IBM SecureWay Policy Director Version 3.0 - Guide d'administration

IBM SecureWay Policy Director Version 3.0 - Guide d'administration

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Annexe B. Remarques» à la page 299.

Octobre 1999

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 détaille les fonctionnalités du produit IBM SecureWay Policy Director, notamment :

- Concepts de Policy Director, notamment : authentification, autorisation et acquisition de 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**).

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

Ce manuel s'adresse aux administrateurs en charge de la gestion des utilisateurs de Policy Director, des groupes, des ressources GSO et des groupes de ressources GSO, des utilisateurs relais, des listes de contrôle d'accès, des autorisations et de l'espace des objets.

La personne chargée d'administrer Policy Director doit également connaître et gérer les procédures d'authentification, d'autorisation et d'acquisition de droits d'accès.

L'administrateur doit être familiarisé avec la gestion 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 se décompose de la manière suivante :

- Les chapitres 1 à 3 décrivent les principes et concepts de Policy Director, en particulier dans les sections «Chapitre 1. Bienvenue dans Policy Director» à la page 1, «Chapitre 2. Authentification et acquisition de droits d'accès» à la page 17 et «Chapitre 3. Principes de l'autorisation» à la page 35.
- Les chapitres 4 à 12 exposent les tâches d'administration de Policy Director :
  - «Chapitre 4. Présentation de la console de gestion» à la page 55
  - «Chapitre 5. Gestion des comptes des utilisateurs et des groupes» à la page 69
  - «Chapitre 6. Gestion des ressources GSO, des groupes de ressources et des droits d'accès des ressources» à la page 75
  - «Chapitre 7. Principes du contrôle d'accès» à la page 81
  - «Chapitre 8. Application du contrôle d'accès» à la page 107
  - «Chapitre 9. Gestion des utilisateurs relais» à la page 113
  - «Chapitre 10. Gestion des serveurs de Policy Director» à la page 123
  - «Chapitre 11. Gestion du service d'autorisation» à la page 133
  - «Chapitre 12. Journalisation et audit de l'activité du serveur» à la page 145

Les chapitres 13 à 16 couvrent l'administration de WebSEAL :

- «Chapitre 13. WebSEAL - Configuration de l'authentification» à la page 159
- «Chapitre 14. WebSEAL - Tâches d'administration générale» à la page 179

- «Chapitre 15. WebSEAL - Administration des jonctions intelligentes» à la page 189
- «Chapitre 16. WebSEAL - Intégration des applications» à la page 219

Les chapitres 17 et 18 détaillent les aspects suivants de NetSEAL :
- «Chapitre 17. Présentation générale de NetSEAL» à la page 229
- «Chapitre 18. NetSEAL - Tâches d'administration générale» à la page 243

Les chapitres 19 à 21 couvrent l'administration de NetSEAT :
- «Chapitre 19. Présentation générale de NetSEAT» à la page 251
- «Chapitre 20. NetSEAT - Tâches d'administration générale» à la page 257
- «Chapitre 21. NetSEAT - Répartiteur des services de répertoire (RSR)» à la page 273

Ce manuel comporte les annexes «Annexe A. Administration de Policy Director avec l'utilitaire ivadmin» à la page 277 et «Annexe B. Remarques» à la page 299.

Conventions utilisées dans ce manuel

Ce manuel utilise les conventions typographiques suivantes :

Convention	Signification
gras	Eléments d'interface utilisateur graphique (GUI) tels que noms et options de menu, zones de saisie, icônes, dossiers, zones de liste, noms de bouton ou cases à cocher. Egalement utilisé pour les remarques et les avertissements.
`monospace`	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 : Sélectionnez **Fichier** → **Exécuter** signifie : Cliquez sur **Fichier**, puis cliquez sur **Exécuter**.

Compatibilité avec l'an 2000

Ces produits sont conçus pour passer l'an 2000 sans incident. Utilisés conformément aux recommandations de leurs manuels, 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. Certains de ces produits peuvent impliquer 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.

Configuration requise et documentation rattachée

Reportez-vous aux documents suivants pour plus d'informations sur les conditions d'utilisation de Policy Director et sur les produits associés.

IBM SecureWay Policy Director

Documentation au format PDF : Les manuels suivants se rapportent à Policy Director et sont disponibles au format PDF dans le répertoire /doc du CD-ROM d'IBM SecureWay Policy Director Version 3.0 :

- Ce manuel, IBM SecureWay Policy Director version 3.0 - Guide d'administration
- IBM SecureWay Policy Director version 3.0 - Guide de programmation et de référence

Documentation imprimée : Le manuel suivant se rapporte également à Policy Director et est fourni en version imprimée avec le produit.

IBM SecureWay Policy Director version 3.0 - Guide de configuration et d'utilisation (SCT6-3KNA-00)

IBM SecureWay FirstSecure

Le manuel suivant se rapporte à IBM SecureWay FirstSecure :

- IBM SecureWay FirstSecure version 2.0 - Guide de planification et d'intégration (S564-8D11-00)

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

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 - Services de sécurité, au format PDF (répertoire /doc) ou sur le site WEB DCE.

IBM DCE pour Windows NT

IBM Distributed Computing Environment for Windows NT Quick Beginnings, Version 2.2, 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.

IBM DCE pour AIX

IBM Distributed Computing for AIX Quick Beginnings Version 2.2, 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.

Transarc DCE pour Solaris

Transarc DCE Version 2.0 Release Notes et Guide d'installation et de configuration, 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 inconvénients connus de DCE DFS.

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

IBM SecureWay Directory

Les documents suivants se rapportent également à IBM SecureWay Directory :

- IBM SecureWay Directory version 3.1.1 - Installation et configuration

  Il existe une version de ce manuel pour chaque système d'exploitation pris en charge.
- IBM SecureWay Directory Client SDK Programming Reference
- IBM SecureWay Directory Server Plug-ins Reference

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. Les CD-ROM fournis sont les suivants :
  - IBM SecureWay Directory version 3.11 pour NT
  - IBM SecureWay Directory version 3.11 pour AIX
  - IBM SecureWay Directory version 3.11 pour Solaris

Les documents suivants se rapportent également à IBM SecureWay Directory :

- IBM SecureWay Directory Client SDK Programming Reference
- IBM SecureWay Directory Server Plug-ins Reference

Comment nous faire part de vos commentaires ?

Vos commentaires nous aident à améliorer la qualité et la précision des informations que nous proposons. Pour nous adresser vos suggestions et remarques sur ce manuel ou sur tout autre document en rapport avec IBM SecureWay Policy Director, consultez la page d'accueil du site de Policy Director à l'adresse suivant :

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

Vous y trouverez une page spécialement destinée à recueillir vos commentaires ainsi que des informations sur les dernières mises à jour de Policy Director.

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. Bienvenue dans Policy Director

IBM SecureWay Policy Director (Policy Director) est une solution complète pour la gestion des autorisations destinée aux applications client-serveur, Web et autres. Policy Director permet de contrôler en toute sécurité l'accès des utilisateurs aux informations protégées. Ce produit s'utilise en association avec les applications Internet standard pour mettre en oeuvre des intranets fonctionnels et hautement sécurisés.

Ce chapitre comprend les sections suivantes :

Principes de la sécurité des réseaux d'entreprise

De nombreuses organisations considèrent désormais l'Internet et les intranets privés comme des outils efficaces, et même vitaux, pour les communications internationales. De plus en plus, le commerce électronique devient un aspect essentiel de la stratégie commerciale pour de nombreuses entreprises. L'enseignement à distance que dispensent nombre d'écoles et universités repose lui aussi sur l'Internet. Les services en ligne permettent d'envoyer des courriers électroniques et de puiser dans l'immense encyclopédie du Web. Des applications traditionnelles, telles que TELNET ou POP3, sont toujours des services de réseau très appréciés.

Les entreprises comprennent qu'elles peuvent utiliser les technologies Internet pour améliorer les processus d'approvisionnement ainsi que les relations et l'interaction avec leurs partenaires commerciaux. Elles peuvent le faire, sous réserve de mettre en oeuvre les ressources nécessaires dans les conditions de sécurité qui s'imposent.

Les entreprises veulent utiliser l'Internet comme vecteur de commercialisation et de distribution à l'échelle internationale. Toutefois, le manque de systèmes de sécurité et de gestion probants les a souvent freinées dans ce projet.

Policy Director est une solution de gestion de la sécurité des données comportant des services de protection de réseau centralisés. Ces services permettent de mettre en place et de gérer des systèmes de sécurité et de gestion des utilisateurs cohérents et fiables.

Terminologie et définitions de la sécurité de réseau

Les services et concepts de sécurité de réseau suivants sont des éléments importants que vous trouverez à maintes reprises dans ce manuel consacré à Policy Director.

Domaine sécurisé
: Groupe d'utilisateurs, de systèmes et de ressources partageant des services communs et ayant, habituellement, une fonction commune.

Authentification
: Processus consistant à identifier une personne qui tente de se connecter à un domaine sécurisé.

droits d'accès
Informations communiquées au cours de l'authentification, qui décrivent l'utilisateur, les associations de groupe (le cas échéant), et d'autres attributs d'identité en rapport avec la sécurité.

Autorisation Processus visant à déterminer si une personne a le droit d'exécuter une opération sur une ressource protégée.

Chiffrement Conversion de données informatiques en un code secret qui empêche les personnes non autorisées d'en prendre connaissance.

Intégrité Faculté des données à ne pas changer entre le moment où elles sont envoyées et le moment où elles sont reçues.

Niveau de protection
Niveau de sécurité des données, déterminé par leurs conditions d'authentification, d'intégrité et de confidentialité.

Modularité Faculté d'un système de réseau à répondre à un nombre croissant d'utilisateurs désirant accéder aux ressources.

Questions courantes sur la sécurité de réseau

Le réseau mondial Internet comme les intranets des entreprises se connectent à des systèmes informatiques, des applications et des réseaux hétérogènes. Cet ensemble de matériels et de logiciels dépareillés a souvent les incidences suivantes sur un réseau :

- Absence de contrôle centralisé de la sécurité des applications ;
- Absence de convention d'appellation uniforme pour les emplacements des ressources ;
- Absence de support commun pour l'accessibilité avancée des applications ;
- Absence de support commun pour la croissance évolutive des réseaux.

Les nouveaux modèles économiques demandent aux entreprises de communiquer des informations à un niveau que nul n'avait prévu. Ces entreprises ont besoin de savoir qu'elles peuvent contrôler l'accès à ces ressources en toute sécurité.

Gérer les règles de sécurité et les utilisateurs dans les réseaux partagés est une tâche ardue pour les personnes chargées des technologies de l'information. La difficulté vient notamment du fait que chaque fabricant de logiciels ou de matériels met en oeuvre ses propres méthodes de contrôle d'autorisation.

Les entreprises réalisent que développer des services d'application pour chacune de leurs applications est un processus coûteux qui génère une infrastructure difficile à administrer. Un service d'autorisation centralisé, auquel les développeurs pourraient accéder via une interface de programme d'application (API), réduirait notablement le temps de mise sur le marché et le coût total de détention des ressources.

Un système de gestion centralisée de la sécurité de réseau doit répondre aux exigences suivantes :

- Coexistence et articulation avec les architectures des systèmes d'authentification et de pare-feu existants ;
- Intégration ou coexistence avec les systèmes de gestion d'applications et de réseaux existants.
- Indépendance par rapport aux applications.

Présentation de Policy Director

Policy Director est une solution complète de gestion des autorisations et de la sécurité des réseaux qui permet d'assurer une protection totale des ressources dans des réseaux internes et externes géographiquement dispersés. 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.

Outre ses remarquables fonctions de gestion des règles de sécurité, Policy Director offre des services d'authentification, d'autorisation et de gestion des ressources. Ce produit s'articule avec les applications Internet standard pour mettre en oeuvre des intranets fonctionnels et hautement sécurisés.

Policy Director permet aux entreprises de gérer en toute sécurité l'accès par réseau à leurs ressources internes. Ces entreprises peuvent aussi pleinement profiter de la connectivité et de la convivialité de l'Internet. Couplé à un pare-feu, Policy Director peut protéger l'intranet de l'entreprise contre les intrusions et accès non autorisés.

Standard de l'API de service d'autorisation de Policy Director

Les services d'autorisation constituent une partie vitale de l'architecture de sécurité d'une application. Lorsque l'utilisateur a suivi le processus d'authentification, les services d'autorisation appliquent les règles de sécurité de l'entreprise et déterminent les services et données auxquels il pourra accéder.

Par exemple, un utilisateur accédant au site Web d'une caisse de retraite peut consulter les données de son compte. Avant de pouvoir consulter ces données, un serveur d'autorisations doit vérifier l'identité, les droits d'accès et les privilèges de cet utilisateur.

L'API d'autorisation standard de Policy Director permet aux applications d'appeler le service d'autorisation centralisé de Policy Director. Cette possibilité évite aux développeurs de devoir élaborer un code d'autorisation pour chaque nouvelle application.

L'API d'autorisation de Policy Director permet de standardiser toutes les applications avec un système d'autorisation sécurisé. Elle permet également aux entreprises de mieux contrôler l'accès aux ressources proposées par leurs réseaux.

Pour une information et une description complètes de l'API d'autorisation de Policy Director, reportez-vous au manuel Policy Director - Guide de programmation et de référence.

Technologies fondamentales de Policy Director

La solution de gestion de la sécurité des réseaux Policy Director repose sur les technologies fondamentales suivantes :

- Authentification
- Autorisation
- Niveau de protection des données
- Modularité
- Contrôle d'activité

Authentification

Cette technologie fondamentale s'appuie sur l'application de méthodes d'authentification par nom d'utilisateur et mot de passe Policy Director.

Clé secrète:

- Kerberos ;
- Protocole LDAP (Lightweight directory access protocol).

Clé publique/privée:

- Connexion par navigateur SSL (secure socket layer) avec nom d'utilisateur et mot de passe définis par l'application :
  - Méthode d'authentification de base (uniquement WebSEAL et le protocole HTTPS de l'interface SSL) ;
  - Méthodes d'authentification par formulaires de Policy Director (uniquement WebSEAL et HTTPS).
- Connexion SSL par certificat X.509 de côté client (Policy Director gère les produits PKI/PKIX tels que IBM SecureWay Trust Authority version 3.1 ou les produits PKI/Entrust tels que IBM Vault Registry version 2.2.2).

  IBM SecureWay Trust Authority version 3.1 comprend un logiciel client, une application d'enregistrement simple, une autorité de certification et un répertoire intégré pour gérer l'ensemble du cycle des certificats (enregistrement et première certification, mise à jour des paires de clés et des certificats, liste des certificats et liste des révocations de certificat, procédure de révocation des certificats). Une interface utilisateur graphique permet de gérer les requêtes adressées à l'autorité de certification, à l'autorité d'enregistrement et au programme End Entity (EE). Une bibliothèque d'API est également fournie.

Acquisition des droits d'accès:

- Service d'acquisition de droits d'accès SAD (extensions d'authentification personnalisée).

Autorisation

Cette technologie fondamentale permet la mise en oeuvre des types d'autorisation Policy Director suivants :

- Le service d'autorisation Policy Director ;
- L'API d'autorisation standard de Policy Director ;
- Un service d'autorisation externe.

Niveau de protection des données

Le niveau de protection caractérise le degré selon lequel Policy Director protège les données transmises entre le client et le serveur. Ce niveau de protection est déterminé par l'effet combiné des processus de transmission par tunnel, des normes de chiffrement et des algorithmes de détection de modification.

Par ordre croissant de sécurité, les niveaux de protection comprennent :

1. Communication TCP (transmission control protocol) standard (sans authentification) ;
2. Authentification uniquement (vérifie l'identité de l'utilisateur) ;
3. Authentification + intégrité des données (protège le contenu des messages contre toute modification pendant la transaction de réseau) ;
4. Authentification + intégrité des données + confidentialité (protège les messages contre la modification ou la lecture non autorisée pendant la transaction de réseau).

Vous pouvez définir les niveaux de protection désirés pour les différents systèmes hôtes et les réseaux.

Normes de chiffrement prise en charge: Policy Director prend en charge les systèmes de chiffrement de données DES (data encryption standard) et non DES suivants par SSL :

- RC2 40 bits
- RC2 128 bits
- RC4 40 bits
- RC4 128 bits
- DES 40 bits
- DES 56 bits
- Triple DES 168 bits

Policy Director NetSEAL et Policy Director WebSEAL prennent en charge le chiffrement DES 40 et 56 bits par DCE-RPC.

Remarque : Les versions nationales peuvent être soumises à des restrictions d'exportation sur les techniques de chiffrement.

Processus de transmission par tunnel: Policy Director prend en charge les protocoles suivants pour la transmission des données codées :

- Transmission par tunnel SSL (Secure socket layer) ;
- Transmission par tunnel GSS (Generic security service).

WebSEAL prend en charge les systèmes de protection d'intégrité et de confidentialité des données du tunnel codé par 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. Ces tentatives de détournement par relecture interviennent lorsque les données d'un utilisateur sont interceptées entre le client de cet utilisateur et le serveur. Le fraudeur va ensuite relire ces données ou les retransmettre au serveur afin de se substituer au premier utilisateur.

Transmission par tunnel SSL : Le protocole SSL permet l'échange de signaux visant à établir une communication entre deux modems. 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 serveurs 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, tels 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 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 Policy Director.

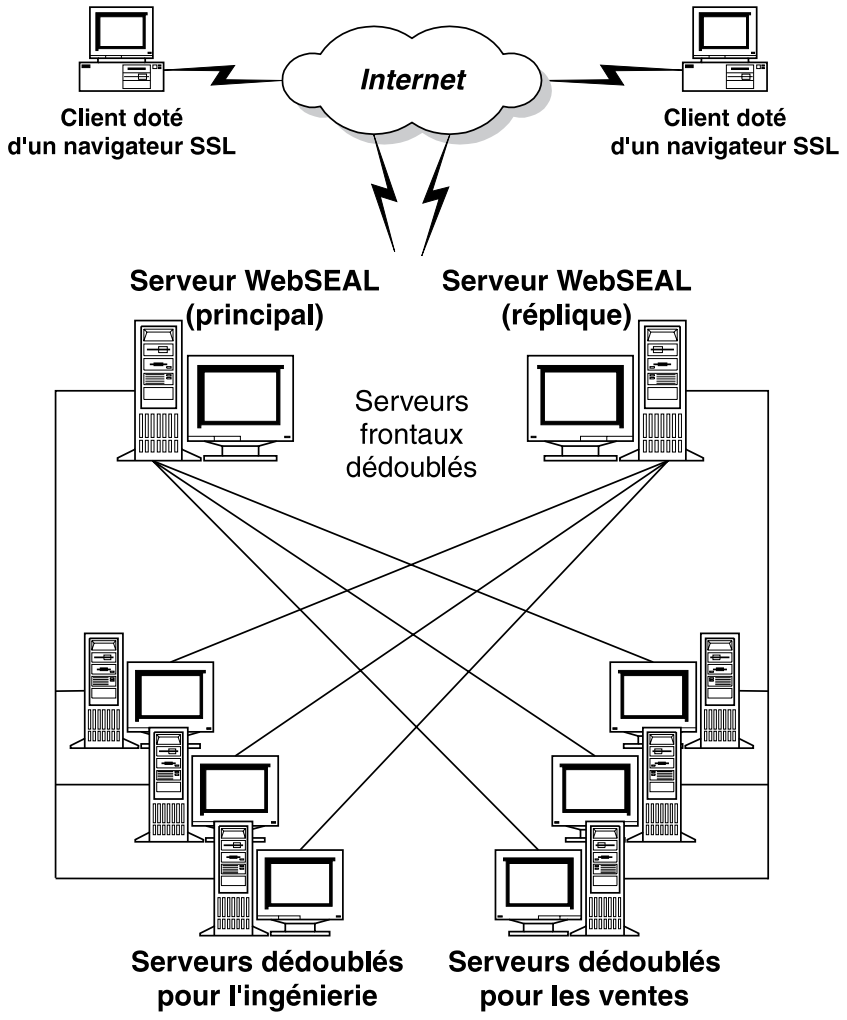
La transmission par tunnel GSS apporte des services de sécurité génériques aux programmes appelants. Ce système repose sur un certain nombre de mécanismes et technologies sous-jacents. Il permet la portabilité des applications vers différents

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.

Modularité

La modularité est la faculté de répondre à un nombre croissant d'utilisateurs désirant accéder aux ressources d'un domaine sécurisé. Pour répondre à cette exigence de modularité, Policy Director applique les techniques suivantes :

- Duplication des services
  - Services d'authentification
  - Services d'autorisation
  - Règles de sécurité
  - Services de chiffrement des données
  - Services d'audit
- Serveurs WebSEAL frontaux dupliqués
  - Copie miroir des ressources pour accessibilité avancée
  - Equilibrage de charge entre les requêtes des clients
- Serveurs d'arrière-plan dupliqués
  - Serveurs d'arrière-plan (serveurs WebSEAL ou serveurs Web tiers)
  - Copie miroir des ressource (espace des noms unifié) pour accessibilité avancée
  - Contenu et ressources supplémentaires
  - Equilibrage de charge des requêtes entrantes via la technologie Smart Junction
- Optimisation des performances par la répartition des services d'authentification et d'autorisation entre différents serveurs
- Déploiement adaptatif des services sans augmentation des tâches de gestion



Contrôle d'activité

Policy Director propose un certain nombre de fonctions d'audit et de journalisation. Des fichiers journaux consignent les messages d'erreur et d'avertissement générés par les serveurs Policy Director et les serveurs DCE (environnement informatique partagé). De plus, des fichiers d'audit permettent de suivre l'activité de Policy Director et des serveurs DCE.

Fichiers journaux

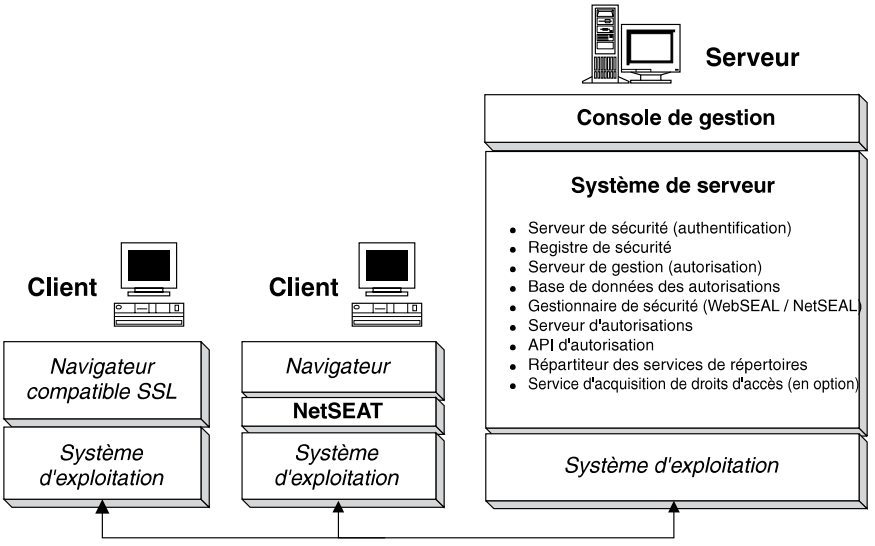
- Fichiers journaux des serveurs Policy Director
- Fichiers journaux des serveurs DCE
- Messages de mise en service DCE
- Fichiers journaux HTTP (HyperText Transfer Protocol) standard

Fichiers d'audit

- Fichiers d'audit des autorisations de Policy Director
- Fichier d'audit WebSEAL
- Fichier d'audit de la gestion de Policy Director
- Fichier d'audit du DCE
- Fichier d'audit LDAP

Composants de Policy Director

Policy Director comprend des logiciels pour systèmes client et serveur. Vous pouvez l'installer sur les plates-formes avec système d'exploitation Sun Solaris, IBM AIX et Microsoft Windows NT.



Console de gestion

La console de gestion 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 la base de données des règles d'autorisation principale (ou primaire).

Les tâches de la console de gestion permettent notamment la création et la suppression de comptes utilisateurs et de groupes de comptes ou l'application de listes de contrôle d'accès aux objets de l'espace des noms. La console de gestion utilise les appels de processus à distance (RPC) sécurisés pour exécuter ces tâches de gestion par le biais de canaux de communication sécurisés.

Vous pouvez déléguer des responsabilités de gestion au niveau local. Par exemple, vous pouvez désigner un administrateur de la sécurité doté de responsabilités limitées. Cet administrateur sera alors habilité à gérer les règles de sécurité pour les ressources placées dans une partie désignée de l'espace des noms d'objet protégé.

Serveur de sécurité

Le serveur de sécurité (secd) peut être soit un serveur LDAP, soit un serveur DCE. Le serveur de sécurité fournit des services d'authentification et gère également une base de données de registre centralisée (LDAP ou DCE) qui contient les entrées de compte rattachées à tous les utilisateurs autorisés à accéder au domaine sécurisé.

