur des ports définis. Pour utiliser la fonction d'interception de NetSEAL, vous devez arrêter, puis redémarrer toutes les applications utilisant les ports spécifiés.

Pour plus d'informations sur la configuration de Policy Director NetSEAL, reportez-vous à la présentation générale de NetSEAL fournie dans le manuel *Policy Director - Guide d'administration*.

Installation du serveur d'autorisations

Pour installer le serveur d'autorisations :

1. Pour installer les fichiers du serveur d'autorisations de Policy Director, tapez le numéro du module IVAcld, puis appuyez sur Entrée.

   Les fichiers sont extraits du CD-ROM puis installés sur le disque dur, dans le répertoire par défaut.

   Si vous utilisez le registre des utilisateurs LDAP, une succession de messages apparaît pour intégrer le serveur d'autorisations au serveur LDAP.
2. Si un message le demande, entrez les données de configuration du serveur LDAP :
   - Nom d'hôte du serveur LDAP
   - Numéro de port du serveur LDAP
   - Numéro de port SSL du serveur LDAP

   Les invites de configuration mentionnées ci-dessus n'apparaissent que si les communications avec le serveur LDAP n'ont été configurées pour aucun autre module de Policy Director sur le système. Si le serveur de gestion (IVMgr) ou le gestionnaire de sécurité (IVNet) ont été configurés sur le système, ces invites n'apparaissent pas à ce stade.
3. Entrez le DN et le mot de passe de l'administrateur du système LDAP.

   Le serveur LDAP contient à présent les données de sécurité de Policy Director.
4. Activez ou désactivez les communications SSL entre le serveur de gestion et le serveur LDAP.

   Vous pouvez activer ou désactiver les communications SSL avec le serveur LDAP, individuellement pour chaque serveur Policy Director concerné. Dans le cas présent, il s'agit des communications entre le serveur de gestion et le serveur LDAP.
5. Si vous avez désactivé les communications SSL, vous pouvez ignorer cette étape. Si vous avez activé les communications SSL, renseignez les paramètres suivants :
   - `Emplacement du fichier de l'anneau de clés SSL`
   - `Etiquette de la clé SSL`
   - `Mot de passe de la clé SSL`
6. Pour activer l'accès à la base de données GSO, indiquez le DN du suffixe de cette base de données (vous l'avez ajouté dans la section «Ajout de suffixes » à la page 31).

Par exemple :

```
o=IBM,c=FR
```

Un message vous demandera d'entrer le nom et le mot de passe de l'administrateur de la cellule du DCE.

7. Entrez les renseignements nécessaires pour accéder au compte de l'administrateur de la cellule DCE.

   ```
   Entrez le nom utilisateur de
   l'administrateur de cellule (cell_admin) :
   Entrez le mot de passe de l'administrateur de cellule :
   ```

   Le serveur d'autorisations est à présent configuré et initialisé.

   Un message annonce la fin de l'installation du module IVAcld. La liste des modules disponibles réapparaît.

Installation de l'API d'autorisation

Pour installer les fichiers de l'API d'autorisation pour langage C, tapez le numéro du module IVAuthADK, puis appuyez sur Entrée.

Les fichiers sont extraits du CD-ROM puis installés sur le disque dur, dans le répertoire par défaut.

Un message annonce la fin de l'installation du module IVAuthADK. La liste des modules disponibles réapparaît.

Installation d'un serveur Policy Director avec un registre des utilisateurs DCE

Si vous voulez installer Policy Director avec un registre des utilisateurs LDAP, reportez-vous à la section «Installation des serveurs de Policy Director avec un registre des utilisateurs LDAP» à la page 76.

Les programmes des serveurs se trouvent dans le répertoire /solaris du CD-ROM *IBM SecureWay Policy Director version 3.0*.

L'installation des modules de Policy Director nécessite de se connecter sous l'ID de l'utilisateur racine.

Si vous désirez réinstaller un module quelconque, supprimez préalablement l'ancien module (**pkgrm**) avant d'installer le nouveau.

Pour installer le serveur de gestion :

1. Entrez la commande **pkgadd** pour afficher la liste des modules contenus dans le CD-ROM :

   ```
   # pkgadd -d /cdrom/cdrom0/solaris
   ```

La liste des modules disponibles apparaît.