Dans un environnement informatique partagé (DCE), les utilisateurs de la base de données du registre sont parfois appelés des principaux.

Le serveur de sécurité a deux fonctions importantes :

- Il définit les groupes et les organisations auxquels l'utilisateur appartient ainsi que les fonctions qu'il peut exercer. La base de données centralisée du registre contient ces informations. Le service d'autorisation de Policy Director prend en compte ces informations pour accorder ou non une autorisation.

- Le serveur de sécurité fournit des services d'authentification lors des tentatives de connexion.

Pour le DCE, le serveur de sécurité peut reproduire la base de données du registre dans tout le domaine sécurisé afin d'éviter la présence d'impasses. Il assure la mise à jour de toutes les instances de la base de données en cas de modification du registre principal.

Serveur de gestion

Le serveur de gestion (ivmgrd) gère la base de données primaire des règles d'autorisation attachée au domaine sécurisé. Il assure également la mise à jour de toutes les instances de la base de données des autorisations à travers le domaine sécurisé. Enfin, il administre les données d'emplacement des autres serveurs Policy Director du domaine sécurisé.

Gestionnaire de sécurité

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

- un composant NetSEAL permettant un contrôle de base des accès par TCP/IP (Transmission Control Protocol/Internet Protocol).
- un composant WebSEAL permettant un contrôle d'accès renforcé sur les transactions HTTP et HTTPS.

WebSEAL

WebSEAL est l'un des deux composants du gestionnaire de sécurité (secmgrd).

WebSEAL est un serveur Web multithread (utilisant simultanément plusieurs unités d'exécution), capable d'accepter les requêtes HTTP et HTTPS comme celles du client NetSEAT. WebSEAL administre le contrôle d'accès pour des ressources telles que :

- les adresses URL (Universal Resource Location) ;
- les expressions régulières avec URL ;
- les programmes CGI en Perl, C, ou C++ ;
- les fichiers HTML (Hypertext Markup Language) ;
- les servlets Java ;
- les fichiers de classes Java.

WebSEAL, en tant que serveur de jonction, protège et administre les serveurs Web tiers à l'aide de la technologie Smart Junction. Les jonctions intelligentes issues de cette technique permettent d'associer des systèmes de fichiers de serveur supplémentaires à l'espace Web et de traiter les ressources comme un espace de noms d'objet unifié.

WebSEAL permet d'attacher les mêmes fonctions de connexion à vos différentes ressources Web. L'utilisateur est authentifié par le serveur WebSEAL par le biais du système Kerberos standard ou de la couche SSL. WebSEAL identifie ensuite cet utilisateur au moyen des méthodes d'authentification HTTP standard et simplifiée. Le serveur WebSEAL peut également utiliser l'identité de l'utilisateur comme variable CGI.

NetSEAL

NetSEAL est l'un des deux composants du gestionnaire de sécurité (secmgrd). Il s'agit d'une solution de réseau privé virtuel (RPV) permettant de sécuriser toutes

les communications TCP/IP en entrée. NetSEAL assure un contrôle d'accès sur la base du port de destination utilisé par le client et de son identité. NetSEAL est une solution de sécurité qui permet de :

- autoriser et sécuriser les services Internet conventionnels tels que TELNET et POP3 ;
- autoriser et sécuriser divers progiciels d'application tels que les systèmes de base de données et les outils de gestion de réseau.

Le composant NetSEAL est un gestionnaire de ressources qui contrôle la capacité des utilisateurs à se connecter à un port défini du serveur (le port 23, TELNET, etc.). Il permet aussi d'accepter et d'autoriser les transactions TCP/IP acheminées par tunnel à partir du client NetSEAT.

Le serveur NetSEAL permet l'intégration de n'importe quel serveur d'applications du réseau avec les services de sécurité de Policy Director. Il constitue aussi un point d'arrivée pour tunnel sécurisé, pour toutes les communications du réseau. L'identité authentifiée de l'utilisateur est transmise avec la requête d'origine via le tunnel SSL ou GSS. Utilisez des tunnels SSL NetSEAL pour communiquer avec le client NetSEAT.

Client NetSEAT

NetSEAT est un module de prise en charge de réseau. Ce module fonctionne de manière transparente comme serveur relais sécurisé pour les applications client. Il permet de coder les données pendant tout le processus de transmission par tunnel SSL ou GSS, pour toutes les transactions client-serveur. Grâce à sa fonction de bibliothèque DLL, le client NetSEAT permet aux utilisateurs d'exploiter pleinement les capacités de Policy Director. Ces capacités comprennent notamment la sécurisation des communications de données et la mise en oeuvre d'une accessibilité avancée.

Le client NetSEAT s'intègre totalement avec le système de sécurité de Policy Director et permet de gérer les ressources pour le compte du client. En outre, il assure la protection des applications TCP/IP. NetSEAT code de manière transparente les données des applications transmises par les tunnels (SSL ou GSS) du RPV, qui peuvent dès lors transiter par des liaisons non sécurisées (telles que celles de l'Internet).

Vous pouvez configurer le client NetSEAT de manière à intercepter les requêtes HTTP en sortie et à les acheminer vers le serveur WebSEAL de destination. Toujours de manière transparente, le client NetSEAT associe les URL logiques à des serveurs WebSEAL physiques en permettant la délocalisation ou la reproduction des ressources Web, sans incidence pour l'utilisateur final.

Remarque : L'installation de NetSEAT n'est pas indispensable pour l'utilisation de Policy Director. Par exemple, les utilisateurs de clients peuvent utiliser un navigateur compatible SSL pour communiquer directement avec WebSEAL.

API d'autorisation

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. L'API d'autorisation de Policy Director offre un accès direct à son service d'autorisation. Cette possibilité signifie que le développeur n'a désormais plus besoin de créer un code d'autorisation pour chaque application.

L'API d'autorisation de Policy Director réduit le temps nécessaire au développement des applications et le coût associé. Dans la mesure où elle permet une gestion centralisée de toute la sécurité du réseau, le coût total et le danger pour la sécurité des applications s'en trouvent diminués.

Serveur d'autorisations

Dans le mode autorisation à distance par utilisation de la mémoire cache, les applications utilisent les appels de fonction de l'API d'autorisation de Policy Director pour communiquer avec le serveur d'autorisations (ivacld). Ce serveur d'autorisations administre une instance de la base de données des règles d'autorisation et évalue les décisions d'autorisation.

L'API d'autorisation de Policy Director transmet chaque requête d'autorisation au serveur d'autorisations. A son tour, le serveur d'autorisations renvoie une recommandation basée sur les règles de sécurité. Le serveur peut également enregistrer un rapport d'audit contenant le détail de la requête d'autorisation.

Répartiteur des services de répertoire

Pendant son installation, Policy Director installe et configure automatiquement le répartiteur des services de répertoire (RSR). Le programme RSR est fourni avec Policy Director comme composant du module Serveur de gestion (IVMgr). L'utilisation du RSR ne nécessite aucune procédure particulière.

Si les clients NetSEAT sont utilisés comme module de support pour les serveurs Policy Director ou la console de gestion, ils utiliseront le répartiteur des services de répertoire. S'ils utilisent exclusivement la transmission par tunnel SSL, ils n'utiliseront pas le RSR.

Le RSR fonctionne comme un serveur de services de répertoire (annuaire) de cellules semi-tiers. Le client NetSEAT dirige les requêtes d'emplacement de ressource et de services vers le RSR. A son tour, le répartiteur des services de répertoire contacte les services de répertoire de cellules (SRC) du domaine sécurisé afin qu'ils répondent à la requête. Ensuite, le RSR renvoie la réponse de la requête au système d'où le client NetSEAT l'avait émise.

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

Le Service d'acquisition de droits d'accès (SAD) de Policy Director est un composant proposé en option. Pendant son installation, Policy Director installe et configure automatiquement le service d'acquisition de droits d'accès.

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 clients SSL autres que ceux de Policy Director, consignés dans un registre externe, peuvent avoir des noms d'utilisateur associés à des identités Policy Director par le biais du SAD de Policy Director. Vous pouvez également créer votre propre service d'acquisition de droits d'accès. 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.

Vous aussi 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 et 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 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.

Principe du modèle de sécurité

Dans le contexte de Policy Director, la sécurité signifie l'accès contrôlé aux informations. Le programme de Policy Director applique les règles de sécurité d'une organisation aux objets de l'espace des noms protégé.

L'accès aux ressources peut être basé sur des règles propres à votre entreprise quelque soit la topologie du réseau. Les utilisateurs peuvent y accéder ou non selon leur identité et leur fonction, et non pas en fonction de leur situation géographique.

Les composants de Policy Director sont des applications reposant sur des programmes clients et serveurs. L'utilisation d'une méthode d'authentification réciproque et l'attribution de droits d'accès permet de rendre accessibles au plus grand nombre des ressources spécifiques. De même, vous pouvez protéger des ressources internes sensibles par un accès plus sécurisé et plus limité. Vos données sont en sécurité, que l'utilisateur autorisé y accède à partir du domaine sécurisé ou par le biais d'une connexion Internet à distance.

Définition de règles de sécurité

Le logiciel de sécurité Policy Director permet de créer un domaine sécurisé au sein duquel toutes les communications sont protégées contre les accès non autorisés et les altérations non détectées.

L'administrateur d'un domaine sécurisé doit déterminer :

- qui peut accéder au domaine sécurisé et aux objets de l'espace des noms d'objet protégé ;
- les objets à protéger ;
- les règles devant protéger ces objets.

Pour traiter une requête client, Policy Director :

- contrôle l'identité du client par l'authentification ;
- acquiert des droits d'accès ;
- délivre ou non l'autorisation selon les droits d'accès obtenus.

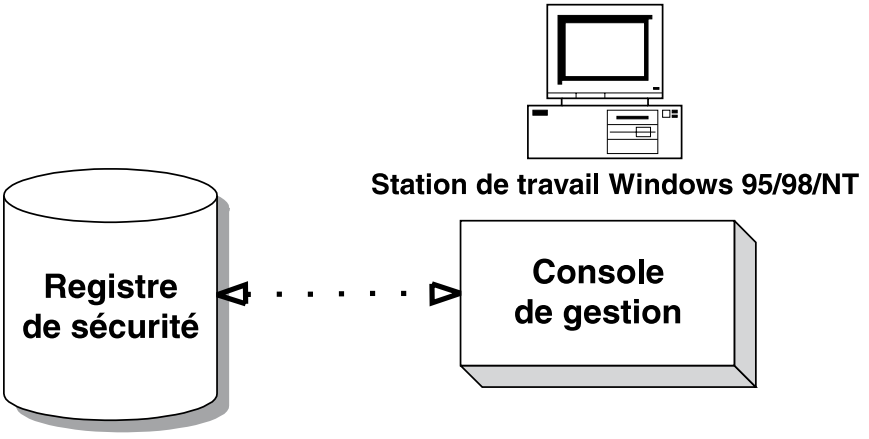
Qui peut accéder au domaine sécurisé ?

L'administrateur gère une liste officielle des utilisateurs (appelés les principaux dans l'environnement DCE) et des groupes membres du domaine sécurisé de Policy Director. Les utilisateurs et les groupes répertoriés dans cette liste peuvent accéder aux ressources du domaine. La base de données du registre (LDAP ou DCE) contient ces données d'utilisateurs et de groupes.

Vous pouvez autoriser un utilisateur à être membre du domaine sécurisé dès la création de son compte.

Tâche d'administration :

- Créez les comptes des utilisateurs et des groupes à l'aide de la console de gestion ou de la commande **ivadmin**.



Quels objets devez-vous protéger et par quelles règles ?

Policy Director peut protéger les types de ressource suivants :

- Les objets Web tels que les fichiers HTML, les programmes CGI et les liens HTML dynamiques ;
- Les services de réseau protégés par NetSEAL, comme TELNET, POP3 et les applications personnelles ;
- Les fonctions de gestion.

Policy Director représente les ressources sous la forme d'objets dans l'espace des noms d'objet protégé. Les autorisations d'accès sont associées à ces objets par le biais de modèles de règle. Policy Director utilise un type de modèle de règle appelé une liste de contrôle d'accès (LCA). Une LCA définit :

- qui peut accéder à l'objet ;
- quelles opérations peuvent être réalisées sur l'objet.

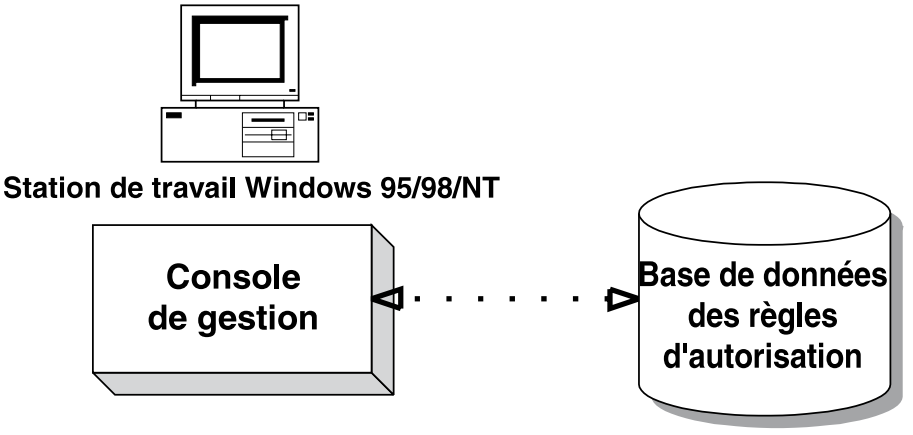
Par exemple, vous pouvez accorder le droit d'affichage de l'objet à tous les groupes mais n'en autoriser qu'un seul à le modifier.

Policy Director emploie un mécanisme qui permet de définir des autorisations globales, appelé modèle de LCA par analyse (ou héritage). Le modèle dit de liste de contrôle d'accès par analyse signifie que la LCA n'est pas attachée directement à chaque objet de la hiérarchie. Ces objets héritent de la LCA appliquée à la racine de celle-ci. Si un objet de la hiérarchie n'est attaché à aucune LCA, la liste de contrôle d'accès qui s'y applique est la première définie plus haut dans cette hiérarchie. Une LCA doit obligatoirement être appliquée à l'objet racine (/) pour que chaque objet de la hiérarchie en hérite.

Lorsque vous utilisez ce mécanisme, vous n'avez pas besoin de définir des autorisations pour chaque fichier ou répertoire.

Tâche d'administration :

- Définissez les règles de sécurité de l'espace des noms par le biais de la console de gestion et appliquez des modèles de règle (LCA) aux objets nécessitant une protection.

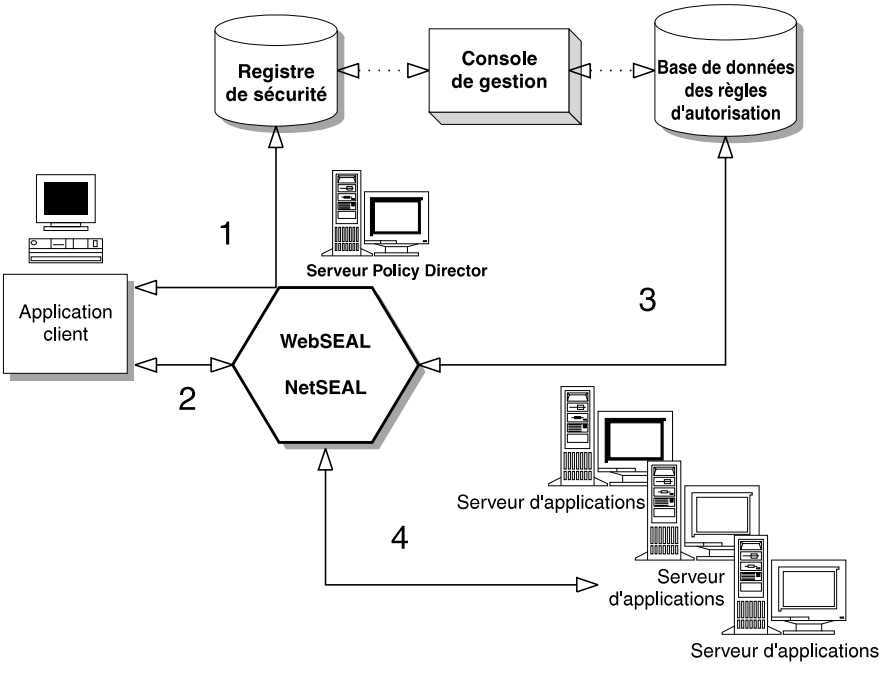


Application de règles de sécurité à une requête client

Lorsqu'un utilisateur demande à accéder à une application ou à un objet protégé, Policy Director exécute les procédures d'authentification et d'autorisation appropriées avant d'accepter la requête.

1. Le serveur de sécurité authentifie l'utilisateur pour prouver son identité. Policy Director gère l'authentification par le biais de méthodes utilisant des clés secrètes et privées.

   Sur la base de cette identité authentifiée, le serveur de sécurité délivre les droits d'accès à l'utilisateur. Les droits d'accès définissent les groupes et les organisations auxquels l'utilisateur appartient ainsi que les fonctions qu'il peut exercer.



2. Un tunnel de communication sécurisé est établi entre le client et le serveur Policy Director.

3. Un contrôle d'autorisation est réalisé à l'aide d'une instance de la base de données centralisée des règles d'autorisation. Policy Director applique les listes de contrôle d'accès sur la base des droits d'accès de l'utilisateur.
4. Si les paramètres d'autorisation correspondent aux droits d'accès de l'utilisateur, Policy Director transmet la requête au serveur d'applications pour faire aboutir la transaction.

Chapitre 2. Authentification et acquisition de droits d'accès

L'authentification est un processus qui consiste à identifier une personne qui tente de se connecter à un domaine sécurisé. La finalité de l'authentification est de prouver l'identité d'un client et d'obtenir les droits d'accès qui lui correspondent. Les droits d'accès peuvent être utilisés par Policy Director pour l'autorisation, l'audit et d'autres services.

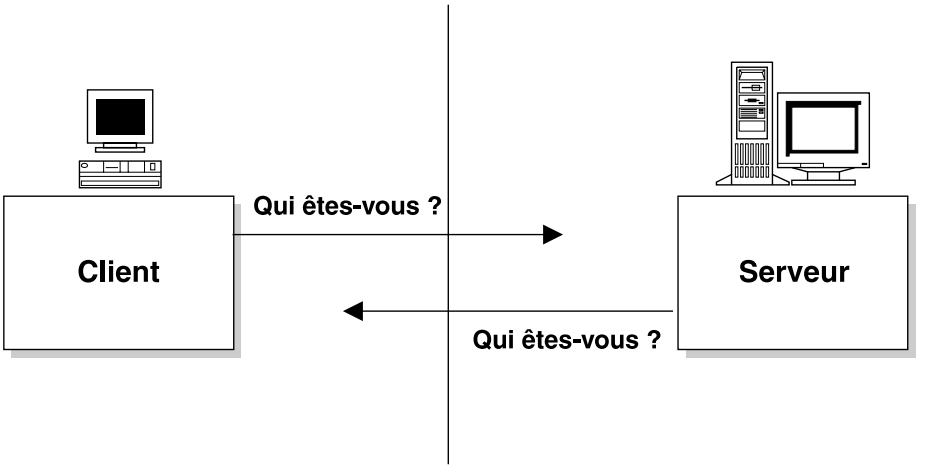
Ce chapitre comprend les sections suivantes :

Principes de base de l'authentification

Lorsque des serveurs assurent la sécurité dans un domaine sécurisé, chaque client doit fournir la preuve de son identité. Lorsque l'accès aux différentes ressources d'un domaine sécurisé est contrôlé par un serveur, les demandes d'authentification et d'autorisation qu'il émet peuvent assurer la sécurité globale du réseau.

L'authentification est un processus qui consiste à identifier une personne qui tente de se connecter à un domaine sécurisé.

Dans les systèmes de sécurité, l'authentification et l'autorisation sont deux choses distinctes. L'autorisation détermine si un utilisateur authentifié a le droit d'exécuter une opération sur une ressource donnée. L'authentification, pour sa part, atteste que cet utilisateur est bien celui qu'il prétend être, mais n'intervient pas quant à sa capacité à exécuter des opérations sur une ressource.



Policy Director propose une approche souple de l'authentification, qui permet d'adapter les règles de sécurité aux besoins de l'entreprise plutôt qu'à la topologie du réseau physique.

Policy Director authentifie l'identité des utilisateurs lorsqu'ils se connectent au domaine sécurisé pour accéder aux informations protégées. Les utilisateurs peuvent exercer un certain nombre de fonctions définies, chacune étant associée à des droits d'accès spécifiques.

Finalité de l'authentification

Le processus d'authentification remplit deux objectifs :

1. Déterminer l'identité du client ;
2. Acquérir les droits d'accès pour ce client.

La procédure d'authentification et la procédure d'acquisition de droits d'accès sont deux processus parfaitement distincts. Policy Director gère un certain nombre de systèmes d'authentification (reportez-vous à la section «Méthodes d'authentification prises en charge»).

Policy Director propose également des services par défaut et adaptables pour l'acquisition des droits d'accès. Un service d'acquisition de droits d'accès convertit les données d'identité produites par le système en droit d'accès au format Policy Director. Les droits d'accès Policy Director utilisent le format EPAC (Extended Privilege Attribute Certificate).

Les droits d'accès sont utilisés par tous les services de Policy Director demandant des informations sur le client. Ils peuvent être utilisés par Policy Director pour plusieurs types de service tels que l'autorisation, l'audit ou la délégation d'autorité.

Méthodes d'authentification prises en charge

Policy Director prend en charge les méthodes d'authentification reposant sur les clés secrètes ou les couples de clés publique/privée :

Clé secrète :

- Kerberos Version 5
- protocole LDAP (Lightweight directory access protocol)

Clé publique/privée :

- Connexion SSL par certificat X.509 de côté client (Policy Director peut utiliser les produits PKI/PKIX tels que IBM SecureWay Trust Authority version 3.1 ou les produits PKI/Entrust tels que IBM Vault Registry version 2.2.2).

  Nécessite un service d'acquisition de droits d'accès.

Types d'authentification

Policy Director prend en charge les types d'authentification suivants :

- Authentification par SSL (pour l'authentification Internet et intranet) ;
- Authentification par nom d'utilisateur et mot de passe (authentification basée sur l'identité de l'utilisateur) ;
- Authentification par clé Kerberos (authentification sur réseau).

Authentification SSL

Le protocole SSL (secure socket layer ou couche de sockets sécurisées) permet l'authentification, la sécurité et la confidentialité des données sur l'Internet. SSL utilise :

- la cryptographie par paire de clés publique/privée pour l'authentification ;
- une clé secrète pour coder les données pendant la connexion SSL.

En tant que mécanisme d'authentification, le protocole SSL prend en charge l'authentification du serveur uniquement et l'authentification réciproque.

Policy Director prend en charge le protocole SSL version 2 et 3.

Caractéristiques du protocole

Le protocole SSL, qui complète le protocole TCP/IP, est indépendant des applications. Il permet l'utilisation simultanée des protocoles d'application tels que HTTP, FTP et TELNET, par couche transparente. Le protocole de communication Web HTTP qui opère avec un canal codé SSL est appelé HTTPS.

Le protocole SSL peut négocier les clés de chiffrement et authentifier le serveur avant que les données ne soient échangées par l'application de communication du niveau supérieur. Il assure la sécurité et l'intégrité du canal de transmission par le biais du chiffrement, de l'authentification et de codes d'authentification des messages.

Tiers sécurisé et autorité de certification

L'authentification par protocole SSL repose sur la confiance accordée à un tiers, lequel garantit la fiabilité de l'une ou des deux parties ayant pouvoir d'authentification. Ce tiers est appelé l'autorité de certification (AC).

L'autorité de certification a pour mission de délivrer des certificats numériques (identités électroniques) pour identifier des personnes, des groupes ou des systèmes utilisant le réseau, et prouver à tous que l'utilisateur est sécurisé par elle.

La signature numérique attribuée aux certificats par l'autorité de certification lie l'identité du propriétaire de chaque certificat à la clé publique qu'il contient. Dès lors que l'on se fie à l'autorité de certification, l'utilisateur ainsi certifié est réputé sécurisé.

Les utilisateurs du réseau peuvent obtenir le certificat de la clé publique de l'autorité de certification et l'utiliser pour vérifier les certificats des autres utilisateurs. Cette vérification faite, ils ont l'assurance que les clés publiques contenues dans ces certificats sont bien celles des propriétaires désignés et que l'autorité de certification (qu'ils reconnaissent par le certificat de racine) garantit cette liaison.

Ayant échangé leurs certificats de clé publique, les deux parties authentifiées peuvent alors coder et signer numériquement les données de la session. Le chiffrement et la signature numérique suppriment le risque de voir d'autres utilisateurs intercepter la communication ou manipuler les données.

Une autorité de certification peut être une société spécialisée dans la vente de certificats sur l'Internet ou un service de l'entreprise spécialement chargé de délivrer des certificats dans le cadre d'un intranet privé. Vous devez décider quelle autorité de certification aura votre confiance et devra vérifier les identités des autres utilisateurs.

La solution IBM SecureWay FirstSecure (FirstSecure) comprend notamment le produit de sécurité IBM SecureWay Trust Authority (Trust Authority). Ce produit permet de délivrer ses propres certificats dans le cadre d'un intranet d'entreprise. Pour plus d'informations sur le produit FirstSecure et ses composants, contactez le site Web :

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

Certificats numériques X.509

L'authentification par SSL implique l'utilisation de certificats numériques. Le certificat est en réalité un fichier qui contient des données d'identification. Il s'achète ou s'obtient gratuitement auprès d'une autorité de certification (AC) sécurisée. Le rôle principal de l'autorité de certification consiste à certifier l'authenticité des utilisateurs.

Les certificats sont des fichiers qui ne peuvent être ni transmis ni reproduits et constituent une sorte de carte d'identité ou de passeport. Ils permettent de s'assurer que les utilisateurs sont bien ceux qu'ils prétendent être. Le fichier est signé avec la clé privée de l'autorité de certification pour garantir son authenticité et son intégrité.

Un navigateur compatible SSL utilise le type de certificat standard X.509. La version 3 du certificat X.509 contient les informations suivantes :

- Version
- Numéro de série
- ID de l'algorithme de signature
- Nom de l'émetteur
- Délai de validité
- Nom du sujet (l'utilisateur)
- Données de la clé publique du sujet
- Identifiant unique de l'émetteur (DN de l'autorité de certification à l'origine du certificat)
- Identifiant unique du sujet (DN de la personne identifiée par le certificat)
- Extensions (version 3 uniquement)
- Signatures pour tous les champs ci-dessus

La norme de certificat X.509 version 3 permet de définir d'autres données d'identification telles que le nom de l'entreprise du détenteur du certificat et son ancienneté. Le certificat est signé par son émetteur pour authentifier le lien entre le nom du sujet (l'utilisateur) et sa clé publique.

Les certificats ne prouvent pas de manière irréfutable que les utilisateurs ou les systèmes sont ceux qu'ils prétendent être mais attestent qu'une autorité de certification les considère comme authentiques. Si vous vous fiez à l'autorité de certification ayant délivré le certificat, vous pouvez échanger des informations avec son détenteur dans une relative confiance.

Principes de base de la méthode d'authentification SSL

Le processus d'échange de protocoles SSL consiste à échanger des signaux pour établir des communications. Ce processus se divise en deux phases :

- «Authentification du serveur par certificat de côté serveur» à la page 21
- «Authentification du client par certificat de côté client» à la page 21 (optionnel)

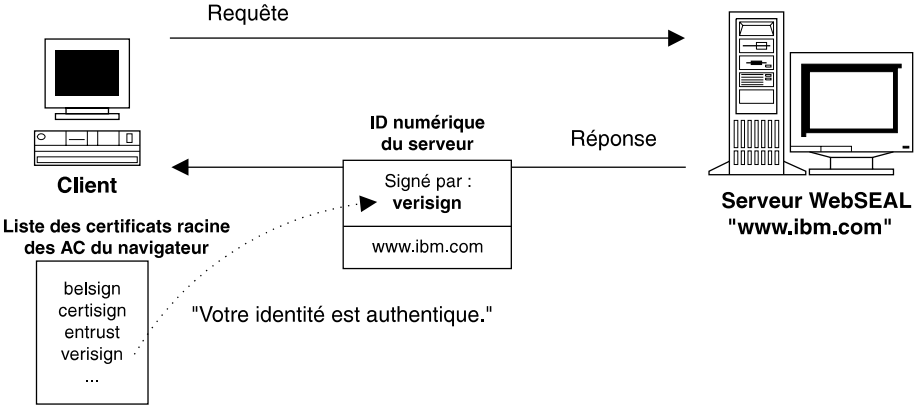
Les clients comme les serveurs peuvent détenir des certificats. Le serveur doit toujours posséder un certificat pour l'authentification par SSL. Les clients peuvent accéder au domaine sécurisé via SSL, avec ou sans certificat de côté client.

Lorsqu'un serveur envoie son certificat à un client, on appelle ce processus l'authentification du serveur. Lorsqu'un client envoie son certificat à un serveur, on appelle ce processus l'authentification du client. La combinaison de l'authentification du client et du serveur est appelée l'authentification réciproque.

Authentification du serveur par certificat de côté serveur

L'authentification du serveur est nécessaire pour établir une connexion SSL. Cette authentification s'effectue de la manière suivante :

1. Un client demande une connexion à un serveur SSL.
2. En réponse, le serveur signe (mais ne code pas) son certificat. Le serveur transmet ensuite le certificat qui contient sa clé publique au client.
3. Le client utilise la clé publique de serveur contenue dans le fichier du certificat pour vérifier que le propriétaire du certificat et son signataire ne font qu'un.
4. Pour vérifier s'il peut accepter l'émetteur du certificat, le client le recherche dans la base de données des certificats de racine des autorités de certification du navigateur. S'il reconnaît et accepte cet émetteur, le client passe à l'étape suivante. Dans le cas contraire, le navigateur informe l'utilisateur que le certificat a été délivré par une autorité de certification inconnue. Il revient donc à l'utilisateur d'accepter ou de rejeter le certificat.
5. Le client génère ensuite une clé primaire, la code avec la clé publique du serveur et transmet cette clé primaire codée au serveur.
6. Le serveur décode la clé primaire et s'authentifie auprès du client en lui renvoyant un message codé avec cette même clé primaire. Les données suivantes sont codées à l'aide de clés issues de cette clé primaire.



Authentification du client par certificat de côté client

Le serveur débloque le certificat numérique d'un client avec la clé publique de celui-ci. Les certificats de clé publique d'un client observent la même syntaxe que les certificats X.509.

L'authentification par certificats de côté client et SSL s'effectue de la manière suivante :

1. Une fois le serveur authentifié, celui-ci envoie au client une question d'authentification.
2. Le client renvoie sa signature numérique avec sa réponse ainsi que son certificat de clé publique. La signature numérique est calculée sur la base de la clé privée du client.
3. Le serveur utilise la clé publique de client contenue dans le fichier du certificat pour vérifier que le propriétaire du certificat et son signataire ne font qu'un.

4. Le serveur tente de rapprocher le certificat d'une autorité de certification sécurisée. Si l'autorité de certification du client n'est pas répertoriée comme étant sécurisée, certains serveurs mettront fin à la transaction, consigneront une erreur et enverront un message dans ce sens au client. D'autres pourront décider de continuer sans action de ce type.
5. Si l'autorité de certification du client s'avère sécurisée, le serveur exécute la transaction.

Les certificats de côté client ne sont pas indispensables à l'authentification pour une connexion SSL et vous pouvez quand même échanger des informations codées dans cette situation. Les certificats de côté client donnent une assurance supplémentaire que client et serveur envoient des données codées aux bons destinataires. L'authentification réciproque n'est possible qu'avec les certificats de côté client.

Dans les deux situations, lorsque le serveur SAD a été configuré pour demander un certificat de client pour le contrôle d'accès, les clients sont refoulés s'ils n'en produisent pas un valide.

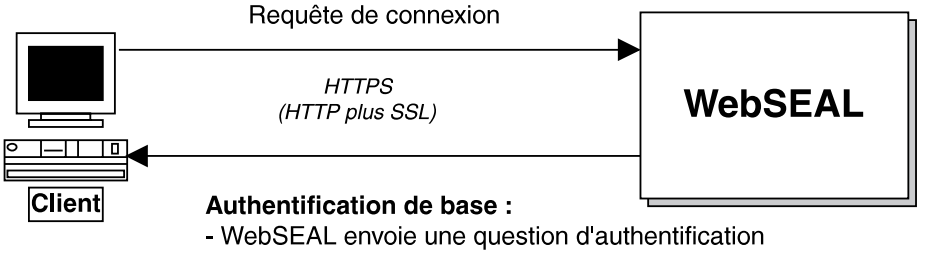
Pour plus d'informations sur les certificats de côté client X.509 utilisés par les clés privées et publiques, reportez-vous à la section «Méthode d'authentification par certificat X.509» à la page 173.

Authentification par nom d'utilisateur et mot de passe

Le processus d'authentification demande au client de fournir des données d'identité au cours de la procédure de connexion. Policy Director WebSEAL prend en charge l'authentification par nom d'utilisateur et mot de passe.

Deux méthodes d'authentification par nom d'utilisateur et mot de passe permettent d'obtenir des données d'identité :

- L'authentification de base
- La connexion avec formulaires



Reportez-vous à la section «Méthodes d'authentification par nom d'utilisateur et mot de passe» à la page 168 pour plus d'informations sur les méthodes d'authentification demandant un nom d'utilisateur et un mot de passe.

Authentification Kerberos

Kerberos version 5 est un protocole d'authentification de réseau qui permet à deux parties de s'authentifier réciproquement afin de pouvoir échanger des informations de manière sécurisée dans le cadre d'un réseau ouvert.

Policy Director peut utiliser l'authentification Kerberos dans le cadre des échanges suivants :

- Console de gestion vers Serveur de gestion
- Console de gestion vers Serveur de sécurité
- Serveur d'autorisations vers Serveur de gestion
- WebSEAL vers Serveur de gestion
- WebSEAL vers le registre DCE (pour l'authentification des clients)

Les serveurs Policy Director communiquent avec les autres serveurs du domaine sécurisé Policy Director à l'aide du protocole Kerberos et du module de support de réseau Client NetSEAT. NetSEAT communique avec le service de sécurité de Policy Director et configure le tunnel SSL sécurisé au cours de la transmission des données.

L'authentification par protocole Kerberos repose sur la confiance accordée à un tiers, lequel garantit la fiabilité des deux parties ayant pouvoir d'authentification. Ce service de gestion de la sécurité est assuré par un tiers sécurisé appelé le serveur de sécurité.

Le serveur de sécurité (secd) de Policy Director est un serveur physiquement sécurisé qui conserve des données en relation avec la sécurité (par exemple, des noms d'utilisateur, de groupe et des mots de passe) dans une base de données appelée le registre.

Le protocole Kerberos utilise un mécanisme de clé secrète (LDAP Secret Key), partagé et fonctionnant par session, pour gérer l'authentification réciproque entre les serveurs. Kerberos repose sur le serveur de sécurité sécurisé pour la répartition des clés. L'échange de données fait appel à la méthode d'appel de processus à distance RPC (Remote Procedure Call).

Le protocole d'authentification Kerberos met en oeuvre une procédure complexe à base d'échanges de messages. Cette série d'échanges de messages contient des clés secrètes et d'autres informations nécessaires à l'identification réciproque des parties. L'objectif de Kerberos est d'empêcher tous les participants de connaître les clés des autres. A cet égard, la durée de vie de nombreuses clés se limite à un simple échange de messages.

Acquisition des droits d'accès

L'un des principaux objectifs du processus d'authentification est d'acquérir des données de droit d'accès décrivant la nature de l'utilisateur du programme client. Policy Director distingue l'authentification de l'utilisateur de l'acquisition des droits d'accès.

L'identité d'un utilisateur ne change jamais. En revanche, les droits d'accès qui caractérisent les groupes ou les fonctions auxquels elle se rattache sont variables. Les droits d'accès liés à un contexte donné changent avec le temps. Par exemple, lorsqu'une personne change de poste, ses droits d'accès doivent refléter son

nouveau niveau de responsabilité. Les droits d'accès d'une personne à son travail ne sont pas ceux dont il jouit vis-à-vis de sa banque.

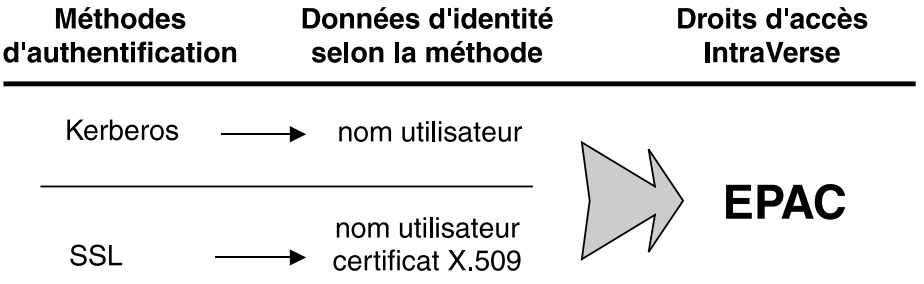
Le processus d'authentification de l'utilisateur produit des données d'identité qui varient selon le contexte et la méthode utilisée. Ces information doivent ensuite être transformées ou reliées (mappées) à une représentation standard selon un format reconnaissable à l'échelle du domaine. Policy Director utilise le format EPAC.

Données d'identité selon la méthode

Pour un même service d'acquisition de droits d'accès, différentes méthodes d'authentification produisent des données d'identité utilisateur différentes.

- Le protocole Kerberos repose sur l'authentification d'un nom d'utilisateur et d'un mot de passe.
- Les certificats numériques côté client X.509 fournissent les données contenues dans leurs champs.
- L'authentification de base et les méthodes de connexion à base de formulaires (SSL) reposent sur l'authentification d'un nom d'utilisateur et d'un mot de passe.

L'illustration suivante montre le type de données d'identification produites selon la méthode d'authentification utilisée et l'utilisation du service d'acquisition de droits d'accès par SSL pour convertir ces données au format EPAC.



Les données d'identité (par exemple et selon la méthode utilisée, les mots de passe, les paires de clés et les certificats) représentent les propriétés de l'identité physique de l'utilisateur. Ces informations servent à établir la session sécurisée avec le serveur.

Le droit d'accès obtenu, qui caractérise la fonction de l'utilisateur dans le domaine sécurisé, décrit cet utilisateur dans un contexte spécifique et n'est valable que sur la durée de vie de la session.

Certificat EPAC

Les droits d'accès sont utilisés par tous les services de Policy Director demandant des informations sur le client. Par exemple, le service d'autorisation Policy Director utilise les droits d'accès pour déterminer si un utilisateur est autorisé à exécuter certaines opérations sur une ressource protégée du domaine sécurisé.

Pour travailler avec les listes de contrôle d'accès, Policy Director peut utiliser les données EPAC qui contiennent des UUID (Universal Unique Identifier). Policy Director utilise les droits d'accès pour d'autres services, notamment :

- le service d'audit ;
- les fonctions de délégation dans les jonctions WebSEAL et NetSEAL.

Policy Director demande les données EPAC suivantes :

Attribut	Description
ID de domaine sécurisé	ID du domaine sécurisé d'origine de l'utilisateur
UUID de principal	UUID de l'utilisateur (ou "principal" si DCE)
UUID de groupe	UUID du ou des groupes auquel l'utilisateur appartient

Les données d'authentification produites par la méthode utilisée doivent être converties en données EPAC :

- Les clients Policy Director sont automatiquement associés aux droits d'accès par WebSEAL.
- Les clients SSL autres que ceux de Policy Director, consignés dans un registre externe, peuvent avoir des noms d'utilisateur associés à des identités Policy Director par le biais d'un service d'acquisition de droits d'accès externe.
- Les données des certificats X.509 de côté client utilisés par les clients pour accéder au serveur peuvent être associées à des identités Policy Director par le biais d'un service d'acquisition de droits d'accès externe.

Chaînes de sécurisation

Au cours de l'échange de protocoles SSL entre le serveur WebSEAL et le client de navigation, le premier communique au deuxième une liste de certificats émis par les autorités de certification reconnues par le serveur. Ensuite, le navigateur affiche une liste de certificats de client de navigation qui sont :

- signés par l'une de ces autorités de certification, ou
- sécurisés en vertu d'une relation de chaîne de sécurisation avec l'une des autorités de certification reconnues par le serveur (le certificat est signé par une autorité de certification elle même certifiée par une autorité de certification reconnue par le serveur).

Ce processus est appelé le chaînage des certificats.

L'utilisateur sélectionne l'un des certificats de client pour transmission au serveur. Si,le certificat de client est signé par l'une des autorités de certification reconnues par le serveur, le navigateur ne lui transmet que ce certificat (ce qui suppose que le serveur détient déjà le certificat de l'autorité de certification l'ayant signé).

Si le certificat de client n'est pas signé par l'une des autorités de certification reconnues par le serveur, le navigateur crée et lui transmet une chaîne de certificats d'AC qui atteste de l'existence d'une chaîne de sécurisation entre le certificat de client et l'une de ces autorités.

Ici encore, le navigateur ne transmet pas le certificat de l'autorité de certification reconnue par le serveur mais part du principe que ce dernier le détient déjà.

Le fichier de configuration de Policy Director secmgrd.conf contient une liste de certificats d'autorités de certification racines reconnues. Il est donc normal que Policy Director accepte les certificats émis par ces autorités de certification.

Le serveur réceptionne chaque certificat d'AC transmis par le navigateur et vérifie si :

- il s'agit bien d'un certificat d'une autorité de certification ;
- la signature qu'il comporte est exacte ;
- le certificat n'est pas arrivé à expiration.

Une chaîne de sécurisation peut s'établir dès lors qu'une première autorité de certification en reconnaît une deuxième, qui en reconnaît une troisième, et ainsi de suite. Si Policy Director reconnaît l'une des autorités de certification appartenant à la chaîne de sécurisation, il peut accepter le certificat du client.

Présentation générale du service d'acquisition de droits d'accès (SAD)

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.

Les droits d'accès issus du processus d'authentification sont utilisés par tous les services de Policy Director demandant des informations sur le client. Il s'agit notamment des services d'autorisation et d'audit. Les principales fonctions de Policy Director dépendent de l'existence de droits d'accès pour chaque client.

Policy Director utilise le format EPAC pour représenter les droits d'accès issus du processus d'authentification.

Policy Director génère automatiquement des droits d'accès pour les clients SSL qui :

- sont membres du domaine sécurisé ;
- s'authentifient avec un nom d'utilisateur et un mot de passe reconnus.

Dans cette situation, le nom d'utilisateur et le mot de passe que vous indiquez doivent correspondre à une entrée de compte du registre par défaut (LDAP).

Avec d'autres scénarios, l'accès par le client se fait selon un modèle différent :

- Le client ne figure pas dans le registre par défaut de Policy Director.
- L'accès client se fait au moyen d'un certificat côté client.

Dans toutes ces situations, Policy Director doit se fier à un service d'authentification et de mappage personnalisé capable de :

- réaliser l'authentification de ces clients ;
- se reporter à un registre de comptes externe (tiers) ;
- mapper des données d'identité externes à une identité Policy Director.

Ce service d'authentification et de mappage personnalisé est appelé un service d'acquisition de droits d'accès externe.

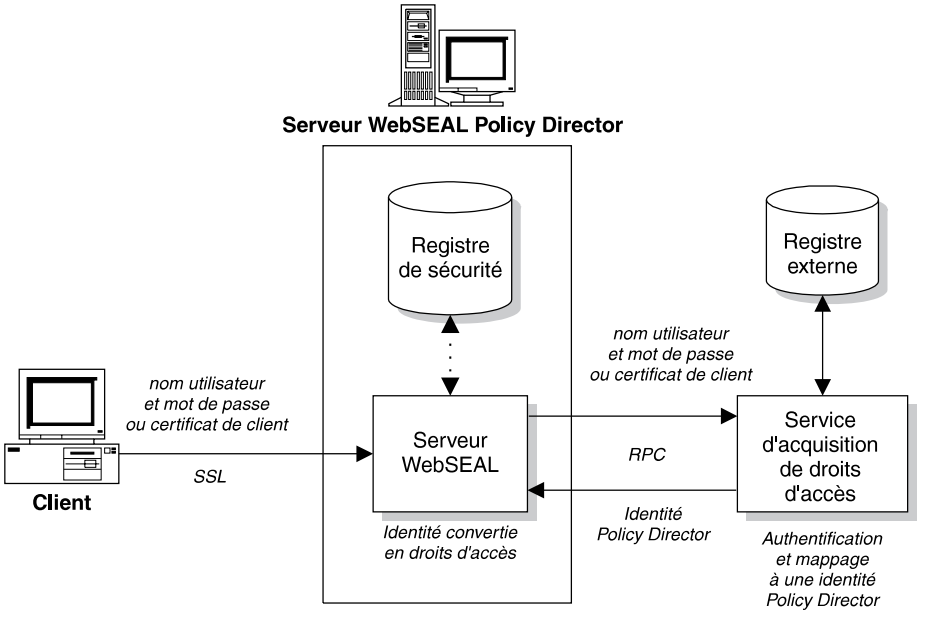
Présentation du service d'acquisition de droits d'accès

Un service d'acquisition de droits d'accès (SAD) permet de remplacer la méthode d'authentification SSL WebSEAL par défaut (basée sur un couple nom d'utilisateur/mot de passe) par un processus d'authentification externe personnalisé, utilisant un registre des utilisateurs (au lieu du registre de sécurité de Policy Director). Ce service d'acquisition de droits d'accès personnalisé peut également mapper des données d'identité (certificats, jetons) à une identité Policy Director.

Le service d'acquisition de droits d'accès doit être élaboré et personnalisé par l'administrateur en fonction des besoins particuliers du domaine sécurisé.

Le service d'acquisition de droits d'accès doit utiliser les appels de processus à distance pour sécuriser toutes les communications entre WebSEAL et le serveur SAD.

Un service d'acquisition de droits d'accès permet à un utilisateur n'ayant pas de compte défini dans le registre par défaut de Policy Director d'accéder au domaine sécurisé. Le service d'acquisition de droits d'accès peut authentifier cet utilisateur (par le biais d'un registre externe au besoin). Il communique ensuite une identité Policy Director au serveur WebSEAL qui la convertira en droits d'accès. Sur la base de ces droits d'accès, Policy Director autorisera ou non l'utilisateur à accéder au domaine sécurisé.



Un service d'acquisition de droits d'accès peut utiliser les bases de données des utilisateurs existants, qu'il serait difficile, voire impossible, de migrer vers le registre normalement utilisé par Policy Director. Par exemple, un système existant peut impliquer l'emploi d'un ID de client et d'un jeton ou PIN (numéro d'identification personnel). Cette méthode d'authentification contrôle les données de l'utilisateur par le biais de sa propre base de données de registre.

Un serveur SAD de démonstration est fourni avec le kit de développement d'applications (ADK) d'autorisation de Policy Director (IVAuthADK). Ce serveur assure l'interface (l'IDL) entre WebSEAL et le service d'acquisition de droits d'accès. L'ADK propose également des codes sources pour créer son propre service d'acquisition de droits d'accès.

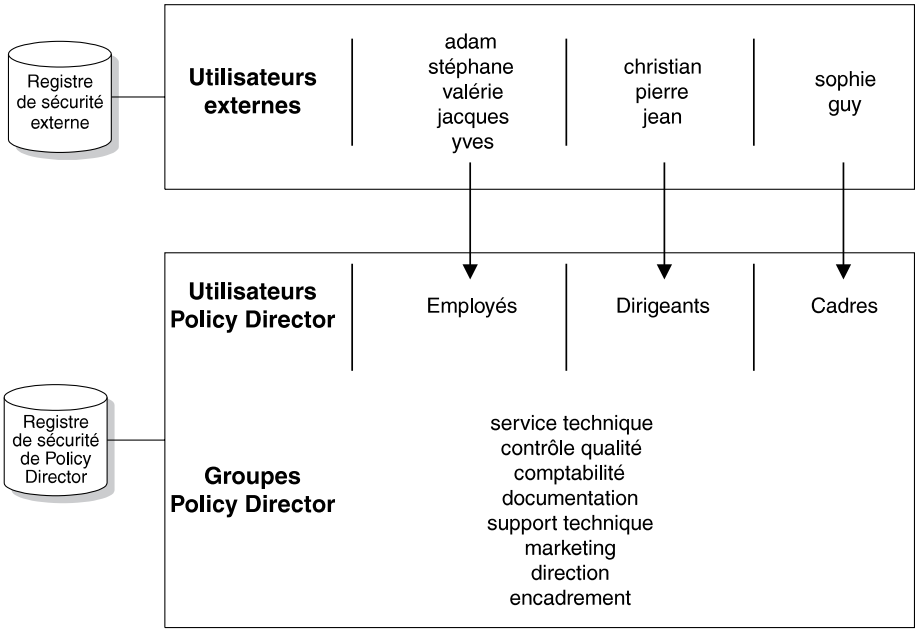
Mappage plusieurs à un

Un service d'acquisition de droits d'accès peut s'avérer adapté dans le cadre d'une solution de type plusieurs à un ; le module permet d'associer plusieurs comptes à un même utilisateur Policy Director.

Avec le mappage de type plusieurs à un, un utilisateur Policy Director peut prendre la place d'un groupe dont les membres sont l'ensemble des utilisateurs de la base de données existante. La solution de mappage plusieurs à un produit des droits d'accès une visibilité et un contrôle d'activité identiques pour tous les utilisateurs

rattachés à un même utilisateur. Tous les utilisateurs rattachés (mappés) à cet utilisateur ont exactement les mêmes autorisations. Cet aspect doit être pris en considération lorsque vous définissez vos règles de sécurité.