Si vous utilisez un autre point de montage pour le lecteur de CD-ROM, indiquez-le dans la commande précédente.

2. Pour installer les fichiers du module de base de Policy Director, tapez le numéro du module IVBase, puis appuyez sur Entrée.

   Cette commande extrait les fichiers du CD-ROM puis les installe sur le disque dur, à l'emplacement que vous avez indiqué.

   Un message annonce la fin de l'installation du module IVBase. La liste des modules disponibles réapparaît.

   Avant de continuer, souvenez-vous qu'il ne doit exister qu'une seule instance du serveur de gestion (IVMgr) dans le domaine sécurisé. Si l'installation a lieu sur un système autonome, passez à l'étape suivante. Dans le cas d'un serveur secondaire, assurez-vous que vous avez lu la section «Composants à installer pour le domaine sécurisé» à la page 23.

3. Pour installer les fichiers du serveur de gestion de Policy Director, tapez le numéro du module IVMgr. Appuyez sur Entrée.

   Cette commande extrait les fichiers du CD-ROM puis les installe sur le disque dur, à l'emplacement que vous avez indiqué.

   Un message vous demande de choisir un type de registre des utilisateurs.

4. Si vous utilisez le registre des utilisateurs DCE, tapez 1 pour le sélectionner.

   Un message vous demandera d'entrer le nom et le mot de passe de l'administrateur de la cellule du DCE.

5. Entrez les renseignements nécessaires pour accéder au compte de l'administrateur de la cellule DCE.

   ```
   Entrez le nom utilisateur de
   l'administrateur de cellule (cell_admin) :
   Entrez le mot de passe de l'administrateur de cellule :
   ```

   Un message annonce la fin de l'installation du serveur de gestion. La liste des modules disponibles réapparaît.

Installation du gestionnaire de sécurité pour WebSEAL et NetSEAL

Le gestionnaire de sécurité (module IVNet) nécessite des ressources fournies par le module de base. Vérifiez que ce module de base est installé avant d'installer IVNet.

1. Pour installer les fichiers du gestionnaire de sécurité de Policy Director, tapez le numéro du module IVNet, puis appuyez sur Entrée.

   Les fichiers sont extraits du CD-ROM puis installés sur le disque dur, dans le répertoire par défaut. Un message vous demandera d'entrer le nom et le mot de passe de l'administrateur de la cellule du DCE.

2. Entrez les renseignements nécessaires pour accéder au compte de l'administrateur de la cellule DCE.

```
Entrez le nom utilisateur de
l'administrateur de cellule (cell_admin) :
Entrez le mot de passe de l'administrateur de cellule :
```

Le gestionnaire de sécurité est à présent configuré et initialisé.

Un message annonce la fin de l'installation du module IVNet. La liste des modules disponibles réapparaît.

Activation de WebSEAL

Pour activer WebSEAL, vous devez préalablement installer le module correspondant (IVWeb).

1. Tapez le numéro désignant le module IVWeb pour installer les fichiers nécessaires à l'activation du serveur HTTP WebSEAL.
2. Appuyez sur Entrée pour continuer.

   Les fichiers sont extraits du CD-ROM puis installés sur le disque dur.

   Une liste de configuration apparaît, avec des valeurs confirmant l'accès des clients par HTTP et HTTPS, les ports TCP utilisés et le répertoire racine par défaut des documents Web.
3. Confirmez les valeurs de configuration courantes :

```
Vérifiez
la configuration du serveur Web :
1. Activer TCP HTTP ?                Oui
2. Port HTTP                         80
3. Activer HTTPS ?                   Oui
4. Port HTTPS                        443
5. Racine documents Web              /opt/Policy Director/www/docs

a. Accepter la configuration et poursuivre l'installation
x. Quitter l'installation

Sélectionnez l'élément à modifier : a
```

4. Tapez a pour accepter cette configuration et continuer l'installation, puis appuyez sur Entrée.
5. Entrez les renseignements nécessaires pour accéder au compte de l'administrateur de la cellule DCE.

```
Entrez le nom utilisateur de
l'administrateur de cellule (cell_admin) :
Entrez le mot de passe de l'administrateur de cellule :
```

Le programme d'installation configure et active WebSEAL sur l'ordinateur. Le gestionnaire de sécurité redémarre automatiquement.