Dans l'illustration suivante, les utilisateurs définis dans un registre externe peuvent être mappés à un même utilisateur Policy Director. Par exemple, l'utilisateur Policy Director (`Employées`) se substitue à un ensemble d'utilisateurs définis dans le registre externe. Bien que les utilisateurs soient rattachés au même compte Policy Director, ils peuvent aussi se différencier en devenant membre d'un ou plusieurs groupes Policy Director. Les décisions d'autorisation de Policy Director peuvent reposer à la fois sur l'identité de l'utilisateur et sur son appartenance de groupe.



Remarque : Le niveau de contrôle d'activité dans le cadre d'un mappage plusieurs à un n'est pas très élevé. Les services d'audit ne surveillent que l'utilisateur Policy Director et pas les utilisateurs qui lui sont rattachés.

Modes de fonctionnement

Un service d'acquisition de droits d'accès peut être créé pour traiter des données d'authentification telles que des certificats de client, des noms d'utilisateur et des jetons. WebSEAL doit être configuré pour accepter les clients SSL hors registre et pour acheminer les données d'authentification vers le service d'acquisition de droits d'accès approprié pour l'authentification de ces données et leur mappage à une identité Policy Director.

Un service d'acquisition de droits d'accès opère l'authentification et le mappage des identités sur la base des données d'identité fournies par le client. Il en découle que vous pouvez concevoir le service d'acquisition de droits d'accès de manière à ce qu'il fonctionne dans l'un des modes suivants :

- «Mappage de certificat X.509» à la page 29
- «Mappage par nom d'utilisateur» à la page 30

Reportez-vous à la section «Service d'acquisition de droits d'accès personnalisé» à la page 33 pour plus d'informations sur l'utilisation d'un service d'acquisition de ce type.

Mappage de certificat X.509

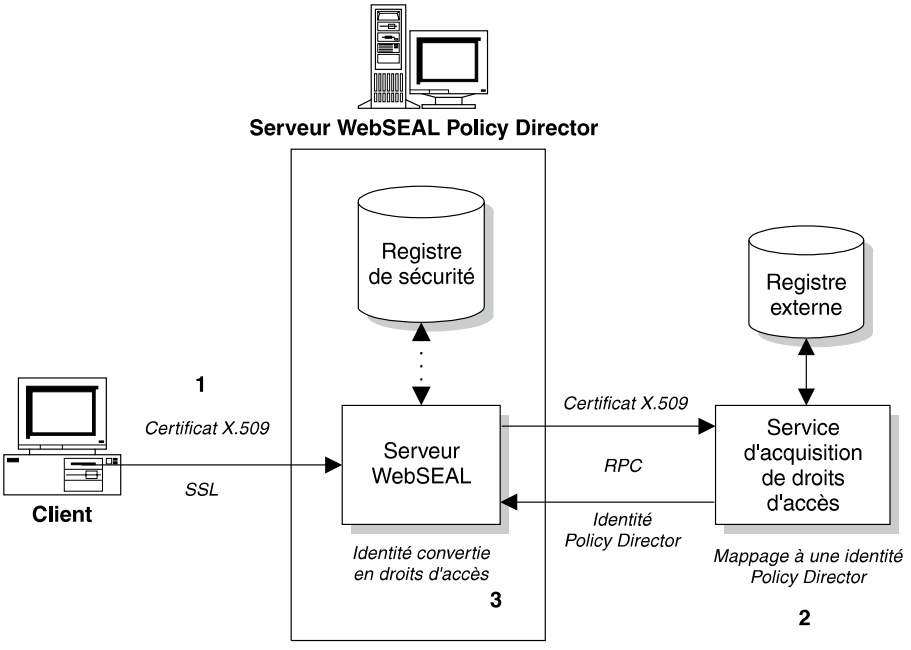
Policy Director peut prendre en charge l'authentification des clients utilisant les certificats numériques X.509 par SSL avec n'importe quel service d'acquisition de droits d'accès. Un service d'acquisition de droits d'accès gérant le mode certificat X.509 mappe les données contenues dans ce certificat à une identité Policy Director. Cette identité Policy Director est ensuite renvoyée à WebSEAL qui la convertit en droits d'accès.

Le mode X.509 est adapté aux conditions suivantes :

1. Les clients communiquent par SSL.
2. Les clients utilisent des certificats numériques X.509 pour l'authentification.
3. Les clients ont besoin d'accéder à des ressources protégées résidant dans le domaine sécurisé par Policy Director.

Un serveur SAD peut mapper les données d'un certificat à une identité Policy Director sur le mode un à un ou plusieurs à un. La finalité du service de mappage est de fournir au service d'autorisation de Policy Director les droits d'accès qui lui serviront à décider d'attribuer ou non des autorisations.

L'illustration suivante montre la succession des événements qui se produisent lorsque WebSEAL est configuré pour utiliser un service d'acquisition de droits d'accès pour le mappage des certificats X.509.



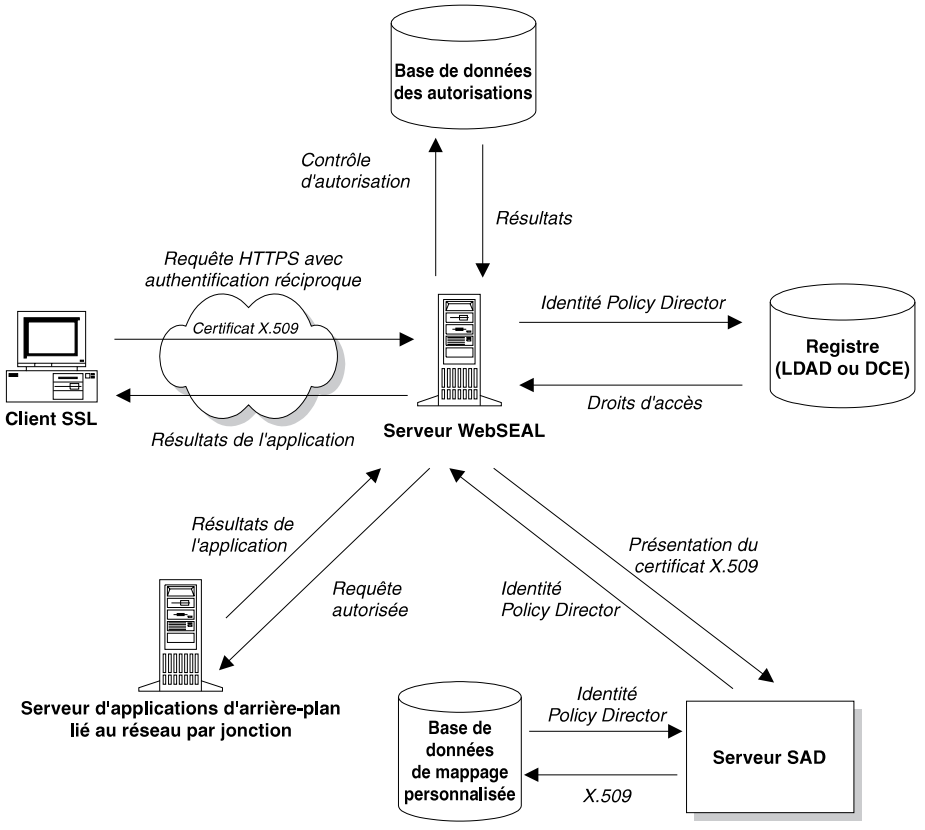
1. Le client accède au serveur WebSEAL par SSL avec un certificat X.509.

   Notez que l'authentification se fait à cette étape au moyen d'un échange de clés privées et publiques. Le service d'acquisition de droits d'accès n'a plus qu'à mapper les droits d'accès de l'utilisateur.
2. Le serveur SAD extrait les données d'identité (de l'application) à partir du certificat validé puis les rattache à une identité Policy Director reconnue. Le serveur SAD peut utiliser un registre externe (tiers) au besoin.
3. L'identité Policy Director est renvoyée à WebSEAL qui utilise alors son registre par défaut pour la convertir en droits d'accès.

Utilisation d'un service d'acquisition de droits d'accès en mode X.509

L'illustration suivante montre la succession d'événements qui se produisent lorsqu'un client, accédant à WebSEAL au moyen d'un certificat X.509, demande une ressource du domaine sécurisé.

1. Les données du certificat sont mappées à une identité Policy Director par le service d'acquisition de droits d'accès qui retourne cette identité à WebSEAL.
2. A partir de cette identité, WebSEAL crée un droit d'accès et décide d'attribuer une autorisation d'accès à une ressource protégée résidant sur un serveur d'applications lié au réseau par une jonction.



Mappage par nom d'utilisateur

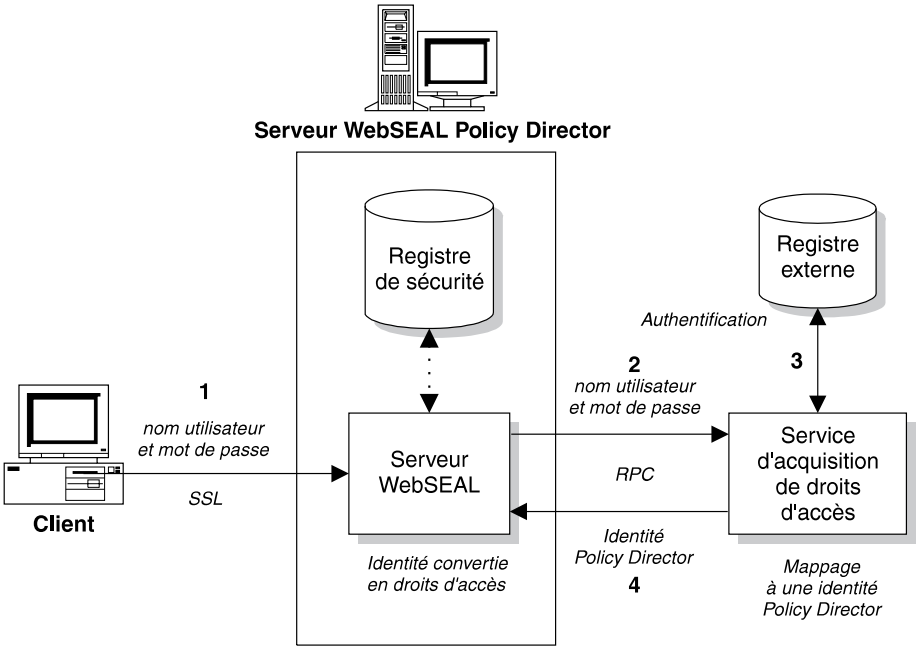
Le mappage des noms d'utilisateur est une autre forme de méthode d'authentification et de mappage des identités. Avec ce mode de mappage, vous pouvez remplacer le processus d'authentification par défaut par une procédure externe personnalisée utilisant un registre d'utilisateurs autre que le registre LDAP (le registre par défaut de Policy Director).

La méthode d'authentification standard de Policy Director, qui utilise SSL, demande à l'utilisateur de se connecter avec un nom d'utilisateur et un mot de passe. L'authentification et l'acquisition de droits d'accès pour cette identité sont déterminées à partir du registre Policy Director.

L'atout majeur d'un service d'acquisition de droits d'accès de ce type est de pouvoir utiliser les bases de données des utilisateurs existants, qu'il serait difficile, voire impossible, de migrer vers le registre Policy Director.

L'illustration suivante montre la succession des événements qui se produisent lorsque WebSEAL est configuré pour utiliser un service d'acquisition de droits d'accès pour le mappage des noms d'utilisateur.

1. Le client accède au serveur WebSEAL par SSL avec un nom d'utilisateur et un mot de passe.
2. WebSEAL est configuré pour communiquer les noms d'utilisateur et les mots de passe au service d'acquisition de droits d'accès pour l'authentification et l'acquisition des droits d'accès.



3. Le service d'acquisition de droits d'accès utilise un registre externe (tiers) pour authentifier l'utilisateur puis l'associe à une identité Policy Director.
4. L'identité Policy Director est renvoyée à WebSEAL qui utilise alors son registre par défaut pour la convertir en un droit d'accès.

Ce mode est plus adapté en tant que solution de mappage plusieurs à un ; plusieurs comptes sont mappés à un même utilisateur Policy Director. Reportez-vous à la section «Mappage plusieurs à un» à la page 27.

Choix du service d'authentification

Vous pouvez choisir l'un des types de service d'authentification suivants :

- Le service d'acquisition de droits d'accès par défaut de Policy Director (reportez-vous à la section «SAD de Policy Director») ;
- Un service d'acquisition de droits d'accès personnalisé (reportez-vous à la section «Service d'acquisition de droits d'accès personnalisé» à la page 33).

SAD de Policy Director

Policy Director comporte un service d'authentification des clients : le module Policy Director — Service d'acquisition de droits d'accès (SAD). Le SAD de Policy Director nécessite l'utilisation du registre des utilisateurs LDAP.

Pour utiliser le SAD de Policy Director pour l'authentification, vous devez configurer WebSEAL comme il convient et vérifier et mettre à jour les fichiers de configuration

iv.conf et secmgrd.conf (voir la section «Configuration du service d'acquisition de droits d'accès de Policy Director» à la page 174).

Le service d'acquisition de droits d'accès de Policy Director mappe les certificats numériques de client transmis par le navigateur SSL à une identité Policy Director. 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 Policy Director tente alors de mapper ce certificat à une identité d'utilisateur reconnue par Policy Director.

Le service d'acquisition de droits d'accès de Policy Director a été conçu de manière à prendre en charge les connexions SSL avec l'un ou l'autre de ces certificats côté client X.509 version 3 :

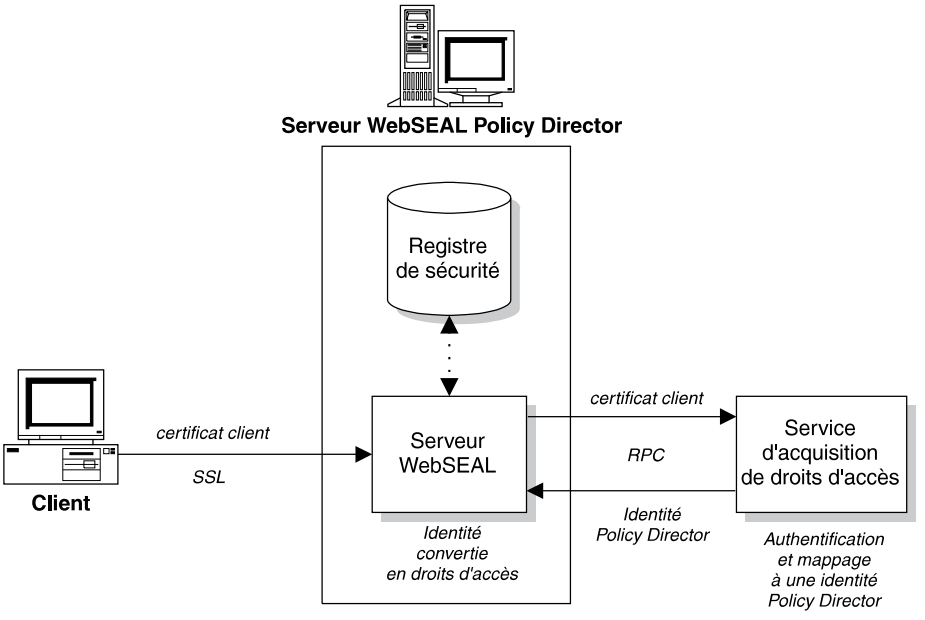
- Produit compatible PKIX (par exemple, IBM SecureWay Trust Authority version 3.1)
- Produit compatible Entrust (par exemple IBM Vault Registry version 2.2.2)

Tous les certificats sont transmis en chiffrement DER (Distinguished Encoding Rules).

Le système utilise une interface RPC entre le service d'acquisition de droits d'accès et WebSEAL. Le service d'acquisition de droits d'accès de Policy Director utilise les appels de processus à distance pour sécuriser toutes les communications entre WebSEAL et le serveur SAD. Dans la mesure où le service d'acquisition de droits d'accès est une application DCE-RPC, un client DCE est nécessaire pour réaliser le mappage des identités de client.

Le service d'acquisition de droits d'accès par défaut de Policy Director :

- permet d'utiliser des certificats de client ou de spécifier qu'ils sont optionnels ;
- n'effectue aucun contrôle de révocation des certificats associés ;
- permet le chaînage des certificats ;
- permet le mappage un à un.



Mappage un à un

Le service d'acquisition de droits d'accès de Policy Director utilise un mode de mappage appelé ″un à un″. Le mappage un à un de comptes existants à des utilisateurs individuels peut alourdir la gestion des comptes. Cependant, dans le fichier de configuration du SAD de Policy Director (cdas.conf), l'administrateur peut créer une table associant le DN d'un certificat à celui d'un utilisateur (LDAP) Policy Director.

Lorsque WebSEAL soumet un certificat au SAD de Policy Director, celui-ci extrait d'abord son DN puis recherche son occurrence dans la table. S'il en trouve une, le SAD Policy Director renvoie à WebSEAL le DN d'utilisateur Policy Director associé. WebSEAL utilise ensuite ce DN pour identifier l'utilisateur Policy Director (LDAP). En l'absence d'occurrence, le SAD renvoie à WebSEAL le DN issu du certificat. Dans cette situation, l'utilisateur Policy Director (LDAP) 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.

Tâches d'administration

Les tâches d'administration nécessaires à la configuration du SAD de Policy Director sont les suivantes :

1. Pour utiliser le SAD pour l'authentification, vous devez configurer WebSEAL comme il convient et vérifier et mettre à jour, si besoin, les fichiers de configuration iv.conf et secmgrd.conf (voir la section «Configuration du service d'acquisition de droits d'accès de Policy Director» à la page 174).
2. Actualisez comme il convient la section de la table de mappage des DN du fichier de configuration cdas.conf (voir la section «Mappage des DN» à la page 176).

Fonctionnement du service d'acquisition de droits d'accès

L'interface du module Policy Director - Service d'acquisition de droits d'accès permet la procédure suivante :

- WebSEAL soumet un certificat au SAD de Policy Director.
- Celui-ci extrait d'abord le DN du certificat puis recherche son occurrence dans la table de mappage des DN.
- S'il trouve une occurrence :
  - Le SAD Policy Director renvoie à WebSEAL le DN d'utilisateur Policy Director associé.
  - WebSEAL utilise ensuite ce DN pour identifier l'utilisateur Policy Director.
- Dans le cas contraire :
  - Le SAD renvoie à WebSEAL le DN issu du certificat.
  - 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.

Service d'acquisition de droits d'accès personnalisé

Du fait de la diversité des serveurs d'applications existant et des méthodes d'authentification associées, aucun service d'acquisition de droits d'accès ne peut prétendre répondre seul à toutes les exigences. Pour cette raison, Policy Director est fourni avec un code source de serveur SAD de démonstration contenu dans le module IVAuthADK. Ce serveur SAD de démonstration peut être pris comme base de départ pour concevoir un système plus personnel, c'est-à-dire avec mappage des noms d'utilisateur de vos applications et ajout de fonctions de gestion de mappage.

WebSEAL doit être configuré pour accepter les clients SSL hors registre et pour acheminer les données d'authentification vers le service d'acquisition de droits d'accès approprié pour l'authentification de ces données et leur mappage à une identité Policy Director.

Le service d'acquisition de droits d'accès personnalisé doit utiliser des appels RPC pour sécuriser toutes les communications entre WebSEAL et le serveur SAD.

Les conditions requises pour le mappage des données des certificats X.509 à une identité Policy Director varient considérablement d'un besoin à l'autre. Bien que Policy Director n'impose pas de règles génériques pour définir un service de mappage, deux recommandation aideront l'administrateur à créer un service de mappage personnalisé.

1. Policy Director propose une interface IDL qui permet au développeur d'élaborer un service capable de mapper les données des certificats X.509 à des identités Policy Director. Pour plus d'informations sur l'interface IDL, reportez-vous au manuel Policy Director - Guide de programmation et de référence.
2. Policy Director est fourni avec un modèle de service de mappage qui constitue la base d'un serveur SAD et renvoie simplement un message d'échec après chaque requête. Ce modèle de base peut être transformé en un serveur SAD parfaitement exploitable pour l'entreprise.

   Le code source de ce service est fourni avec le module d'installation de Policy Director - IVAuthADK.

Tâches d'administration

Les tâches d'administration nécessaires à la création d'un service d'acquisition de droits d'accès personnalisé sont les suivantes :

1. Création d'un SAD personnalisé utilisant l'interface IDL fournie avec Policy Director.
2. Configuration de WebSEAL pour utiliser le service d'acquisition de droits d'accès externe pour l'authentification.

Fonctionnement d'un service d'acquisition de droits d'accès personnalisé

L'interface du service d'acquisition de droits d'accès personnalisé permet les fonctions suivantes :

- Validation des noms d'utilisateur et des mots de passe avec un registre d'utilisateurs autre que le registre par défaut de Policy Director.
- Mappage de plusieurs utilisateurs à une même identité Policy Director.
- Gestion des mots de passe d'utilisateurs externes.
- Ajout de données d'audit personnalisées au droit d'accès. Policy Director enregistre l'ensemble des données du droit d'accès dans son journal d'audit.

Chapitre 3. Principes de l'autorisation

L'autorisation est un processus qui détermine si une entité identifiée détient le droit ou l'autorité nécessaire pour :

- démarrer un service donné ;
- exécuter une opération sur une ressource d'un domaine sécurisé.

Le service d'autorisation de Policy Director facilite la mise en place des règles de sécurité d'un réseau en contrôlant le processus de décision d'attribution des autorisations.

Ce chapitre comprend les sections suivantes :

Modèle conceptuel d'autorisation

Lorsque des serveurs assurent la sécurité dans un domaine sécurisé, chaque client doit fournir la preuve de son identité. Ensuite, les règles de sécurité déterminent si le client a le droit d'exécuter une opération sur la ressource demandée. Le serveur contrôle l'accès à toutes les ressources du domaine sécurisé. A cet égard, les demandes d'authentification et d'autorisation qu'il produit peuvent assurer la sécurité globale du réseau.

L'authentification est un processus qui consiste à identifier une personne qui tente de se connecter à un domaine sécurisé.

Dans les systèmes de sécurité, l'authentification et l'autorisation sont deux choses distinctes.

- L'authentification est un processus qui consiste à identifier une personne qui tente de se connecter à un domaine sécurisé. L'authentification atteste que cet utilisateur est bien celui qu'il prétend être, mais n'intervient pas quant à son droit d'exécuter des opérations sur une ressource protégée.
- L'autorisation détermine si un client authentifié a le droit d'exécuter une opération sur une ressource donnée d'un domaine sécurisé. Dans le modèle d'autorisation, Policy Director applique les règles d'autorisation indépendamment de la procédure d'authentification utilisée. Les utilisateurs peuvent faire authentifier leur identité à l'aide d'une paire de clés privée/publique, d'une clé secrète, ou de procédures personnalisées.

Le processus d'authentification implique notamment l'acquisition d'un droit d'accès qui caractérise l'identité du client. Le service d'autorisation décide de l'attribution d'une autorisation sur la base de ces droits d'accès.

Les ressources d'un domaine sécurisé sont associées à un niveau de protection déterminé par les règles de sécurité définies pour le domaine. Ces règles de sécurité définissent les membres autorisés à accéder au domaine sécurisé et le niveau de protection propre à chaque ressource protégée.

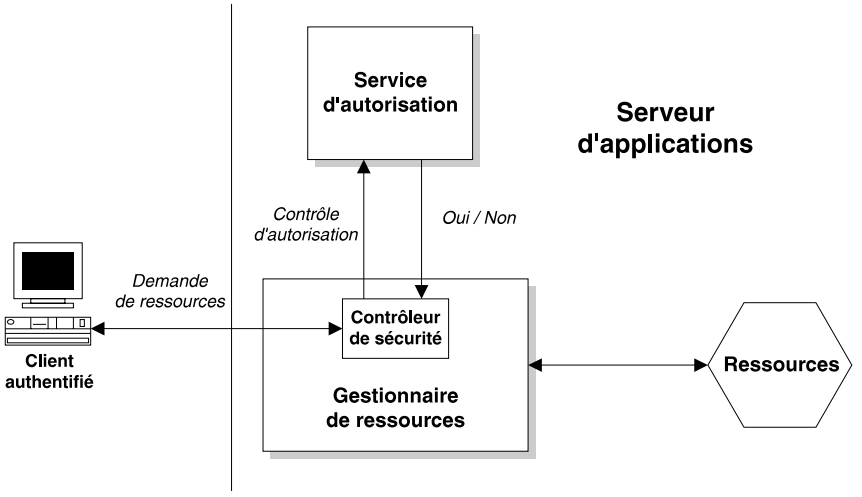
Le processus d'autorisation met en oeuvre les composants suivants :

Gestionnaire de ressources

Le gestionnaire de ressources est chargé de mener à bien l'opération demandée lorsque Policy Director a accordé l'autorisation requise. Le gestionnaire de ressources comprend un composant appelé le Contrôleur de sécurité. Sa mission consiste à router la requête vers le service d'autorisation afin qu'elle y soit traitée.

Service d'autorisation

Le service d'autorisation prend la décision d'autoriser ou non la requête.



Les applications conventionnelles englobent les actions du contrôleur de sécurité et du gestionnaire de ressources dans un même processus. Cette structure est notamment représentée par Policy Director WebSEAL et certaines applications tiers. L'indépendance de ces composants permet une grande souplesse dans la conception d'une stratégie de mise en place d'une sécurité.

Cette indépendance permet notamment à l'administrateur de la sécurité de contrôler :

- l'emplacement des processus ;
- l'auteur du code des processus ;
- la manière dont les processus s'accomplissent.

Avantages d'un service d'autorisation standard

Dans la plupart des systèmes, récents ou plus anciens, l'autorisation est étroitement liée aux applications proprement dites. Les entreprises développent leurs applications pour répondre à leurs besoins. Nombreuses parmi ces applications sont celles qui requièrent une forme ou une autre d'autorisation.

Cette situation produit souvent une grande diversité d'applications avec autant de systèmes d'autorisation différents. Ces programmes d'autorisation propriétaires nécessitent une gestion spécifique, sont difficiles à intégrer et induisent un coût de détention souvent élevé.

Un service d'autorisation partagé adapté peut apporter à ces applications indépendantes une méthode de prise de décision d'autorisation commune et standard.

Un service d'autorisation standard présente les avantages suivants :

- Réduction du coût de développement et de gestion des applications ;
- Réduction du coût total de détention et de gestion des différents systèmes d'autorisation ;
- Articulation avec l'infrastructure de sécurité existante ;
- Ouverture mieux sécurisée pour les nouvelles entreprises ;
- Possibilité d'utiliser davantage d'applications différentes ;
- Cycles de développement raccourcis ;
- Partage sécurisé des informations.

Avantages du service d'autorisation de Policy Director

Policy Director s'intègre parfaitement aux systèmes existants comme aux nouvelles infrastructures et offre des fonctions de gestion centralisée et sécurisée des règles de sécurité. Le service d'autorisation de Policy Director (associé à WebSEAL et au gestionnaire de ressources NetSEAL) constitue un système d'autorisation standard dédié aux systèmes de réseau des entreprises.

Les applications existantes peuvent utiliser le service d'autorisation sans nécessiter de modification. Les règles d'autorisation de Policy Director reposent sur les fonctions des utilisateurs ou des groupes. Vous pouvez appliquer ces règles d'autorisation aux entités suivantes :

- Serveurs de réseau ;
- Transactions ou requêtes de base de données ;
- Données Web ;
- Activités de gestion ;
- Objets définis par l'utilisateur.

L'API d'autorisation de Policy Director permet aux applications d'appeler le service d'autorisation de Policy Director. Ce service prend ensuite la décision d'accorder ou non l'autorisation demandée sur la base des règles de sécurité de l'entreprise. Pour plus d'informations, reportez-vous à la section «API d'autorisation de Policy Director» à la page 46.

Les fonctions du service d'autorisation de Policy Director peuvent également être étendues. Vous pouvez notamment le configurer pour qu'il appelle d'autres services d'autorisation en vue d'un traitement supplémentaire, par ″le biais de l'API d'autorisation externe.

Le service d'autorisation de Policy Director présente les avantages suivants :

- Indépendance vis-à-vis des applications ;
- Utilisation d'un style de chiffrement des autorisations indépendant du langage utilisé (l'API d'autorisation de Policy Director) ;
- Gestion centralisée et facilitée (par exemple, l'ajout d'un nouveau salarié nécessite de modifier la base de données des privilèges dans un emplacement central au lieu de plusieurs systèmes) ;
- Mise en oeuvre de services de sécurité dans un environnement hétérogène (composé de plates-formes différentes) ;
- Intégration des systèmes d'autorisation externes par le biais de fonctions de gestion adaptées ;
- Architecture évolutive et adaptable s'intégrant facilement aux moyens existants ;
- Possibilité d'autorisation multi-niveaux (le service transmet un paquet de droits d'accès à travers les différentes couches d'un processus ou d'une transaction) ;

- Utilisation d'un modèle d'audit commun et performant ;
- Indépendance vis-à-vis des autres méthodes d'authentification.

Policy Director - Service d'autorisation

Le service d'autorisation de Policy Director facilite la mise en place des règles de sécurité d'un réseau en contrôlant le processus de décision d'attribution des autorisations. Les décisions d'autorisation prises par le service consistent à accepter ou refuser les requêtes des clients désirant exécuter des opérations sur les ressources protégées du domaine sécurisé.

Composants du service d'autorisation de Policy Director

Le service d'autorisation de Policy Director comprend trois composants de base :

- La base de données principale (primaire) des règles d'autorisation ;
- Le serveur de gestion ;
- Le programme d'évaluation des décisions d'autorisation.

Base de données primaire des règles d'autorisation

La base de données primaire des règles d'autorisation contient les règles de sécurité applicables à toutes les ressources du domaine sécurisé. Elle contient également les données de droit d'accès des membres du domaine sécurisé.

Les informations de la base de données se modifient à l'aide de la console de gestion de Policy Director.

Serveur de gestion

Le serveur de gestion (ivmgrd) exécute les tâches suivantes :

- Gestion de la base de données primaire des règles d'autorisation ;
- Duplication des règles à travers le domaine sécurisé ;
- Mise à jour des instances (ou répliques) de la base de données en cas de modification de la base de données primaire des règles d'autorisation.

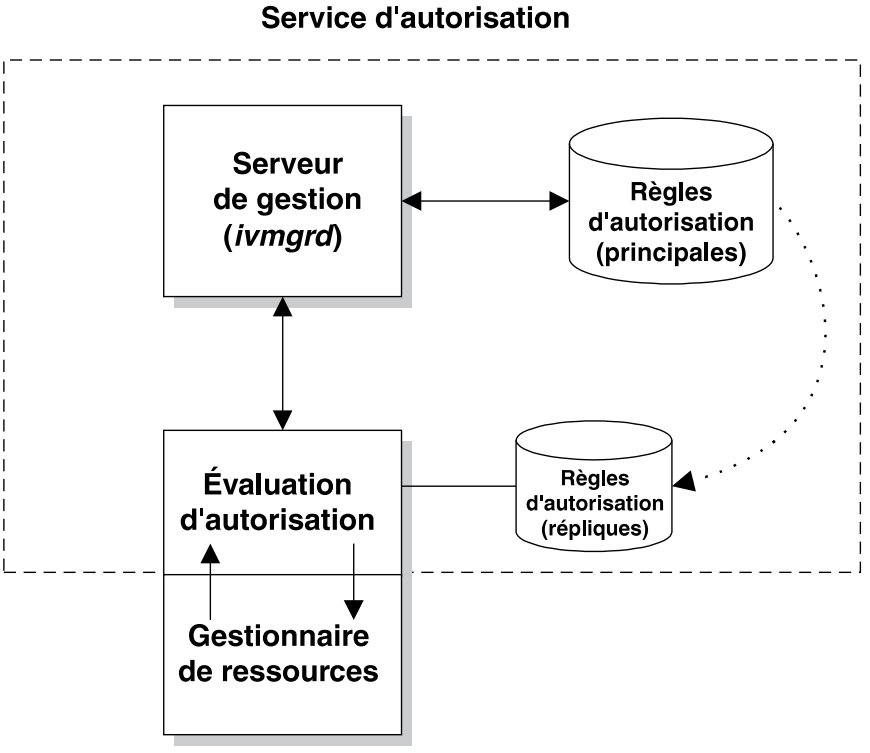
Le serveur de gestion administre également les données d'emplacement des autres serveurs (Policy Director ou non) du domaine sécurisé.

Remarque : Un domaine sécurisé ne doit contenir qu'une seule instance de serveur de gestion.

Evaluation des décisions d'autorisation

L'évaluation d'autorisation est le processus de décision qui détermine la capacité d'un client à accéder à une ressource protégée, sur la base des règles de sécurité définies. Le programme transmet une recommandation au gestionnaire de ressources qui, à son tour, répond à la requête en conséquence.

L'illustration suivante détaille les principaux composants du service d'autorisation de Policy Director :



Interfaces du service d'autorisation de Policy Director

Le service d'autorisation de Policy Director utilise deux interfaces pour exécuter ses opérations :

Interface de gestion

L'administrateur de la sécurité gère les règles de sécurité en vigueur dans le réseau. Il utilise la console de gestion de Policy Director ou l'utilitaire **ivadmin** pour :

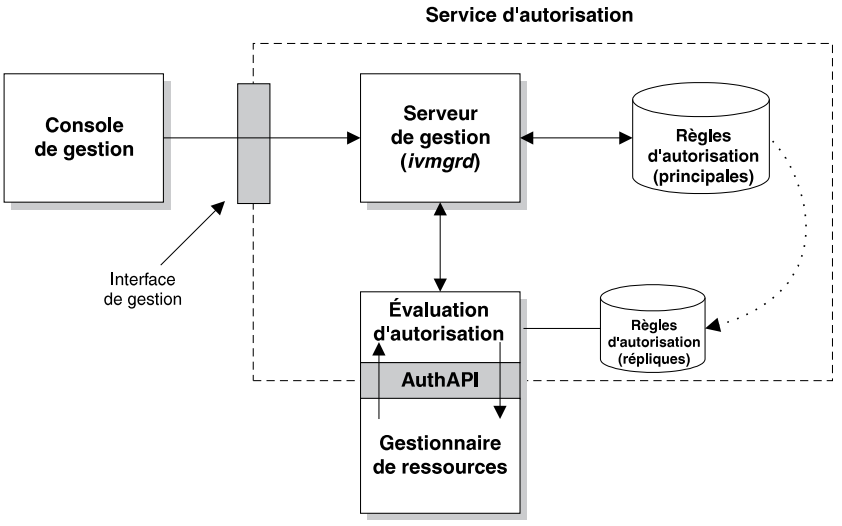
- appliquer les règles de sécurité (les modèles) aux ressources du réseau ;
- enregistrer les droits d'accès des membres du domaine sécurisé.

La console de gestion enregistre les règles de sécurité dans la base de données primaire des règles d'autorisation qui utilise le serveur de gestion.

Cette interface implique une parfaite connaissance de l'espace des noms, des modèles de règle et des droits d'accès.

API d'autorisation

L'API d'autorisation de Policy Director transmet les requêtes du gestionnaire de ressources au programme d'évaluation d'autorisation qui retourne une recommandation. Pour plus d'informations sur cette API, reportez-vous au manuel Policy Director - Guide de programmation et de référence.



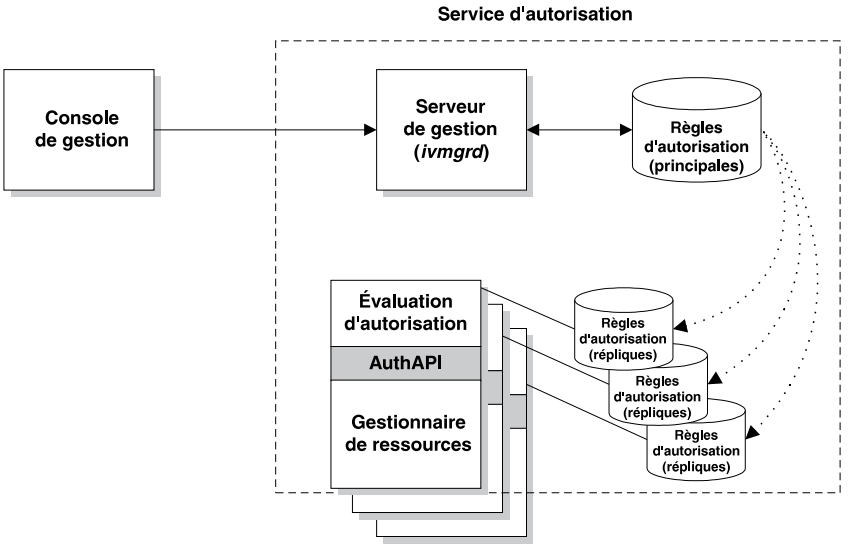
Duplication du service d’autorisation

Vous pouvez dupliquer le service d’autorisation de Policy Director pour accroître sa disponibilité dans un environnement particulièrement actif.

Policy Director duplique automatiquement la base de données primaire des règles d’autorisation qui contient les règles de sécurité et les droit d’accès. Les applications faisant appel au service d’autorisation ont deux options pour accéder aux informations de cette base de données :

- L’application peut utiliser le cache local de la base de données si elle est configurée pour fonctionner en mode transparent avec l’évaluation d’autorisation. La duplication de la base de données intervient pour chaque application utilisant le service d’autorisation en mode cache local.
- L’application utilise une instance partagée mise en antémémoire par le serveur d’autorisations distant de Policy Director. La duplication de la base de données intervient pour chaque instance du serveur d’autorisations de Policy Director. De nombreuses applications ne peuvent accéder qu’à un seul serveur d’autorisations.

Une notification de mise à jour envoyée par le serveur de gestion déclenche la mise à jour de toutes les instances par le processus d’antémémoire. Ces notifications de mise à jour interviennent à chaque modification de la base de données primaire des règles d’autorisation.



Remarques sur les performances

- Les serveurs d'applications reçoivent les notifications de mise à jour directement de la part du serveur de gestion. En outre, ils vérifient la version de la base de données primaire des règles d'autorisation plusieurs fois par heure afin de s'assurer qu'ils n'ont pas manqué une notification de mise à jour.

  Si une notification de mise à jour ne parvient pas à un serveur, Policy Director consigne l'événement par une entrée de journal. Dans les deux cas, un nouvel essai permet de s'assurer que la mise à jour se fera plus tard.
- La mise en antémémoire des règles d'autorisation accroît considérablement les performances du système. Par exemple, lorsque WebSEAL effectue un contrôle d'autorisation, il vérifie le modèle de règle contenu dans sa propre version cache de la base de données. WebSEAL n'a pas besoin d'accéder au réseau pour obtenir ces informations de la base de données primaire. Il en découle de meilleurs temps de réponse (performances) pour les contrôles d'autorisation.
- Le serveur d'applications à l'origine de l'appel ne met pas en antémémoire les résultats des requêtes d'autorisation.

Règles de sécurité du réseau

La manière dont vous contrôlez l'accès des utilisateurs et des groupes au domaine sécurisé détermine les règles de sécurité de ce domaine. Les règles de sécurité appliquées aux ressources nécessitant une protection sont appelées des modèles de règle.

Le service d'autorisation de Policy Director met en oeuvre ces règles en rattachant l'identité de l'utilisateur à des droits d'accès à l'aide du modèle de règle associé à la ressource demandée. Policy Director transmet la recommandation obtenue au gestionnaire de ressources qui répond à la requête d'origine.

Définition des règles de sécurité du réseau

Le service d'autorisation de Policy Director utilise une base de données centralisée qui répertorie toutes les ressources du domaine sécurisé et les modèles de règle qui leur sont attachés. La base de données primaire des règles d'autorisation et le

registre de sécurité sont les composants fondamentaux qui permettent de définir les règles de sécurité d'un réseau. Le registre de sécurité contient les données des comptes des utilisateurs et des groupes.

Sommairement, les règles de sécurité du réseau contrôlent :

- les utilisateurs et les groupes autorisés à accéder au domaine sécurisé (le registre de sécurité contient et gère ces informations) ;
- le niveau de protection de tous les objets du domaine sécurisé (la base de données primaire des règles d'autorisation gère ces information).

Espace des noms d'objet protégé

L'espace des noms d'objet protégé est une représentation hiérarchique des ressources d'un domaine sécurisé. Les objets apparaissant dans un espace des noms hiérarchisé représente les ressources du réseau.

- Une **ressource système** est un fichier physique, un service de réseau ou une application.
- Un **objet protégé** est la représentation d'une ressource système utilisée par le service d'autorisation de Policy Director, la console de gestion et les autres utilitaires de gestion de Policy Director.

Vous pouvez associer des modèles de règle aux objets dans l'espace des noms afin d'assurer une protection aux ressources correspondantes. Le service d'autorisation de Policy Director décide d'accorder ou non les autorisations sur la base de ces modèles de règle.

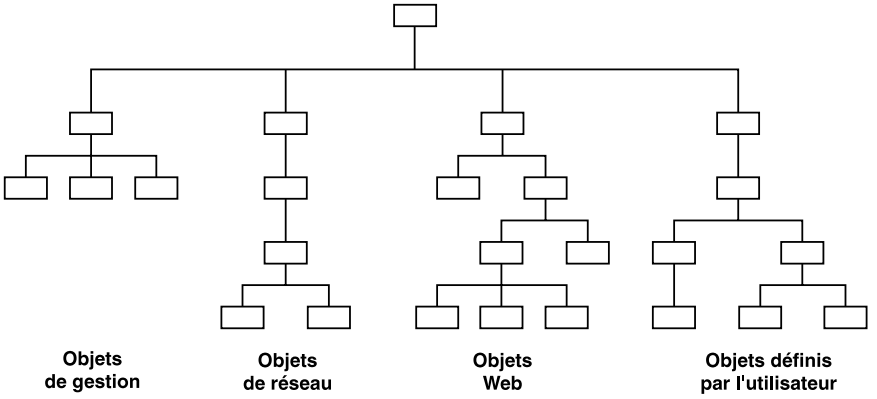
Policy Director utilise les catégories d'objet suivantes :

Objets Web
Ces objets correspondent à toute entité pouvant être liée à une adresse URL HTTP (pages Web statiques, URL dynamiques, etc.). Vous pouvez convertir des pages Web statiques et des URL dynamiques en requêtes de base de données ou en un autre type d'application.

Objets de réseau
Ces objets représentent des applications TCP (telles que TELNET et FTP) qui se rattachent aux adresses de réseau TCP (les ports) utilisées par les applications.

Objets de gestion
Ces objets se rattachent aux actions exécutées au moyen de la console de gestion de Policy Director. Ils représentent les tâches permettant de définir les utilisateurs et les règles de sécurité. Policy Director permet de déléguer les activités de gestion et de limiter le droit d'un administrateur à créer des règles de sécurité à une partie définie de l'espace des noms.

Objets définis par l'utilisateur
Ces objets représentent les tâches ou les ressources de réseau protégées par des applications utilisant le service d'autorisation de Policy Director (qui utilise pour sa part l'API d'autorisation).



Définition et application de modèles de règle

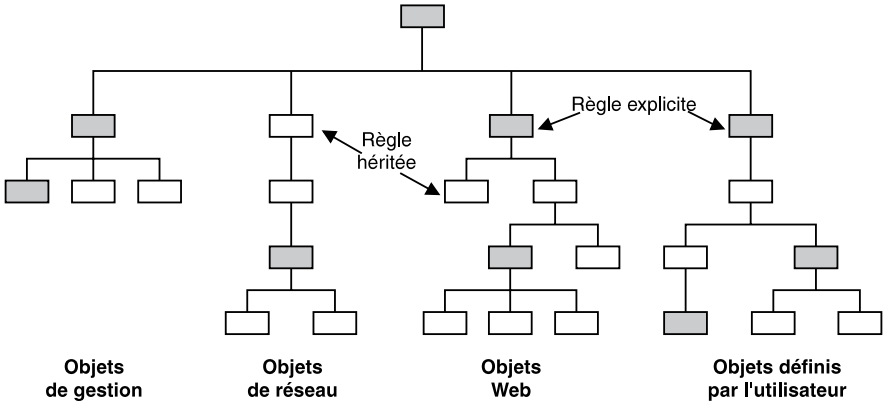
L'administrateur de la sécurité protège les ressources du système au moyen de modèles de règle appliqués aux objets représentant ces ressources dans l'espace des noms.

Le service d'autorisation de Policy Director prend des décisions d'autorisation sur la base des modèles de règle appliqués aux objets de l'espace des noms. Lorsque Policy Director autorise une requête sur un objet protégé, l'application en charge de la ressource exécute l'opération demandée.

Un même modèle de règle peut déterminer les paramètres de protection de plusieurs objets. Chaque modification de la règle se répercute sur tous les objets soumis au modèle.

Règles explicites et règles héritées

Un modèle de règle peut s'appliquer à un objet explicitement ou par héritage. L'espace des noms d'objet protégé permet la transmission par héritage des attributs des règles de sécurité. Cet aspect est important pour l'administrateur de la sécurité ayant la charge de gérer l'espace des noms. En substance, cet administrateur n'a qu'a appliquer de manière explicite les modèles de règle désirés sur les objets de la hiérarchie pour lesquels les règles doivent changer.



Il existe différent types de modèle de règle, notamment :

- les règles codées dans le programme ;
- les règles d'autorisation externes ;
- les étiquettes sécurisées spéciales ;

- les listes de contrôle d'accès.

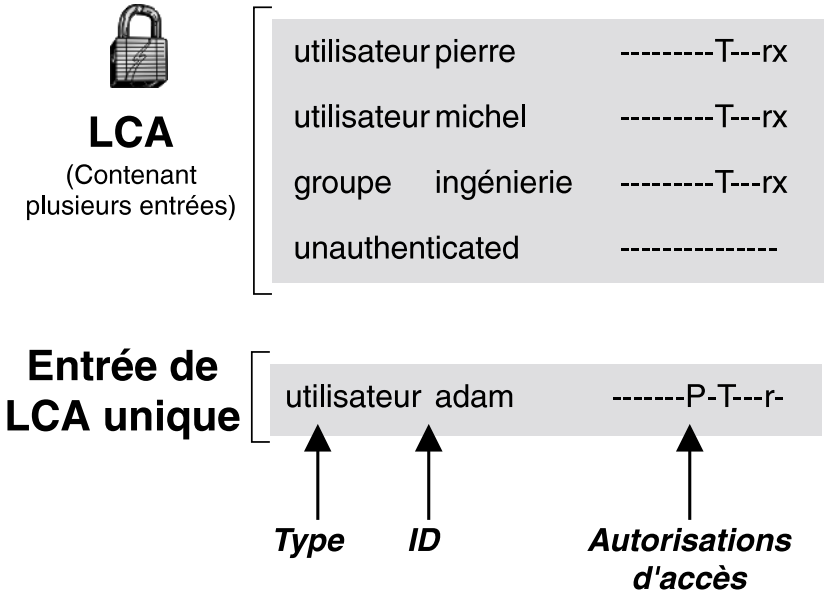
Liste de contrôle d'accès

Une liste de contrôle d'accès (LCA) est un type de modèle de règle parmi d'autres. Policy Director utilise les listes de contrôle d'accès comme principal modèle de règle.

Une liste de contrôle d'accès se compose d'une série de contrôles (autorisations) qui définissent les conditions requises pour exécuter certaines opérations sur la ressource associée. Les définitions de LCA jouent un rôle important dans les règles de sécurité établies pour le domaine sécurisé. Comme tous les modèles de règle, les listes de contrôle d'accès définissent les règles de sécurité qu'une organisation applique à ses ressources, représentées dans l'espace des noms d'objet protégé.

Une liste de contrôle d'accès contrôle en particulier :
- les opérations exécutées sur la ressource ;
- les personnes pouvant exécuter ces opérations.

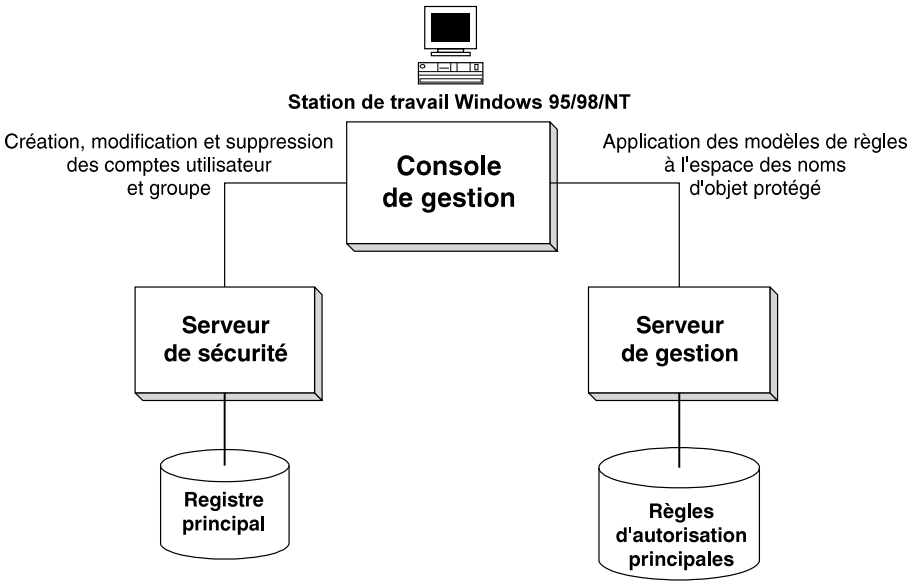
Une liste de contrôle d'accès se compose d'une ou plusieurs entrées définissant les noms des utilisateurs et des groupes ainsi que leurs autorisations et droits d'accès.