Activation de NetSEAL

Pour activer NetSEAL, vous devez préalablement installer le module correspondant (IVTrap).

1. Tapez le numéro désignant le module IVTrap pour installer les fichiers nécessaires à l'activation du composant NetSEAL (contrôle d'accès TCP/IP standard).

   NetSEAL est à présent configuré et activé.

   Un message vous demandera d'entrer le nom et le mot de passe de l'administrateur de la cellule du DCE.

2. Entrez les renseignements nécessaires pour accéder au compte de l'administrateur de la cellule DCE.

   Un message vous informe que vous devez indiquer les ports protégés à l'aide de la commande **ivadmin**.

   Un nouveau message vous demande de réamorcer le système pour placer tous les ports protégés sous le contrôle de NetSEAL.

   Un message annonce la fin de l'installation du module IVTrap. La liste des modules disponibles réapparaît.

Policy Director NetSEAL peut intercepter les requêtes arrivant sur des ports définis. Pour utiliser la fonction d'interception de NetSEAL, vous devez arrêter, puis redémarrer toutes les applications utilisant les ports spécifiés. Pour plus d'informations sur la configuration de Policy Director NetSEAL, reportez-vous à la présentation générale de NetSEAL fournie dans le manuel *Policy Director - Guide d'administration*.

Installation du serveur d'autorisations

Pour installer le serveur d'autorisations :

1. Pour installer les fichiers du serveur d'autorisations de Policy Director, tapez le numéro du module IVAcld, puis appuyez sur Entrée.

   Les fichiers sont extraits du CD-ROM puis installés sur le disque dur, dans le répertoire par défaut. Un message vous demandera d'entrer le nom et le mot de passe de l'administrateur de la cellule du DCE.

2. Entrez les renseignements nécessaires pour accéder au compte de l'administrateur de la cellule DCE.

   ```
   Entrez le nom utilisateur de
   l'administrateur de cellule (cell_admin) :
   Entrez le mot de passe de l'administrateur de cellule :
   ```

   Le serveur d'autorisations est à présent configuré et initialisé.

   Un message annonce la fin de l'installation du module IVAcld. La liste des modules disponibles réapparaît.

Installation de l'API d'autorisation

Pour installer les fichiers de l'API d'autorisation pour langage C, tapez le numéro du module IVAuthADK, puis appuyez sur Entrée.

Les fichiers sont extraits du CD-ROM puis installés sur le disque dur, dans le répertoire par défaut.

Un message annonce la fin de l'installation du module IVAuthADK. La liste des modules disponibles réapparaît.

Configuration du Service d'acquisition de droits d'accès

Le SAD de Policy Director s'installe automatiquement. Pour utiliser ce SAD comme seul et unique service d'acquisition de droits d'accès, vous devez le configurer comme tel. Pour plus d'informations sur la configuration d'un service d'acquisition de droits d'accès, reportez-vous au manuel *Policy Director - Guide d'administration*.

Installation de la console de gestion

Policy Director comporte une console de gestion qui permet de gérer plusieurs de ses composants.

La console de gestion pour Solaris s'installe au moyen du module d'installation IVConsole. Vous devez utiliser la commande **pkgadd** pour installer et configurer ce module.

1. Connectez-vous en qualité d'utilisateur racine.
2. Insérez et montez le CD-ROM intitulé *IBM SecureWay Policy Director version 3.0* dans le lecteur de CD-ROM du serveur Policy Director.
3. Pour afficher la liste des modules disponibles, entrez la commande suivante :

   ```
   # pkgadd -d /cdrom/cdrom0/solaris
   ```
4. Tapez le numéro du module IVBase s'il n'est pas déjà installé. Dans le cas contraire, passez à l'étape 6.
5. Tapez `o` pour continuer.

   La liste des modules apparaît.
6. Tapez le numéro du module IVConsole.
7. Tapez `o` pour continuer.

   Un message vous informe que l'installation a réussi. La console de gestion peut s'initialiser.

Démarrage de la console de gestion

Pour démarrer la console de gestion :

1. Vérifiez que les modules de Policy Director sont installés et actifs.
2. Entrez la commande suivante :

```
$ /opt/intraverse/bin/ivconsole
```

Suppression de Policy Director

La suppression des serveurs de Policy Director se fait au moyen de l'utilitaire **pkgrm**. Les modules doivent être supprimés dans l'ordre inverse de leur installation. Les commandes **pkgrm** et **pkgadd** font partie de la même famille d'utilitaires et utilisent la même interface utilisateur. L'utilitaire **pkgrm** doit être exécuté par l'utilisateur racine.

Cette commande peut être utilisée de plusieurs manières :

- Exécutez la commande **pkgrm** sans argument.

  La liste des modules installés sur l'ordinateur apparaît. Tapez le numéro du module à supprimer.
- Entrez la commande **pkgrm** et spécifiez un nom de module comme argument. Par exemple :

  ```
  # pkgrm IVBase
  ```
- Entrez la commande **pkgrm** et spécifiez une suite de noms de module comme arguments. Par exemple :

  ```
  # pkgrm IVAuthADK IVAcld IVTrap IVWeb IVNet IVMgr IVBase
  ```

Pour plus d'informations sur la commande **pkgrm**, reportez-vous à la documentation du système d'exploitation Solaris.

Remarque : Vous devez supprimer les modules de Policy Director dans l'ordre inverse de leur installation.

Pour supprimer Policy Director :

1. Connectez-vous en qualité d'utilisateur racine.

   Utilisez l'une des méthodes précédentes pour exécuter la commande **pkgrm**.
2. Les composants de Policy Director doivent être supprimés dans l'ordre suivant :
   - IVTrap
   - IVWeb
   - IVNet
   - IVAuthADK
   - IVAcld
   - IVMgr
   - IVBase

   Votre configuration ne comprend pas nécessairement tous les modules figurant dans cette liste. La console de gestion de Policy Director (IVConsole) peut être supprimée à tout moment, avant le module de base (IVBase).

Suppression de la console de gestion

Pour supprimer la console de gestion :

1. Connectez-vous en qualité d'utilisateur racine.
2. Entrez la commande suivante :

```
# pkgrm ivconsole
```

Chapitre 8. Documentation annexe

Vous pouvez utiliser les documents présentés dans ce chapitre pour obtenir plus d'informations sur le produit Policy Director version 3.0 et sur les produits annexes.

Documentation de Policy Director

Le présent manuel, *IBM SecureWay Policy Director version 3.0 - Guide de configuration et d'utilisation* est fourni avec le produit Policy Director. Il est également disponible dans une série de documents. La documentation de Policy Director comprend ce manuel et les informations liées aux licences d'utilisation de Policy Director.

En plus de ce manuel, des documents sur Policy Director sont disponibles au format PDF (PostScript Document Format) dans le sous-répertoire /doc du CD-ROM *IBM SecureWay Policy Director version 3.0* :

- *IBM SecureWay Policy Director version 3.0 - Guide d'administration*

  Ce manuel fournit des instructions détaillées pour l'administration de Policy Director. Il détaille les fonctionnalités du produit IBM SecureWay Policy Director, notamment :

  - Concepts de Policy Director (notamment l'authentification, l'autorisation et l'acquisition des droits d'accès)
  - Tâches d'administration générale avec la console de gestion
  - Administration de WebSEAL
  - Administration de NetSEAL
  - Administration de NetSEAT
  - Ressources d'administration (utilitaire **ivadmin**)
- *IBM SecureWay Policy Director version 3.0 - Guide de programmation et de référence*

  Ce manuel couvre les composants de l'API d'autorisation et les procédures à suivre pour les opérations suivantes :
  - Création d'applications avec l'API d'autorisation
  - Initialisation du service d'autorisation de Policy Director
  - Authentification d'un serveur d'applications ou d'un client
  - Obtention de droits d'accès par un utilisateur
  - Processus des décisions d'autorisation
  - Exécution des tâches optionnelles
  - Nettoyage et arrêt du système
  - Déploiement des applications avec l'API d'autorisation

Le fichier README de Policy Director contient des informations de dernière minute sur Policy Director. Ces informations remplacent celles des manuels.