Administration des règles de sécurité

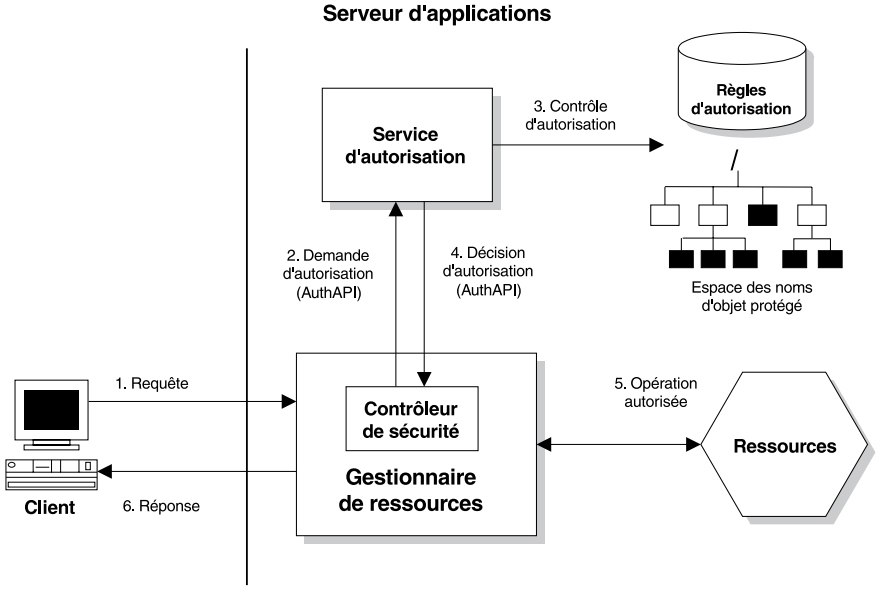
La console de gestion de Policy Director est une application graphique Java qui permet d'administrer les règles de sécurité dans un domaine sécurisé par Policy Director. L'utilitaire de ligne de commande **ivadmin** offre les mêmes fonctions que la console de gestion.

A partir de la console de gestion, ou par le biais de l'utilitaire **ivadmin**, vous pouvez gérer le registre du serveur de sécurité, la base de données primaire des règles d'autorisation et tous les serveurs de Policy Director. Vous pouvez également créer des utilisateurs et des groupes et appliquer des modèles de règle ou des listes de contrôle d'accès aux objets du réseau.



Etapes du processus d’autorisation

Le schéma suivant illustre le processus d’autorisation :



1. Policy Director dirige une requête de ressource émanant d’un client authentifié vers le serveur du gestionnaire de ressources. Le contrôleur de sécurité intercepte la requête.

   Le gestionnaire de ressources peut être WebSEAL (pour l’accès HTTP et HTTPS), NetSEAL (pour l’accès réseau TCP/IP), ou une application tiers.
2. Le contrôleur de sécurité utilise l’API d’autorisation de Policy Director (voir la section «API d’autorisation de Policy Director» à la page 46) pour appeler le service d’autorisation en vue d’obtenir une décision d’autorisation.
3. Le service d’autorisation effectue un contrôle d’autorisation sur la ressource représentée par un objet dans l’espace des noms d’objet protégé de Policy Director. Le modèle de règle appliqué à l’objet est comparé aux droits d’accès du client.

4. Le service d'autorisation renvoie au gestionnaire de ressources (par le biais du contrôleur de sécurité) une recommandation l'invitant à accepter ou refuser la requête.
5. Si le contrôle d'autorisation approuve la requête, le gestionnaire de ressources la transmet à l'application en charge de la ressource.
6. Le client obtient alors les résultats de l'opération demandée.

API d'autorisation de Policy Director

L' interface de programme d'application (API) du service d'autorisation de Policy Director permet aux applications Policy Director et aux autres applications de demander des décisions d'autorisation au service d'autorisation de Policy Director.

L'API d'autorisation de Policy Director sert d'interface entre le gestionnaire de ressources (qui demande le contrôle d'autorisation) et le service d'autorisation lui-même. Elle permet à l'application responsable de la mise en oeuvre des règles de sécurité de demander une décision d'autorisation. En d'autres termes, l'API d'autorisation masque la complexité du processus de prise de décision proprement dit.

L'API d'autorisation de Policy Director permet d'utiliser un modèle de programmation standard pour le chiffrement des requêtes d'autorisation et des décisions. Elle permet d'adresser des appels standardisés au service d'autorisation centralisé à partir de n'importe quelle application, nouvelle ou ancienne.

L'API d'autorisation de Policy Director peut s'utiliser en deux modes :

Mode cache distant

Dans ce mode, Policy Director initialise l'API pour appeler son serveur d'autorisations distant (ivacld) afin qu'il prenne une décision d'autorisation au bénéfice de l'application. Ce serveur d'autorisations gère son propre cache qui contient une instance de la base de données des règles d'autorisation. Ce mode convient pour gérer les requêtes d'autorisation des clients de type application.

Reportez-vous à la section «Mode cache distant» à la page 48.

Mode cache local

Dans ce mode, Policy Director initialise l'API pour télécharger et gérer une instance locale de la base de données des autorisations pour l'application. Le mode cache local permet à l'application de prendre toutes les décisions d'autorisation localement, ce qui induit un gain de performances et de fiabilité.

Cependant, la charge induite par la duplication de la base de données et les implications de ce mode pour la sécurité le rende surtout adapté aux serveurs d'applications sécurisés. Les serveurs d'applications sécurisés comprennent notamment WebSEAL et NetSEAL.

Reportez-vous à la section «Mode cache local» à la page 49.

L'atout et l'avantage majeurs de l'API d'autorisation de Policy Director résident dans le fait qu'elle dissimule à l'utilisateur la complexité du mécanisme du service d'autorisation lui-même. En effet, l'API d'autorisation de Policy Director masque les opérations liées à la gestion, au stockage, à la mise en antémémoire, à la duplication de la base de données, au format des droits d'accès et aux méthodes d'authentification.

L'API d'autorisation de Policy Director fonctionne également indépendamment de l'infrastructure de sécurité sous-jacente, du format des droits d'accès et du processus d'évaluation. Elle permet d'adresser une requête de contrôle d'autorisation et d'obtenir une simple recommandation "oui" ou "non" en retour. Le déroulement du processus de contrôle d'autorisation est parfaitement invisible pour l'utilisateur.

L'API d'autorisation de Policy Director peut être utilisée sur les plates-formes suivantes :

- Microsoft Windows NT, Windows 98 et Windows 95
- IBM AIX version 4.3
- Sun Solaris version 2.6

Exemples d'API d'autorisation

Les services d'autorisation WebSEAL et NetSEAL opèrent un contrôle d'accès respectivement sur les adresses URL et sur les ports. Une application tiers peut utiliser l'API d'autorisation de Policy Director pour réaliser des contrôles d'accès sur des processus très spécifiques et spécialisés.

Exemple 1 : Vous pouvez concevoir une interface utilisateur graphique (GUI) pour afficher dynamiquement les boutons de tâche comme actifs ou inactifs, selon le résultat du contrôle d'autorisation.

Exemple 2 : L'illustration suivante détaille une autre forme d'utilisation de l'API d'autorisation de Policy Director. Elle illustre comment une application Web peut adresser une requête de transaction CGI.

Le premier niveau de contrôle d'autorisation (illustration A) implique un contrôle d'accès de type "tout ou rien" sur une adresse URL. Ce contrôle d'autorisation allégé ne fait que déterminer si le client peut ou non exécuter le programme CGI. Une fois l'accès autorisé à l'application CGI, plus aucun contrôle ne se fait sur les ressources manipulées par cette application.

Dans l'illustration B, les contrôles d'accès portent sur une série de ressources que le programme CGI manipule. L'application Web est configurée pour utiliser l'API d'autorisation de Policy Director. Ici, le programme CGI peut appeler le service d'autorisation de Policy Director pour obtenir les autorisations requises pour les ressources qu'il désire manipuler. Les décisions d'autorisation peuvent reposer sur l'identité du client à l'origine de la requête.

Figure A

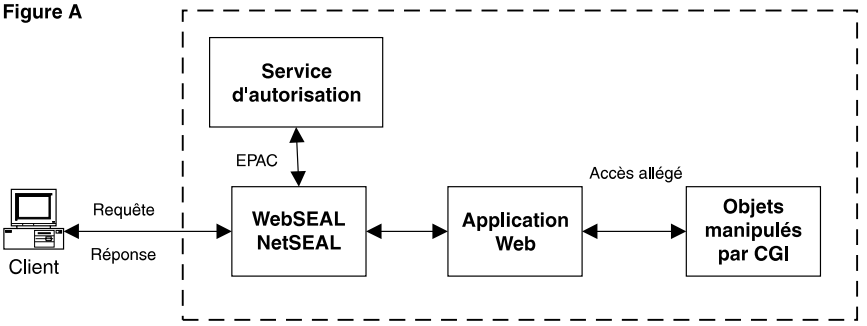
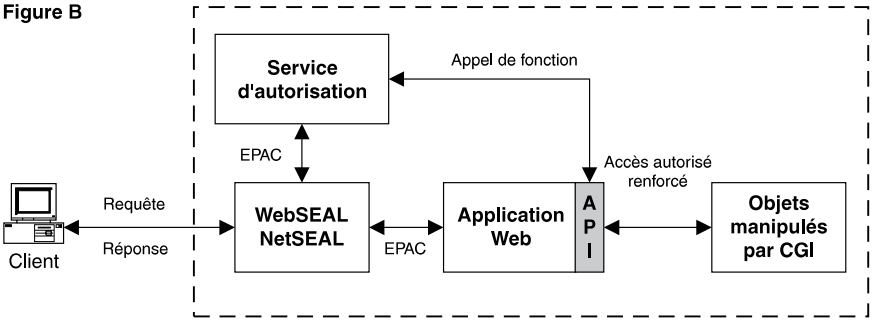


Figure B

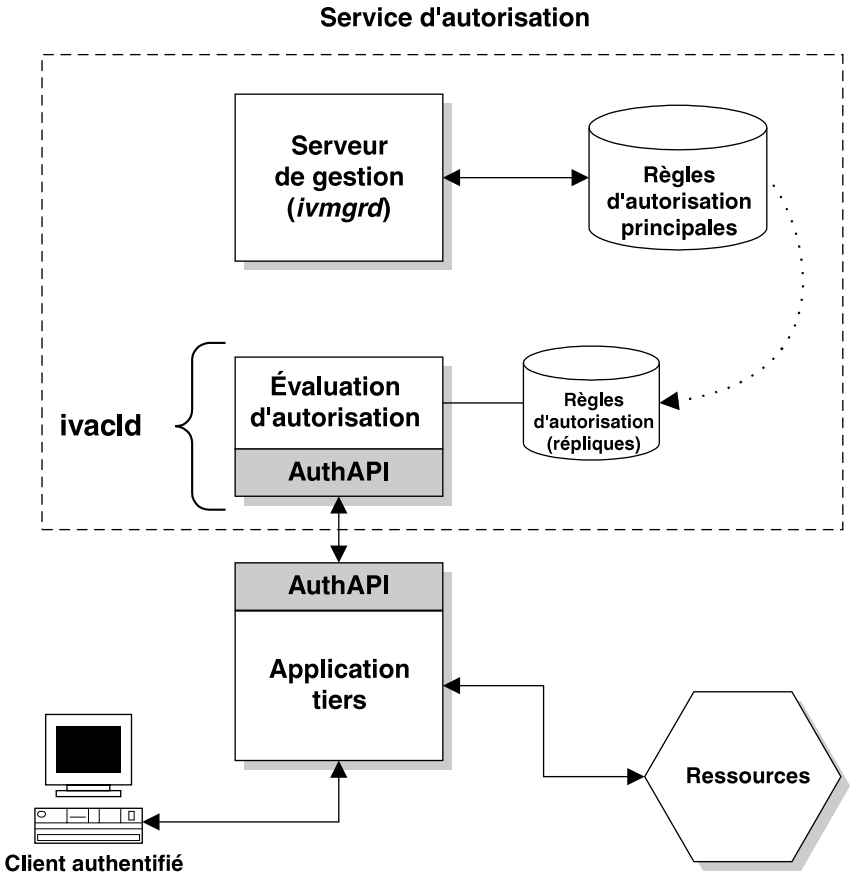


Mode cache distant

Dans le mode cache distant, les applications utilisent les appels de fonction de l'API d'autorisation de Policy Director pour communiquer avec le serveur d'autorisations distant de Policy Director (ivacld). Ce serveur d'autorisations fonctionne comme le programme d'évaluation des décisions d'autorisation et gère sa propre instance de la base de données des règles d'autorisation.

Le serveur d'autorisations de Policy Director prend la décision et renvoie une recommandation à l'application au moyen de l'API. Le serveur peut également enregistrer un rapport d'audit contenant le détail de la requête d'autorisation.

Il doit impérativement exister un serveur d'autorisations Policy Director défini quelque part dans le domaine sécurisé. Ce serveur peut résider sur la même machine que l'application ou sur une autre. Vous pouvez également l'installer sur plusieurs machines d'un domaine sécurisé pour obtenir une plus grande accessibilité. L'API d'autorisation de Policy Director échoue de manière transparente en cas de défaillance d'un serveur d'autorisations.



Mode cache local

En mode cache local, l'API télécharge et gère une instance de la base de données des règles d'autorisation dans le système de fichiers local de l'application. Elle effectue toutes les opérations de décision dans la mémoire, ce qui induit un gain de performances et de fiabilité.

L'instance locale est entretenue en permanence pendant les appels de l'application. L'API démarre en mode réplique, puis contrôle l'existence de mises à jour de la base de données primaire des règles d'autorisation. Ces mises à jour peuvent être intervenues après la création de l'instance locale.

Figure A

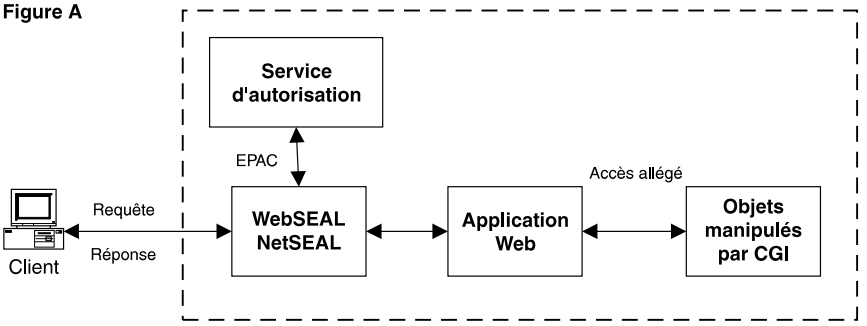
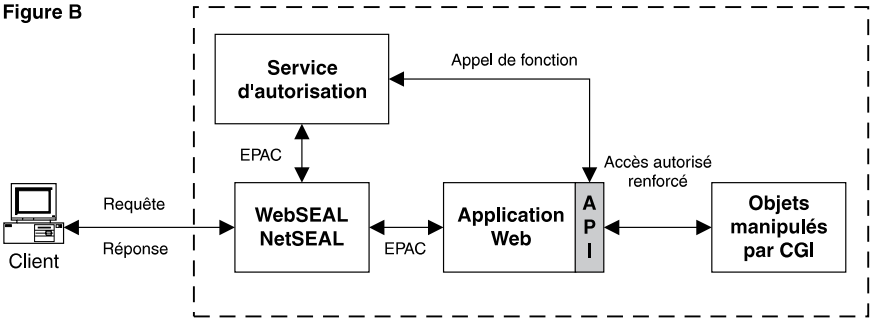


Figure B



Fonction d'autorisation externe

Dans certaines situations, la série d'autorisations standard de Policy Director peut ne pas exprimer toutes les règles de sécurité voulues par une entreprise. Pour cette raison, Policy Director propose une fonction d'autorisation externe, installable en option, afin de répondre aux besoins particuliers en matière d'autorisation.

Un service d'autorisation externe permet d'imposer des contrôles d'autorisation et des conditions supplémentaires définis par un programme de serveur d'autorisations externe et séparé.

Extension du service d'autorisation

Le service d'autorisation de Policy Director intègre automatiquement une fonction d'autorisation externe. Si vous configurez ce type de service, le service d'autorisation de Policy Director ajoutera simplement les nouveaux contrôles et les nouvelles conditions à son processus d'évaluation.

Les applications utilisant le service d'autorisation de Policy Director comprennent WebSEAL, NetSEAL et toutes les applications ayant recours à l'API d'autorisation de Policy Director. Ces applications tirent partie de la contribution supplémentaire, mais transparente, d'un service d'autorisation externe. Tout ajout aux règles de sécurité par l'utilisation d'un service d'autorisation externe est transparent pour ces applications et ne nécessite pas de les modifier.

L'architecture du service d'autorisation externe permet son intégration totale avec les services de sécurité existants d'un réseau d'entreprise et pérennise l'investissement initialement réalisé dans les systèmes de sécurité. Ce type de service d'autorisation externe permet aux serveurs existants de trouver leur place dans le processus de décision d'autorisation de Policy Director.

La configuration d'un service d'autorisation externe implique les étapes suivantes :

1. Conception d'un programme de serveur qui sera utilisé au cours du processus de décision d'autorisation.
2. Enregistrement du service d'autorisation externe dans le registre de Policy Director.

Une fois le service enregistré, un nouveau droit d'accès lui correspondant apparaît dans la console de gestion de Policy Director. Vous pouvez ensuite faire figurer ce droit d'accès dans une entrée de liste de contrôle d'accès.

Lorsque ce droit d'accès apparaîtra au cours d'un contrôle d'autorisation, le service d'autorisation externe sera consulté pour la prise de décision d'autorisation correspondante.

Pour plus d'informations sur la configuration d'un service d'autorisation externe, reportez-vous au manuel Policy Director - Guide de programmation et de référence.

Conditions applicables aux requêtes de ressources

Vous pouvez également utiliser un service d'autorisation externe pour imposer une condition particulière à une tentative d'accès, réussie ou non.

Les conditions concernées sont notamment les suivantes :

- Déclenchement de l'enregistrement de la tentative d'accès réussie ou non par une procédure d'audit.
- Surveillance active de la tentative d'accès et émission d'une alerte ou d'une alarme en cas de détection d'un comportement interdit.
- Exécution de transactions de facturation et de paiement électronique.

Processus d'évaluation des autorisations

Une décision d'autorisation impliquant un service d'autorisation externe se prend de la manière suivante :

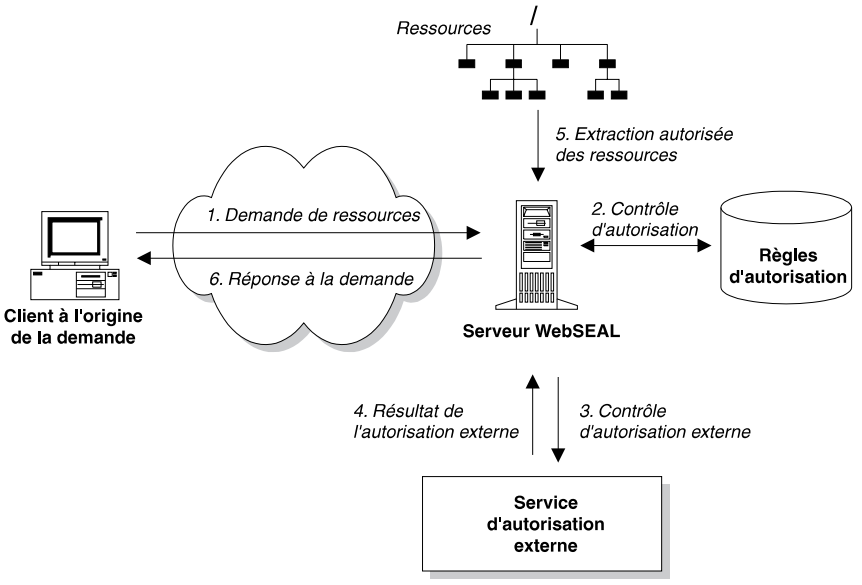
1. Le processus vérifie la liste de contrôle d'accès pour déterminer les droits d'accès détenus par l'utilisateur.
2. Il envoie une requête d'autorisation via un appel RPC authentifié à chaque service d'autorisation externe dont les droit d'accès figurent dans la liste de contrôle d'accès.

   Ce contrôle d'autorisation externe intervient que l'utilisateur ait les droits d'accès nécessaires ou non.
3. Le processus récapitule tous les résultats des décisions d'autorisation.

   L'interdiction d'accès peut résulter de la vérification de la liste de contrôle d'accès de Policy Director ou d'un contrôle d'autorisation externe. En cas de refus de droit d'accès, le service d'autorisation de Policy Director rejettera la requête d'autorisation.

Exemple :

L'illustration suivante détaille une décision d'autorisation impliquant un serveur WebSEAL et un service d'autorisation externe.



Dans cet exemple, la finalité du service d'autorisation externe est d'imposer des restrictions de durée pour l'accès aux objets. Le caractère utilisé pour représenter le droit d'accès dans la console de gestion est ″k″.

1. Le serveur WebSEAL réceptionne une requête de la part d'un client désirant accéder à un document technique sensible. Le client est membre du groupe des ingénieurs.
2. Le serveur WebSEAL consulte tout d'abord la réplique de la base de données des règles d'autorisation pour déterminer les droits d'accès définis pour l'objet du document.

   ```
   group ingénierie rk
   ```

   Si l'entrée de liste de contrôle d'accès ne contient pas le droit d'accès du service d'autorisation externe, la décision d'autorisation finale reposera sur ces seules informations.

   Dans l'exemple ci-dessus, l'entrée de LCA contient un droit de lecture standard. L'entrée contient également un droit d'accès supplémentaire (k) qui renvoie à un serveur d'autorisations externe à consulter pour mieux évaluer l'autorisation.
3. Policy Director envoie une requête au serveur d'autorisations externe au moyen d'un appel RPC authentifié. La série de droits d'accès accordée a été déterminée au cours de l'étape 2. Policy Director transmet cette série de droits d'accès avec la requête de manière à ce que le serveur d'autorisations externe puisse baser sa décision sur ces informations.

   Dans cet exemple, la conception du serveur d'autorisations externe permet de limiter l'accès à ce document à des périodes déterminées. L'accès au document n'est autorisé qu'entre 08h00 et 18h00, du lundi au vendredi.
4. Dans cet exemple, le client a adressé sa requête un mardi à 10h00. Le serveur d'autorisations renvoie une réponse positive au serveur WebSEAL.

   L'ensemble des décisions d'autorisation aboutit à une recommandation finale d'autoriser l'accès à l'objet du document.
5. Le serveur WebSEAL récupère la ressource demandée.
6. Le serveur WebSEAL autorise le client à visualiser le document.

Pour plus d'informations sur la mise en oeuvre d'un service d'autorisation externe, reportez-vous au manuel Policy Director - Guide de programmation et de référence.

Stratégies de mise en oeuvre

Policy Director permet de mettre en place un service d'autorisation externe de plusieurs manières :

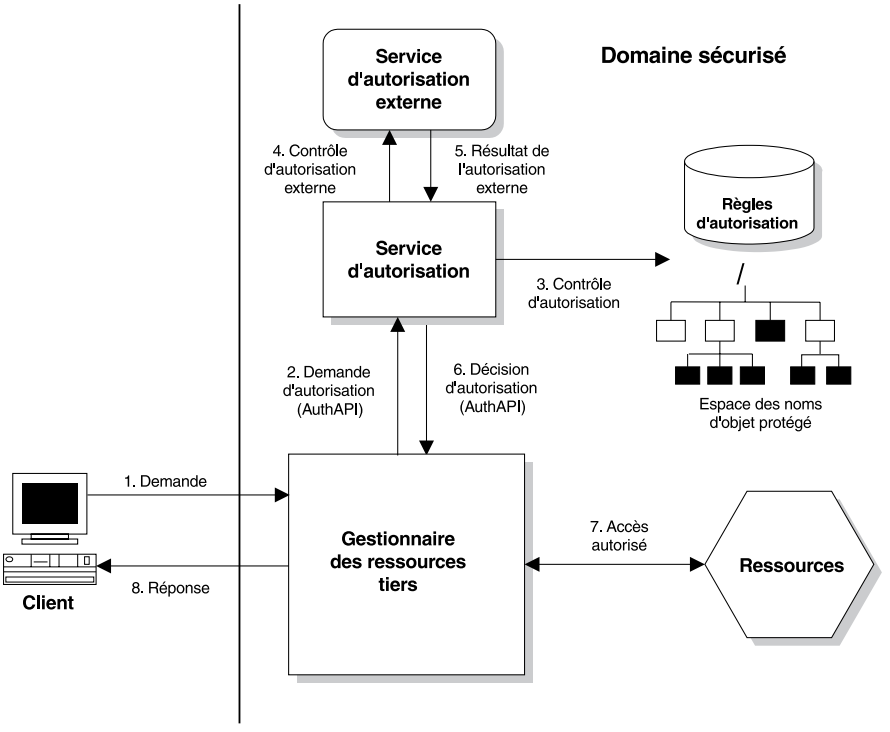
- Vous pouvez ajouter autant de services d'autorisation externes que vous le désirez à votre domaine sécurisé pour les différents types d'évaluation d'autorisation dont vous avez besoin. Chaque droit d'accès figurant dans une liste de contrôle d'accès correspond à un service différent.
- Vous pouvez appeler plusieurs serveurs d'autorisation externes pour un droit d'accès donné en les chaînant ensemble. Chaque serveur de la chaîne transmet l'identité authentifiée au serveur suivant et recueille les résultats obtenus jusque là.
- Vous pouvez dupliquer un service d'autorisation externe à travers le domaine sécurisé.

Chacune de ces implémentations est indépendante des autres et peut être mise en oeuvre de manière combinée.

Extensibilité et adaptabilité

La combinaison de l'API d'autorisation de Policy Director et d'un service d'autorisation externe produit une solution extensible et adaptable pour mettre en place des règles de sécurité.

L'illustration suivante détaille l'architecture évolutive que vous pouvez mettre en place au moyen des fonctions combinées de l'API d'autorisation de Policy Director, pour une application tiers, et d'un service d'autorisation externe.



Chapitre 4. Présentation de la console de gestion

La console de gestion de Policy Director est une application graphique Java qui permet d'administrer en toute sécurité les composants de Policy Director dans le cadre d'un réseau partagé. A partir de la console de gestion, vous pouvez gérer le registre du serveur de sécurité, la base de données primaire des règles d'autorisation et tous les serveurs de Policy Director. La console de gestion permet également de créer ou de supprimer des utilisateurs et des groupes et d'appliquer des listes de contrôle d'accès.

Ce chapitre comprend les sections suivantes :

Présentation générale de la console de gestion

La console de gestion de Policy Director est une application graphique Java qui permet d'administrer les règles de sécurité dans un domaine sécurisé par Policy Director. L'utilitaire de ligne de commande **ivadmin** offre les mêmes fonctions d'administration que la console de gestion.

A partir de la console de gestion, ou par le biais de l'utilitaire **ivadmin**, vous pouvez :

- modifier la base de données du registre (comptes) ;
- modifier la base de données primaire des règles d'autorisation (LCA) ;
- ajouter ou supprimer des utilisateurs ;
- ajouter ou supprimer des groupes ;
- appliquer des modèles de règle ou des listes de contrôle d'accès aux objets ;
- ajouter, supprimer ou modifier des ressources GSO, des groupes de ressources et des droits d'accès de ressources ;
- ajouter, supprimer ou modifier un utilisateur relais (facultatif).

Caractéristiques de la console de gestion

La fenêtre de la console de gestion affiche des informations et propose des outils permettant d'effectuer des tâches de gestion. Les principaux outils et zones d'affichage sont les suivants :

- onglets des tâches
- panneaux des tâches de gestion (panneau du haut et panneau du bas)
- boutons de commande
- barre d'outils
- tableau d'informations (panneau inférieur par défaut)

- barre d'état
- barre de titre

Outils des panneaux des tâches de gestion

Les panneaux des tâches de gestion proposent les outils suivants :

- onglets des tâches
- panneaux des tâches de gestion (panneau du haut et panneau du bas)
- boutons de commande

Onglets des tâches

La console de gestion contient les onglets de tâches suivants :

- Connexion
- Utilisateurs
- Groupes
- Ressources GSO
- Groupes de ressources GSO
- LCA
- Espace objets
- Utilisateur relais (facultatif)

Panneaux des tâches de gestion

Chaque onglet de tâches ouvre un panneau de tâches de gestion qui comprend plusieurs zones d'affichage d'informations également présentes dans le panneau supérieur de la console de gestion.

Les tâches de gestion comprennent :

Connexion La tâche Connexion est la première étape pour se connecter ou se déconnecter de la console de gestion.

Utilisateurs	Permet de créer et de gérer les utilisateurs membres du domaine sécurisé.
Groupes	Permet de créer et de gérer les groupes membres du domaine sécurisé.
Ressources GSO	Permet de créer et de gérer les données des ressources GSO.
Groupes de ressources GSO	Permet de créer et de gérer les données des groupes de ressources GSO.
LCA	Permet de créer et de gérer les modèles de règle et les listes de contrôle d'accès (LCA).
Espace objets	Permet d'associer des modèles de règle aux objets définis dans l'espace des noms.
Utilisateur relais	Permet de créer et de gérer les données des utilisateurs relais.

Boutons de commande

Chaque onglet de tâches comporte une série de boutons de commande spécifique. Ces boutons de commande permettent d'exécuter des opérations de gestion. Ils apparaissent sur le côté gauche du panneau. Les boutons de commande permettent notamment de modifier et de mettre à jour les différentes bases de données.

Mode d'affichage des panneaux

Vous pouvez afficher les informations des panneaux de tâches de gestion selon trois modes d'affichage différents. Chaque type de vue a ses caractéristiques distinctives :

Détail La vue détaillée contient des champs dynamiques permettant la saisie des données.

Liste Les données d'une vue avec liste peuvent être triées par ordre croissant ou décroissant. Pour cela cliquez sur la barre de titre de la colonne désirée. Certaines listes permettent les requêtes.

Arborescence

Une vue arborescente peut être agrandie ou réduite.

Lorsque vous sélectionnez un élément actif dans l'arborescence, celui-ci se met en relief en devenant bleu.

Lorsque vous sélectionnez un élément inactif dans l'arborescence, celui-ci devient gris.

Barre d'outils

La barre d'outils se trouve dans la partie supérieure de la fenêtre de la console de gestion et comprend des boutons qui activent des fonctions de la console.

Le bouton **Déplacer tâche en bas** déplace la tâche de gestion courante du panneau du haut dans celui du bas.

Le bouton **Déplacer tâche en haut** déplace la tâche de gestion courante du panneau du bas dans celui du haut.

Le bouton **Attacher vue** copie dans le panneau du bas les informations actives sélectionnées dans le panneau du haut. Les informations actives sélectionnées dans le panneau supérieur peuvent, par exemple, représenter une liste d'utilisateurs ou de groupes. Un nouvel onglet apparaît également pour le panneau sélectionné. Les informations contenues dans ce panneau ne sont qu'une copie statique (non dynamique) des données d'origine. En revanche, vous pouvez agrandir ou réduire les vues arborescentes, notamment l'arborescence de l'espace des objets et la liste des groupes.

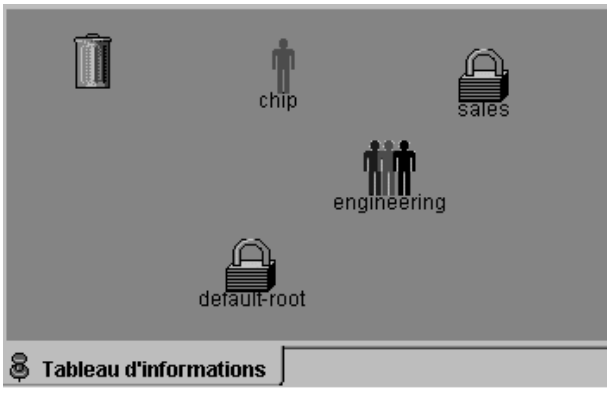
Le bouton **Effacer** efface la vue sélectionnée de la console de gestion. Cette action ne fait qu'effacer la vue de l'écran et est sans effet sur les informations de la base de données.

Le bouton **Arrêter** interrompt l'action en cours et redonne le contrôle de la console de gestion à l'administrateur. La console de gestion ignore le résultat de l'action abandonnée et réagit comme si l'opération avait échoué.

Tableau d'informations

Le Tableau d'informations est le panneau inférieur par défaut de la console de gestion. Il permet de stocker provisoirement n'importe quel objet que vous voulez utiliser plusieurs fois au cours d'une session d'administration. Ces objets comprennent les fichiers, les listes de contrôle d'accès, les listes d'utilisateurs et de groupes, ainsi que les attributs. Pour utiliser ces objets dans les tâches d'administration, faites glisser les icônes associées dans le Tableau d'informations.

Les icônes standard du Tableau d'informations sont notamment l'icône **Corbeille** et l'icône **Attacher vue**.



Icône Corbeille

Pour supprimer les icônes placées dans le Tableau d'informations, faites-les glisser sur l'icône **Corbeille**.

Panneau de rattachement de vue

Vous pouvez sélectionner (mettre en évidence) des objets et des informations dans les différents panneaux de tâches de gestion et les faire glisser sur l'icône **Attacher vue** du Tableau d'informations.

Dans le bas de l'écran apparaît alors un nouveau panneau contenant une copie des informations sélectionnées. Un nouvel onglet apparaît également.

Les informations contenues dans ce panneau ne sont qu'une copie statique (non dynamique) des données d'origine. En revanche, vous pouvez agrandir ou réduire les vues arborescentes, notamment l'arborescence de l'espace des objets et la liste des groupes.

S'il s'agit d'une liste de groupes, seuls les groupes sélectionnés (mis en évidence) apparaîtront dans le panneau de rattachement de vue.

Pour fermer ce panneau, cliquez sur le bouton de fermeture de fenêtre placé dans l'angle supérieur droit de la fenêtre Windows.

Remarque : La même chose se produit si vous sélectionnez ces informations et que vous cliquez sur le bouton **Attacher vue** de la barre d'outils.

Barre d'état

La barre d'état placée en bas de la fenêtre de la console de gestion contient des messages d'erreur et des messages d'état.

- Les données d'état générales apparaissent en **noir**.
- Les avertissements apparaissent en **bleu**.
- Les erreurs sont indiquées en **rouge**.

Une icône d'indicateur d'état apparaît à gauche de la zone des messages :

icône de l'état Terminé

icône de l'état Avertissement

icône de l'état Erreur

Si vous cliquez deux fois sur l'icône de l'indicateur d'état, la barre d'état affiche :

- la version de la console de gestion ;
- le domaine sécurisé concerné par les actions ;
- la version Java.

Barre de titre

La barre de titre de la console de gestion affiche deux informations importantes :

- Le domaine sécurisé concerné par les actions de la console de gestion ;
- L'état de connexion de l'utilisateur (mise à jour ou en lecture seule).

Lorsque le registre du serveur de sécurité primaire est indisponible, vous ne pouvez pas modifier les données de compte par la console de gestion. Dans cette rare situation, la console de gestion obtient les données des comptes à partir de répliques du registre. Un message d'erreur s'affiche si vous tentez de modifier des informations ayant une incidence sur le registre.

Tâche de gestion Connexion

Le panneau de tâche Connexion est le premier des panneaux de la console de gestion apparaissant à un utilisateur authentifié. Si la requête de connexion aboutit, l'ensemble des onglets des tâches de gestion apparaissent également.

Lorsque l'utilisateur se déconnecte, le contexte est perdu et les onglets de tâches disparaissent de l'écran.

Onglet de tâches

Onglet de tâches : **Connexion**

Tâche de gestion

Le panneau de tâches de gestion Connexions contient des champs de saisie permettant d'entrer un **nom d'utilisateur** et un **Mot de passe**. Le champ **Domaine sécurisé** contient au départ le nom du domaine sécurisé configuré par défaut pour NetSEAT.

Le menu Connexion permet de choisir un autre domaine sécurisé pour exécuter les tâches de la console de gestion.

Boutons de commande

Les boutons de commande du panneau **Connexion** sont les suivants :

- Connexion
- Déconnexion

Tâche de gestion Utilisateurs

Le panneau de tâches de gestion Utilisateurs permet de créer et de gérer les utilisateurs membres du domaine sécurisé. Lorsque vous sélectionnez un utilisateur dans la liste, ou dans l'arborescence, les champs de la vue détaillée sont automatiquement renseignés avec les données associées à la sélection courante.

Onglet de tâches

Onglet de tâches : **Utilisateurs**

Tâche de gestion

Le panneau de tâches de gestion Utilisateurs contient trois vues : une liste des utilisateurs, une vue détaillée des utilisateurs et une liste des groupes.

La vue Groupes contient deux onglets supplémentaires : Ressources GSO et Groupes de ressources GSO.

Boutons de commande

Les boutons de commande du panneau **Utilisateurs** sont les suivants :

- Nouveau
- Extraction
- Sauvegarde
- Suppression

Tâche de gestion Groupes

Le panneau de tâches de gestion Groupes permet de créer et de gérer les groupes membres du domaine sécurisé. Lorsque vous sélectionnez un groupe dans la liste, ou dans l'arborescence, les champs de la vue détaillée sont automatiquement renseignés avec les données associées à la sélection courante.

Onglet de tâches

Onglet de tâches : **Groupes**

Tâche de gestion

Le panneau de tâches de gestion Groupes contient trois vues : une liste des groupes, une vue détaillée des groupes et une liste des ID utilisateur.

Boutons de commande

Les boutons de commande du panneau **Groupes** sont les suivants :

- Nouveau
- Extraction
- Sauvegarde
- Suppression

Tâche de gestion Ressources GSO

Le panneau de tâches de gestion Ressources GSO permet de créer et de gérer des ressources GSO dans le domaine sécurisé. Les ressources GSO sont systématiquement des ressources Web. Lorsque vous sélectionnez une ressource GSO dans la liste, ou dans l'arborescence, les champs de la vue détaillée sont automatiquement renseignés avec les données associées à la sélection courante.

Onglet de tâches

Onglet de tâches : **Ressources GSO**

Tâche de gestion

Le panneau de tâches de gestion Ressources GSO contient deux vues : une liste des ressources GSO et une vue détaillée de ces ressources.

Boutons de commande

Les boutons de commande du panneau **Ressources GSO** sont les suivants :

- Nouveau
- Extraction

- Sauvegarde
- Suppression

Tâche de gestion Groupes de ressources GSO

Le panneau de tâches de gestion Groupes de ressources GSO permet de créer et de gérer des groupes de ressources GSO dans le domaine sécurisé. Un groupe de ressources est un groupe de serveurs Web utilisant tous la même série d'ID utilisateur et de mots de passe. Lorsque vous sélectionnez un groupe de ressources GSO dans la liste, ou dans l'arborescence, les champs de la vue détaillée sont automatiquement renseignés avec les données associées à la sélection courante.

Vous pouvez créer un droit d'accès unique pour toutes les ressources membres du groupe de ressources. Policy Director utilise un seul droit d'accès pour un groupe de ressources au lieu d'en affecter un séparément à chacune des ressources membres du groupe.

Onglet de tâches

Onglet de tâches : **Groupes de ressources GSO**

Tâche de gestion

Le panneau de tâches de gestion Groupes de ressources GSO contient trois vues : une liste des groupes de ressources, une vue détaillée des groupes de ressources et une liste des ressources GSO.

Boutons de commande

Les boutons de commande du panneau **Groupes de ressources GSO** sont les suivants :

- Nouveau
- Extraction
- Sauvegarde
- Suppression

Tâche de gestion LCA

Le panneau de tâches de gestion LCA permet de créer et de gérer les modèles de règle des listes de contrôle d'accès. Lorsque vous sélectionnez une LCA dans la vue **Liste des LCA**, les champs de la vue Définition de LCA sont automatiquement renseignés avec les données associées à la sélection courante.

Onglet de tâches

Onglet de tâches : **LCA**

Tâche de gestion

Le panneau de tâches de gestion LCA contient trois vues : une vue Liste des LCA, une vue détaillée Définition de LCA et une vue détaillée Entrée de LCA (avec arborescence des droits d'accès).

Boutons de commande

Les boutons de commande du panneau **LCA** sont les suivants :

- Nouvelle LCA
- Nouvelle entrée
- Sauvegarde
- Suppression
- Extraction
- Liste
- Utilisation par

Tâche de gestion Espace objets

Le panneau de tâches de gestion Espace objets permet d'associer des listes de contrôle d'accès aux objets définis dans l'espace des noms ou d'en supprimer.

Lorsque vous sélectionnez un objet dans l'arborescence de l'espace des objets, la liste des LCA dont il hérite apparaît dans la vue arborescente LCA héritées. Cette liste indique tous les objets dotés de LCA explicitement associées et ayant une incidence sur les droits d'accès de l'objet sélectionné du fait de cet héritage.

Onglet de tâches

Onglet de tâches : **Espace objets**

Tâche de gestion

Le panneau de tâches de gestion Espace objets propose trois vues que vous pouvez sélectionner à partir de sous-onglets.

- **LCA héritées** (vue par défaut)

  Cette vue est celle qui s'affiche par défaut. Elle présente la chaîne des listes de contrôle d'accès auxquelles l'objet sélectionné est soumis. Une flèche signale la LCA à l'origine du contrôle en cours dans la vue arborescente de l'espace des objets.
- **Edition LCA**

  Cette vue contient la partie du panneau de gestion des LCA qui permet de modifier directement les attributs de la liste de contrôle d'accès.
- **Héritages**

  Cette vue contient une arborescence de la chaîne d'héritages de LCA ayant une incidence directe sur l'objet sélectionné.

Boutons de commande

Les boutons de commande du panneau **Espace objets** sont les suivants :

- Attacher LCA
- Supprimer LCA
- Rechercher LCA
- Enregistrer LCA
- Liste

Tâche de gestion Utilisateur relais

Couplé à un pare-feu, Policy Director peut protéger intégralement l'intranet de l'entreprise contre les intrusions et les accès non autorisés. Le panneau de tâches de gestion Utilisateur relais permet de créer et de gérer des utilisateurs relais dans le domaine sécurisé. Lorsque vous sélectionnez un utilisateur relais dans l'arborescence, les champs de la vue détaillée sont automatiquement renseignés avec les données associées à la sélection courante.

Onglet de tâches

Onglet de tâches : **Utilisateur relais**

Tâche de gestion

Le panneau de tâches de gestion Utilisateur relais contient une liste Utilisateurs relais et une vue Données utilisateur relais.

La vue Données utilisateur relais contient des champs indiquant les caractéristiques de l'utilisateur relais par défaut.

Boutons de commande

Les boutons de commande du panneau **Utilisateur relais** sont les suivants :

- Sauvegarde
- Suppression

Propriétés et commandes de la console de gestion

La console de gestion nécessite d'installer le programme client Policy Director NetSEAT pour Microsoft Windows NT ou Windows 95 ou 98 pour exécuter les tâches de gestion avec des canaux de communication sécurisés. Pour AIX et Solaris, la console de gestion utilise le client DCE du système pour exécuter les tâches de gestion.

Prendre/déposer

Pour exécuter les opérations de la console de gestion, vous pouvez dans de nombreux cas faire glisser les objets avec la souris d'un endroit à un autre. Par exemple, pour ajouter un utilisateur à un groupe, vous pouvez faire glisser l'icône **Utilisateur** à partir de la liste des utilisateurs. Vous n'avez plus qu'à la déposer ensuite sur la vue arborescente des groupes.

Le curseur change d'aspect lorsqu'il surplombe une icône que vous pouvez faire glisser.

Vous pouvez faire glisser les objets suivants :

- Utilisateurs
- Groupes
- LCA
- Entrées de LCA
- Objets de l'espace des noms
- Ressources GSO et Groupes de ressources GSO
- Utilisateurs relais

Remarque : Tous les déplacements d'objet induisant des mises à jour de la base de données déclenchent l'affichage d'une boîte de dialogue de confirmation ou d'alerte.

La méthode prendre/déposer permet de formuler des requêtes de données. Par exemple, si vous faites glisser une icône **LCA** depuis le tableau d'informations vers la vue Définition de LCA, les données de la sélection courante s'insèrent automatiquement dans les champs correspondants.

Si vous déposez un objet (une icône) sur un emplacement n'acceptant pas cette opération, l'objet déplacé regagne automatiquement son lieu d'origine.

Remarque : Les opérations du type prendre/déposer ne fonctionnent que dans le contexte de la console de gestion.

Opérations des panneaux supérieur et inférieur

Les opérations de mise à jour réalisées à partir de la console de gestion s'opèrent dans le panneau du haut comme dans celui du bas de la fenêtre. Vous pouvez faire glisser des objets depuis le panneau inférieur vers le panneau supérieur. N'oubliez pas de sauvegarder les modifications apportées à la base de données.

Policy Director synchronise sans cesse les informations liées aux listes de contrôle d'accès affichées dans le panneau de l'espace des objets comme dans le panneau LCA.

Sélection de plusieurs éléments dans une liste

Vous pouvez sélectionner des listes et des tables à l'aide des techniques de sélection standard de Windows :

- Cliquez une fois sur un élément pour le sélectionner.
- Maintenez enfoncée la touche CTRL pour ajouter d'autres éléments à la sélection.
- Cliquez une fois puis appuyez sur la touche MAJ et cliquez à nouveau pour sélectionner le bloc de texte situé entre les deux clics.
- Pour sélectionner tous les éléments d'une liste, appuyez conjointement sur **CTRL + a**.

Edition des zones de saisie

Lorsque vous éditez une zone de saisie, n'oubliez pas les usages suivants :

- Pour activer ou désactiver une zone de saisie, appuyez sur la touche Entrée.
- Pour restaurer le contenu initial d'une zone de saisie, appuyez sur la touche Echap.
- Sur les machines hébergeant un client Windows, vous pouvez utiliser les raccourcis clavier standard de Windows pour effectuer des opérations telles que copier, couper et coller, avec la console de gestion.
- Lorsque vous quittez un champ dans lequel vous avez modifié des données, un témoin rouge apparaît dans l'angle supérieur gauche de la vue. Cliquez sur le bouton **Sauvegarde** pour valider les modifications apportées à la base de données.
- Vous pouvez renseigner certaines zones de données par une action prendre/déposer.

Requêtes sur les listes

Plusieurs des vues avec liste proposent des fonctions de requête. L'icône de requête apparaît dans l'angle supérieur gauche de la fenêtre contenant la liste.

Navigation

Pour passer d'un champ à un autre :

- Dans le cadre d'une vue détaillée, la touche de tabulation déplace le curseur d'une zone de saisie vers la suivante.
- Lorsque le curseur se trouve dans le dernier champ d'une vue détaillée, la touche de tabulation le déplace dans la vue suivante. Le curseur se déplace de gauche à droite.
- Lorsque le curseur se trouve dans une liste ou dans une arborescence, la touche de tabulation le déplace dans la vue suivante. Le curseur se déplace de gauche à droite.
- Pour déplacer le curseur de droite à gauche, appuyez sur MAJ + touche de tabulation.
- La touche Origine déplace le curseur en haut de la vue. La touche Fin le déplace en bas de la vue.

Dans une vue détaillée, lorsque tous les champs sont inactifs, les touches Origine et Fin déplacent le curseur respectivement en haut et en bas de la vue. Si un champ est actif, les mêmes touches déplacent le curseur respectivement au début et à la fin de ce champ.

Utilisation des icônes des objets

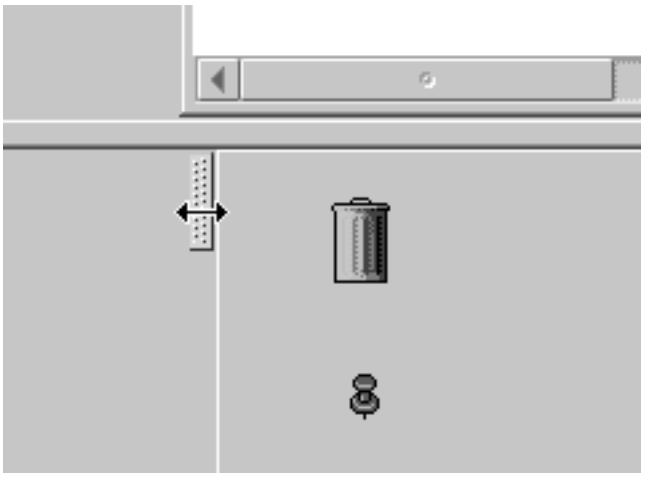
Lorsque vous utilisez les icônes des objets, n'oubliez pas les usages suivants :

- Une icône représente de manière unique chaque type d'objet dans l'espace des noms.
- Chaque onglet de tâche contient l'icône de l'objet concerné par la tâche de gestion exécutée.
- Les vues détaillées font apparaître l'icône de l'objet en cours de modification dans l'angle supérieur gauche de la vue.
- Toute opération du type prendre/déposer déclenche l'affichage de l'icône de l'objet sélectionné.
- Pour déplacer un objet, il suffit de faire glisser son icône.
- Le curseur change d'aspect lorsqu'il surplombe une icône que vous pouvez faire glisser.

Modification de la taille des vues à l'aide de l'icône de fractionnement

Chaque panneau de tâches de gestion contient une ou plusieurs vues. Pour redimensionner une de ces vues, utilisez l'icône de fractionnement située dans l'angle supérieur gauche de la vue sélectionnée. Vous pouvez également redimensionner les colonnes des listes en déplaçant le curseur sur l'icône de fractionnement entre deux titres de colonne.

Lorsque le curseur arrive sur l'icône de fractionnement, il prend l'aspect d'une double flèche, indiquant ainsi que vous pouvez redimensionner la vue.