Pour obtenir le dernier fichier README disponible, contactez le site WEB d'IBM SecureWay Policy Director, à l'adresse suivante :

`http://www.ibm.com/software/security/policy/library`

Documentation du produit IBM SecureWay FirstSecure

Le manuel suivant contient des informations sur FirstSecure :

- *IBM SecureWay FirstSecure version 2.0 - Guide de planification et d'intégration (STC7-EHFR-00)*

  Ce manuel décrit FirstSecure et ses composants. Il couvre également la préparation des systèmes à l'utilisation de tous les produits IBM SecureWay.

IBM SecureWay Policy Director (Policy Director) est disponible comme composant du progiciel IBM SecureWay FirstSecure et comme produit autonome. Si vous avez acquis Policy Director dans le cadre de la solution FirstSecure, ce manuel est fourni avec cette solution. Si vous avez acquis Policy Director comme programme autonome, vous pouvez vous procurer ce manuel sur le site Web de FirstSecure à l'adresse suivante :

`http://www.ibm.com/software/security/firstsecure/library`

Documentation sur IBM Distributed Computing Environment (DCE)

Les documents suivants expliquent comment installer l'environnement informatique partagé DCE et sont disponibles sur le CD-ROM *IBM SecureWay Policy Director Security Services*, au format PDF (répertoire /doc) ou sur le site WEB consacré au produit DCE :

`http://www.ibm.com/network/dce/library/`

IBM DCE pour Windows NT

Le manuel *IBM Distributed Computing Environment for Windows NT Quick Beginnings, Version 2.2* est disponible à l'adresse Web :

`http://www.software.ibm.com/network/dce/library/publications/dcent.html`

Ce manuel décrit le produit IBM Distributed Computing Environment (DCE) pour Windows NT version 2.2 et explique comment planifier, installer et configurer ce produit.

Le manuel *IBM Distributed Computing Environment for Windows NT Quick Beginnings, Version 2.2*, est également disponible sur le CD-ROM *IBM SecureWay Policy Director Security Services*, dans le répertoire /doc/DCE22_QuickBeginnings_NT.pdf.

IBM DCE pour AIX

Le manuel *IBM Distributed Computing for AIX Quick Beginnings Version 2.2* est disponible à l'adresse Web :

`http://www.software.ibm.com/network/dce/library/publications/dceaix.html`

Ce manuel décrit le produit IBM Distributed Computing Environment pour AIX version 2.2 (DCE 2.2 pour AIX) et explique comment planifier, installer et configurer ce produit.

Le manuel *IBM Distributed Computing Environment for AIX Quick Beginnings, Version 2.2*, est également disponible sur le CD-ROM *IBM SecureWay Policy Director Security Services*, dans le répertoire /doc/DCE22_QuickBeginnings_AIX.pdf.

Transarc DCE pour Solaris

Les manuels *Transarc DCE Version 2.0 Release Notes* et *Guide d'installation et de configuration* sont disponibles à l'adresse Web :

`http://www.transarc.com/library/documentation/dce/2.0/index.html`

Le document *Transarc DCE Version 2.0 Release Notes* couvre les aspects suivants du produit Transarc DCE :

- Différences entre OSF DCE et DCE * DFS
- Différences entre les versions 2.0 et 1.1 de DCE * DFS
- Limites et incidents connus de DCE * DFS

Le document *Transarc DCE Version 2.0 Release Notes* est également disponible sur le CD-ROM *IBM SecureWay Policy Director Security Services*, dans le répertoire /doc/DCE20_ReleaseNotes_Solaris.pdf.

Le *Guide d'installation et de configuration* couvre l'installation, la configuration et la mise à niveau du produit DCE DFS version 2.0.

Le *Guide d'installation et de configuration* est également disponible sur le CD-ROM *IBM SecureWay Policy Director Security Services*, dans le répertoire /doc/DCE20_InstallGuide_Solaris.pdf.

Documentation du produit IBM SecureWay Directory

Le manuel suivant contient des informations en rapport avec l'installation et la configuration du produit IBM SecureWay Directory (LDAP) :

- *IBM SecureWay Directory version 3.1.1 - Installation et configuration*

  Il existe une version de ce manuel au format HTML pour chaque système d'exploitation pris en charge. Le manuel associé à chaque système d'exploitation se trouve sur le CD-ROM correspondant, dans le fichier /doc/wparent.htm. Les CD-ROM fournis sont les suivants :

  – *IBM SecureWay Directory version 3.1.1 pour Windows NT*

  – *IBM SecureWay Directory version 3.1.1 pour AIX*

  – *IBM SecureWay Directory version 3.1.1 pour Solaris*

  Après l'installation de LDAP, l'emplacement du fichier .htm contenant les informations sur l'installation et la configuration est :

  ```
  C:\Program
  Files\IBM\LDAP\nls\html\enUS1252\config\wparent.htm
  ```

Le manuel suivant (fichier HTML) contient des informations sur l'administration d'IBM SecureWay :

- *IBM SecureWay Directory version 3.1.1- Guide d'administration*

  1. Après avoir réalisé une installation standard de LDAP, vous pouvez accéder aux documents disponibles à l'adresse Web suivante :

     ```
     C:\Program
     Files\IBM\LDAP\nls\html\enUS1252\config\wparent.ht
     ```

Le manuel suivant (format HTML) contient des informations sur le client IBM SecureWay Directory :

- *IBM SecureWay Directory Client SDK Programming Reference, Version 3.1.1*

  Ce manuel contient des liens renvoyant aux informations suivantes sur LDAP :

  – Informations du manuel LDAP Client SDK Plugin Programming Reference.

    1. Après avoir réalisé une installation standard de LDAP, vous pouvez accéder aux documents disponibles à l'adresse Web suivante :

       ```
       C:\Program Files\IBM\doc\progref.htm
       ```

    2. Ouvrez le document *IBM SecureWay Directory Client SDK Programming Reference*.
    3. Cliquez sur **Appendices**.
    4. Cliquez sur **LDAP Client SDK Plugin Programming Reference**.

  – Informations couvrant l'utilisation de GSKit et de l'utilitaire de gestion des clés **ikmguiw** pour configurer le serveur LDAP avec SSL.

1. S'il n'est pas déjà ouvert, ouvrez le document *IBM SecureWay Directory Client SDK Programming Reference*.
2. Cliquez sur **API categories**.
3. Cliquez sur **SSL**.
4. Cliquez sur **LDAP_SSL API**.
5. Recherchez le lien **Using IKMGUI** pour ouvrir le fichier HTML approprié.

Le document suivant se rapporte également au serveur IBM SecureWay Directory :

- *IBM SecureWay Directory Server Plug-ins Reference*

Annexe. Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Cela ne signifie pas qu'IBM ait l'intention de les y annoncer. 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.

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.

Le présent document peut également contenir des programmes réduits fournis par IBM à titre de simple exemple et d'illustration. Ces programmes n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes. LES GARANTIES IMPLICITES DE QUALITE MARCHANDE OU D'ADAPTATION A VOS BESOINS SONT EXPRESSEMENT EXCLUES.

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 brevets. 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 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
Department LZKS
11400 Burnet Road
Austin, TX 78758
U.S.A.

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux termes du Contrat sur les produits et services IBM, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut

confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

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.

Tous les tarifs indiqués sont les prix de vente actuels suggérés par IBM et sont susceptibles d'être modifiés sans préavis. Les tarifs appliqués peuvent varier selon les revendeurs.

Marques

Les termes qui suivent sont des marques d'International Business Machines Corporation dans certains pays :

AIX
DB2
FirstSecure
IBM
Policy Director
SecureWay

Les termes qui suivent sont des marques d'autres sociétés :

AuthAPI	DASCOM Inc.
DASCOM	DASCOM Inc.
Internet Explorer	Microsoft Corporation
Netscape et logos Netscape	Netscape Communications Corporation
Netscape Communicator	Netscape Communications Corporation
Netscape Navigator	Netscape Communications Corporation
NetSEAL	DASCOM Inc.
NetSEAT	DASCOM Inc.
Solaris	Sun Microsystems Inc.
WebSEAL	DASCOM Inc.

Java et toutes les marques et logos incluant Java, sont des marques de Sun Microsystems, Inc.

Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation dans certains pays.

UNIX est une marque enregistrée aux Etats-Unis et/ou dans d'autres pays. Unix et utilisée avec l'autorisation exclusive de la société X/Open Company Limited.

Index

D

E

F

G

I

K

L

M

N

O

P

R

S

T

U

V

W

Référence: CT63KFR

CT63KFR