Tri des listes

Pour trier et afficher les informations des listes par ordre croissant ou décroissant, cliquez sur la barre de titre de la colonne à trier. Une icône affichée à droite de la barre de titre indique l'ordre de tri courant.

Les éléments sélectionnés dans une liste avant un tri demeurent sélectionnés une fois le tri terminé.

Développement et réduction des vues arborescentes

Dans le contexte de la console de gestion, une vue arborescente ressemble à une fenêtre de Windows Explorer qui affiche les fichiers et les répertoires d'un système. Pour développer ou réduire un noeud, vous devez voir une icône ; une boîte contenant un signe plus ou moins. Cliquez deux fois sur cette icône pour développer ou réduire la vue arborescente, selon son mode d'affichage initial. Le raccourci clavier équivalent est **CTRL + e**.

Si un noeud n'a ni sous-objets ni sous-noeuds, l'indicateur de développement/réduction disparaît lorsque vous cliquez sur lui.

Pour régénérer l'affichage de l'arborescence, développez le noeud racine, puis réduisez-le.

Utilisation des flèches d'affichage des noeuds de l'espace des objets

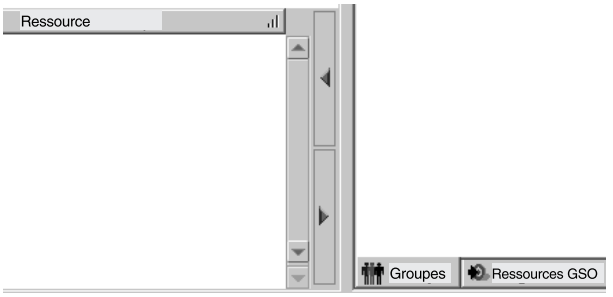
La barre de titre de la vue **Espace objets** contient deux flèches bleues. Ces deux flèches permettent de centrer la vue arborescente sur une partie de l'arborescence.

- **Flèche pointée à gauche :** Cette flèche décale le noeud ou l'objet sélectionné complètement sur la gauche pour le faire apparaître comme à la racine.
- **Flèche pointée à droite :** Cette flèche fait remonter l'arborescence affichée d'un noeud en arrière chaque fois que vous cliquez sur elle. Après avoir utilisé la flèche pointée à gauche, cliquez (une ou plusieurs fois) sur celle pointée à droite pour restaurer l'arborescence dans sa présentation normale.

Utilisation des flèches de sélection

Les flèches de sélection permettent de déplacer les informations sélectionnées de la fenêtre d'une vue vers une autre. Ceci a pour effet de renseigner automatiquement les champs de la seconde fenêtre avec les informations ainsi

importées.



Chapitre 5. Gestion des comptes des utilisateurs et des groupes

Le modèle de sécurité de Policy Director demande l'authentification de l'identité d'un utilisateur avant de lui permettre d'accéder à un objet. Pour authentifier cette identité, vous pouvez la rapprocher, avec le mot de passe associé, des données de compte contenues dans la base de données de registre primaire. Par défaut, Policy Director utilise le registre LDAP. L'administrateur de la sécurité peut utiliser la console de gestion pour créer et gérer les utilisateurs et les groupes membres du domaine sécurisé.

Ce chapitre comprend les sections suivantes :

Principes des utilisateurs, des groupes et des comptes

Le service de sécurité de Policy Director repose sur un registre primaire des comptes. Il s'agit d'une base de données contenant des informations relatives aux utilisateurs, aux groupes et aux comptes définis dans le domaine sécurisé. Par défaut, Policy Director utilise le registre LDAP.

Utilisateurs

Les utilisateurs, ou principaux, sont les membres du domaine sécurisé. Dans ce contexte, le terme d'utilisateur peut désigner une personne, un processus de serveur, une machine ou un autre domaine sécurisé.

Un utilisateur est une entité susceptible de prendre part à un échange d'authentifications avec un autre utilisateur. L'authentification est un processus qui consiste à vérifier qu'un utilisateur est bien celui qu'il prétend être. Chaque utilisateur possède un mot de passe, ou une clé secrète, qu'il utilise pour l'authentification.

Vous pouvez lier les utilisateurs à des droits d'accès. Chaque utilisateur possède aussi un identifiant unique, ou UUID (Universal Unique Identifier), qui reste invariable même si le nom de cet utilisateur vient à changer. Policy Director communique cet UUID au service de sécurité sous la forme d'un droit d'accès.

Groupes

Un groupe est un ensemble d'utilisateurs identifié par un nom de groupe. Les groupes peuvent correspondre à différents niveaux de fonction de sécurité ou de responsabilité. Policy Director traite les utilisateurs membres d'un groupe de manière identique s'agissant de la sécurité. Un utilisateur peut appartenir à plusieurs groupes, selon ses fonctions et attributions.

La création de groupes facilite la gestion des règles de sécurité que vous pouvez établir à l'aide de listes de contrôle d'accès. Lorsque le rôle, la responsabilité ou le statut d'un utilisateur est modifié, toutes les entrées des listes de contrôle d'accès qui lui sont rattachées doivent aussi changer. Sans l'existence des groupes, la

modification de toutes les listes de contrôle d'accès contenant des entrées pour cet utilisateur représenterait une tâche virtuellement impossible.

Une entrée de LCA pour un groupe permet de représenter la fonction ou la responsabilité de tous les utilisateurs membres de ce groupe. Dans ce contexte, pour modifier le statut d'un utilisateur, il suffit de l'ajouter aux membres du groupe ou de l'en supprimer.

Comme les utilisateurs, les groupes possèdent un UUID, en plus du nom de groupe. Cet UUID de groupe constitue l'un des éléments des droits d'accès des utilisateurs.

Comptes

Un compte institue une relation entre un utilisateur, le ou les groupes associés et des données de sécurité. Dans le registre, le compte définit l'identité d'un utilisateur dans le réseau en l'associant à un ou plusieurs groupes et à des données de sécurité telles que le mot de passe qu'il utilise pour l'authentification.

Vous devez créer un compte pour tout utilisateur désirant établir une communication dans le domaine sécurisé, que cette communication soit authentifiée ou non.

Vous pouvez associer un compte utilisateur avec le mot de passe de l'utilisateur et avec toutes les informations utilisées lorsqu'il accède au domaine sécurisé. Les données de compte peuvent comprendre les répertoires personnels des utilisateurs, leurs shells de connexion et les règles d'authentification qui les concernent (les mots de passe notamment). Ces informations facilitent le contrôle de l'accès au domaine sécurisé.

Remarque : Un groupe doit être ajouté au registre avant de pouvoir intégrer les données d'un compte utilisateur.

Gestion des groupes

Un groupe est un ensemble composé d'un ou plusieurs utilisateurs. Les groupes créés correspondent généralement à des services de l'entreprise (par exemple, les départements Ventes, Formation ou Ingénierie). Vous pouvez également créer des catégories de groupe en fonction des tâches dévolues (par exemple, une pour les administrateurs système et une autre pour les personnes chargées des sauvegardes périodiques).

Définir des catégories de groupe peut simplifier la gestion du contrôle d'accès dans le domaine sécurisé Policy Director. Pour permettre aux nouveaux utilisateurs d'accéder aux informations, il suffit de les faire entrer dans la catégorie de groupe appropriée. Cette approche évite de devoir créer de nouvelles entrées de LCA pour chaque nouvel utilisateur.

Par exemple, lorsqu'un nouvel employé intègre le département Ingénierie, vous pouvez créer un compte utilisateur et en faire un membre de la catégorie de groupe `Ingénierie`. Le nouvel utilisateur pourra ensuite lire tous les documents techniques accessibles aux membres du groupe `Ingénierie`. Il est inutile de créer une entrée de liste de contrôle d'accès pour cet utilisateur dans le modèle de LCA des ressources techniques.

La console de gestion permet d'ajouter, de modifier ou de supprimer des entrées de groupe dans le registre de sécurité de Policy Director.

Lorsque vous avez créé une ou plusieurs entrées de groupe, vous pouvez affecter des utilisateurs à ces groupes. Un utilisateur peut appartenir à plusieurs groupes, selon ses fonctions et responsabilités.

Utilisation du panneau de gestion Groupes

L'administrateur de la sécurité attaché au domaine sécurisé crée les groupes à l'aide de la console de gestion :

1. Connectez-vous à la console de gestion sous un ID d'administrateur tel que `cell_admin`.
2. Cliquez sur l'onglet de tâches **Groupes**.

   Le panneau de tâches de gestion Groupes apparaît.

Utilisation des boutons de commande pour les tâches de gestion des groupes

Les boutons de commande du panneau **Groupes** exécutent des opérations de gestion des groupes. Le tableau suivant décrit les tâches de chaque bouton de commande :

Bouton de commande	Description
Nouveau	Crée une entrée de groupe pour le domaine sécurisé.
Extraction	Récupère les informations liées à un groupe désigné et renseigne les champs des fenêtres des vues détaillées.
Sauvegarde	Enregistre l'entrée de groupe définie. La nouvelle entrée apparaît dans la fenêtre de la liste appropriée.
Suppression	Supprime le groupe sélectionné de la base de données du registre.

Utilisation des champs de définition des groupes

Le tableau suivant décrit les champs de la vue **Données du groupe** de la console de gestion :

Champ	Description
Nom du groupe	Nom principal affecté à un groupe du domaine sécurisé. Le champ Nom du groupe peut être utilisé comme variable pour les requêtes portant sur le registre.
Description	Chaîne de texte décrivant les caractéristiques du groupe. Le champ Description est une zone de saisie facultative et ses données ne sont pas utilisées par le registre.
LDAP	Pour LDAP : • Pour cn =, tapez un nom commun (le CN), par exemple, `crédit` • Pour dn=, tapez un nom distinctif (le DN), par exemple, `cn=crédit,o=IBM,ou=Arles,c=FR`

Création d'un groupe

Pour créer un groupe :

1. Cliquez sur le bouton de commande **Nouveau**.

Activez les zones de saisie **Nom du groupe** et **Description** dans la zone Données du groupe.

2. Tapez le nom du nouveau groupe dans le champ **Nom du groupe** et, éventuellement, entrez une description dans le champ **Description**.
3. Ajoutez les données requises dans le registre LDAP si vous utilisez ce registre par défaut.
4. Pour ajouter des utilisateurs au nouveau groupe, faites glisser leurs icônes à partir de la vue de la liste des ID vers la fenêtre ID utilisateur de la vue Données du groupe.

   Vous pouvez également utiliser les flèches de sélection pour déplacer les utilisateurs dans ou hors du panneau ID utilisateur.
5. Cliquez sur le bouton de commande **Sauvegarde**.

   Une nouvelle entrée de groupe apparaît dans la vue de la liste des groupes.

Modification des données des groupes

Pour modifier la composition ou le nom d'un groupe :

1. Sélectionnez un groupe dans la vue de la liste des groupes.

   Les propriétés du groupe s'insèrent dans les champs de la vue Données du groupe.
2. Dans la zone Données du groupe, sélectionnez le champ à modifier (reportez-vous à la section «Utilisation des champs de définition des groupes» à la page 71) et entrez-y la nouvelle valeur.
3. Vous pouvez également ajouter d'autres utilisateurs au groupe ou en supprimer.

   Dans la colonne ID utilisateur, cliquez deux fois de suite sur l'icône d'un utilisateur. Faites glisser ensuite cette icône dans la fenêtre ID utilisateur de la vue Données du groupe. Vous pouvez également utiliser les flèches de sélection.
4. Cliquez sur **Sauvegarde**.

Suppression d'un groupe

Pour supprimer un groupe :

1. Dans la vue de la liste des groupes, sélectionnez le nom du groupe à supprimer.

   La liste des membres du groupe apparaît dans la vue Données du groupe.
2. Sélectionnez chaque membre l'un après l'autre, puis supprimez-les du groupe.
3. Dans la vue de la liste des groupes, sélectionnez le groupe à supprimer.
4. Cliquez sur **Suppression** pour supprimer totalement l'entrée du groupe.

Gestion des comptes utilisateur

Les utilisateurs demandant accès aux services et aux objets du domaine sécurisé doivent se faire authentifier par Policy Director. Tout utilisateur voulant accéder au domaine sécurisé Policy Director doit posséder un compte dans le registre LDAP.

Utilisation du panneau de gestion des utilisateurs

L'administrateur de la sécurité attaché au domaine sécurisé crée les comptes utilisateur à l'aide de la console de gestion :

1. Connectez-vous à la console de gestion sous un ID d'administrateur tel que `cell_admin`.
2. Cliquez sur l'onglet de tâches **Utilisateurs**.

Le panneau de tâches de gestion Utilisateurs apparaît.

Utilisation des boutons de commande pour les tâches de gestion des utilisateurs

Les boutons de commande du panneau **Utilisateurs** exécutent des opérations de gestion des utilisateurs. Le tableau suivant décrit les tâches de chaque bouton de commande :

Bouton de commande	Description
Nouveau	Crée un compte utilisateur dans le domaine sécurisé.
Extraction	Récupère les informations liées à un utilisateur désigné et renseigne les champs des fenêtres des vues détaillées.
Sauvegarde	Enregistre le compte utilisateur créé. La nouvelle entrée apparaît dans la fenêtre de la liste appropriée.
Suppression	Supprime l'utilisateur sélectionné de la base de données du registre.

Utilisation des champs de définition des utilisateurs

Le tableau suivant décrit les champs de la vue **Données utilisateur** de la console de gestion :

Champ	Description
ID utilisateur	Nom principal affecté à un utilisateur du domaine sécurisé. Le champ ID utilisateur peut être utilisé comme variable pour les requêtes portant sur le registre.
Description	Chaîne de texte décrivant les caractéristiques de l'utilisateur. Le champ Description est une zone de saisie facultative et ses données ne sont pas utilisées par le registre.
Validation du compte	Cette case à cocher permet de contrôler la capacité de l'utilisateur à accéder ou non au domaine sécurisé. Si la case est vide, le compte n'y donne pas accès mais ses données demeurent dans le registre cependant.
Validation du mot de passe	Cette case à cocher permet d'imposer une modification du mot de passe lors de la prochaine connexion de l'utilisateur au domaine sécurisé. Si la case est vide, un message informera l'utilisateur que son mot de passe est arrivé à expiration.
Utilisateur GSO	Cette case à cocher indique que l'utilisateur peut accéder aux ressources GSO.
LDAP	Pour LDAP : • Pour cn =, tapez un nom commun (le CN), par exemple, `Diana Lucas` • Pour sn= , tapez un nom d'usage (le SN), par exemple `Lucas` • Pour dn=, tapez un nom distinctif (le DN), par exemple, `cn=Diana Lucas,o=IBM,ou=Arles,c=FR`

Ajout d'un compte utilisateur

Pour ajouter un compte utilisateur :

1. Cliquez sur le bouton de commande **Nouveau**.

   Des zones de saisie vides apparaissent dans la vue Données utilisateur.

2. Entrez les données appropriées dans chacun de ces champs. Pour plus d'informations sur ces zones de saisie, reportez-vous à la section «Utilisation des champs de définition des utilisateurs» à la page 73.

   Pour renseigner les champs de la fenêtre Membre des groupes, faites glisser les icônes d'un ou plusieurs groupes à partir de la vue arborescente Groupes, ou utilisez les flèches de sélection.
3. Ajoutez les données requises dans le registre LDAP si vous utilisez ce registre par défaut.
4. Cliquez sur **Sauvegarde**.

Modification des propriétés d'un compte utilisateur

Pour modifier les propriétés d'un compte existant :

1. Sélectionnez l'utilisateur désiré dans la liste de la vue ID utilisateur.

   La zone Données utilisateur affiche les propriétés de l'utilisateur sélectionné.
2. Dans la vue Données utilisateur, cliquez sur le champ à modifier.
3. Entrez-y les nouvelles données.
4. Cliquez sur **Sauvegarde**.

Suppression d'un compte utilisateur

Pour supprimer un compte utilisateur :

1. Sélectionnez l'utilisateur désiré dans la liste de la vue ID utilisateur.
2. Cliquez sur **Suppression**.

Création de comptes d'administrateur

Un utilisateur administratif doit être membre des groupes indiqués plus bas. S'il en est membre, il détient alors l'autorité requise pour créer, modifier ou supprimer des utilisateurs, des groupes et des organisations dans le domaine sécurisé.

- acct-admin
- subsys/dce/sec-admin
- subsys/dce/cds-admin

Lorsque vous créez un domaine sécurisé, le seul compte contenant cette combinaison de groupes est cell_admin.

Lorsqu'il atteint une certain dimension, le domaine sécurisé devient extrêmement délicat à gérer pour un seul administrateur étant considéré le nombre croissant de tâches. La gestion d'un grand domaine sécurisé implique la délégation de responsabilités administratives.

Vous pouvez créer des comptes d'administrateur supplémentaires disposant de la même capacité d'utilisation de la console de gestion en les faisant membres d'un des trois groupes indiqués plus haut. La planification et l'organisation de cette délégation d'autorité doit coïncider avec la création de ces comptes.

Importation d'informations à partir d'autres sources

Vous pouvez entrer dans le registre des données d'utilisateurs et de groupes provenant d'autres sources que la console de gestion.

Chapitre 6. Gestion des ressources GSO, des groupes de ressources et des droits d'accès des ressources

Policy Director supporte une solution de connexion unique, ou SSO (Single Sign-On), plus souple en intégrant la technologie IBM de connexion globale, ou GSO (Global Sign-On). Cette intégration s'obtient au moyen des fonctions de jonction intelligente de Policy Director. Pour une information complète sur les jonctions intelligentes, reportez-vous à la section «Chapitre 15. WebSEAL - Administration des jonctions intelligentes» à la page 189.

Lorsque le serveur WebSEAL réceptionne une requête pour une ressource localisée sur un serveur relié par jonction, il utilise le serveur GSO pour récupérer les données d'authentification associées. Le serveur GSO contient une base de données des correspondances pour chaque utilisateur enregistré, laquelle fournit les noms d'utilisateur et les mots de passe des différentes ressources et applications. Policy Director stocke les données GSO directement dans le registre LDAP d'IBM SecureWay Directory.

La combinaison de WebSEAL et de GSO produit une solution Web SSO complète qui offre en plus les avantages du chiffrement des données, de l'accessibilité avancée et de la modularité.

Reportez-vous à la section «Intégration du serveur GSO et de la solution SSO de WebSEAL» à la page 210 pour plus d'informations.

Principes des ressources GSO et des groupes de ressources GSO

La base de données du serveur GSO contient un droit d'accès de ressource spécifique à l'utilisateur qui associe une ressource GSO à un couple nom d'utilisateur/mot de passe déterminé. Ce nom d'utilisateur et ce mot de passe sont attachés à une ressource GSO destinée aux utilisateurs, par exemple, un serveur Web ou un groupe de serveurs Web.

Le serveur GSO fournit des données d'authentification au serveur WebSEAL. Lorsqu'un utilisateur veut exécuter une ressource d'application, WebSEAL demande les données d'authentification de l'utilisateur au serveur GSO. Le serveur GSO gère une base de données complète contenant des mises en correspondance entre des ressources et des données d'authentification. Le mappage des ressources d'application à des combinaisons nom d'utilisateur/mot de passe produit ce que l'on appelle les droits d'accès des ressources GSO. Ces droits d'accès ne peuvent être créés que pour les utilisateurs enregistrés.

Remarque : La ressource ou le groupe de ressources GSO doit être défini pour que l'on puisse lui appliquer un droit d'accès.

Gestion des ressources GSO

Une ressource GSO est un serveur Web. Vous pouvez nommer cette ressource Web pour l'identifier.

Utilisation du panneau de gestion Ressources GSO

Les ressources GSO demandant accès aux services et aux objets du domaine sécurisé doivent se faire authentifier par Policy Director. Toute ressource GSO voulant accéder au domaine sécurisé Policy Director doit posséder un compte dans le registre LDAP.

Utilisation des boutons de commande du panneau de gestion Ressources GSO

Les boutons de commande du panneau **Ressources GSO** permettent d'exécuter des opérations de gestion sur les ressources GSO. Le tableau suivant décrit les tâches de chaque bouton de commande :

Bouton de commande	Description
Nouveau	Crée un compte de ressource GSO dans le domaine sécurisé.
Extraction	Récupère les informations liées à une ressource GSO désignée et renseigne les champs des fenêtres des vues détaillées.
Sauvegarde	Enregistre le compte de ressource GSO créé. La nouvelle entrée apparaît dans la fenêtre de la liste appropriée.
Suppression	Supprime la ressource GSO sélectionnée de la base de données du registre.

Utilisation des champs de définition des ressources GSO

Le tableau suivant décrit les champs de la vue **Données de la ressource** de la console de gestion :

Champ	Description
Nom de la ressource	Nom affecté à une ressource GSO du domaine sécurisé. Le champ Nom de la ressource peut être utilisé comme variable pour les requêtes portant sur le registre.
Description	Chaîne de texte décrivant les caractéristiques de la ressource. Le champ Description est une zone de saisie facultative et ses données ne sont pas utilisées par le registre.

Ajout d'une ressource GSO

Pour créer une ressource GSO :

1. Cliquez sur le bouton de commande **Nouveau**.

   Des zones de saisie vides apparaissent dans la vue Données de la ressource.
2. Entrez les données appropriées dans chacun de ces champs. Pour plus d'informations sur ces zones de saisie, reportez-vous à la section «Utilisation des champs de définition des ressources GSO».

   Pour renseigner les champs de la fenêtre Membre des groupes de ressources GSO, faites glisser les icônes d'un ou plusieurs groupes de ressources à partir de la vue arborescente Groupes de ressources, ou utilisez les flèches de sélection.
3. Cliquez sur le bouton de commande **Sauvegarde**.

Création d'un droit d'accès de ressource GSO

Une fois créée la définition de la ressource, vous pouvez créer le droit d'accès associé pour un utilisateur.

Pour créer un droit d'accès de ressource :

1. Sélectionnez l'onglet **Utilisateurs**.
2. Sélectionnez le nom de l'utilisateur à attacher au droit d'accès que vous allez créer.
3. Dans la section Ressources GSO de la vue Données utilisateur, sélectionnez l'onglet **Ressources** pour afficher la liste des ressources disponibles.
4. Sélectionnez la ressource à laquelle le droit d'accès s'applique.
5. Faites glisser la ressource choisie sur le panneau Ressources de la vue Données utilisateur.

   Les valeurs de l'ID de connexion et du mot de passe du compte de l'utilisateur deviennent automatiquement celles du nouveau droit d'accès.
6. Les valeurs de ce couple ID de connexion/mot de passe peuvent être modifiées en cliquant sur le bouton **ID de connexion** ou **Mot de passe**, puis en entrant les valeurs associées à l'utilisateur.
7. Cliquez sur le bouton de commande **Sauvegarde**.

Modification des données des ressources GSO

Pour modifier les propriétés d'un compte existant :

1. Sélectionnez la ressource GSO désirée dans la vue de la liste des ressources.

   La zone Données de la ressource affiche les propriétés de la ressource sélectionnée.
2. Dans la vue Données de la ressource, cliquez sur le champ à modifier.
3. Modifiez les données existantes ou entrez-en de nouvelles.
4. Cliquez sur le bouton de commande **Sauvegarde**.

Suppression d'une ressource GSO

Pour supprimer un compte utilisateur :

1. Sélectionnez la ressource GSO désirée dans la vue de la liste des ressources.
2. Cliquez sur **Suppression**.

Gestion des groupes de ressources GSO

Un groupe de ressources est un groupe de serveurs Web utilisant tous les mêmes séries d'ID utilisateur et de mots de passe.

Utilisation du panneau de gestion Groupes de ressources GSO

L'administrateur de la sécurité attaché au domaine sécurisé crée les groupes de ressources GSO à l'aide de la console de gestion :

1. Connectez-vous à la console de gestion sous un ID d'administrateur tel que `cell_admin`.
2. Cliquez sur l'onglet de tâches **Groupes de ressources GSO**.

   Le panneau de tâches de gestion Groupes de ressources GSO apparaît.

Utilisation des boutons de commande du panneau de gestion Groupes de ressources GSO

Les boutons de commande du panneau Groupes de ressources GSO permettent d'exécuter des opérations de gestion sur les groupes de ressources GSO. Le tableau suivant décrit les tâches de chaque bouton de commande :

Bouton de commande	Description
Nouveau	Crée une entrée de groupe de ressources GSO pour le domaine sécurisé.
Extraction	Récupère les informations liées au groupe de ressources GSO désigné et renseigne les champs des fenêtres des vues détaillées.
Sauvegarde	Enregistre l'entrée de groupe de ressources GSO définie. La nouvelle entrée apparaît dans la fenêtre de la liste appropriée.
Suppression	Supprime le groupe de ressources GSO sélectionné de la base de données du registre.

Utilisation des champs de définition des groupes de ressources GSO

Le tableau suivant décrit les champs de la vue **Données du groupe de ressources** de la console de gestion :

Champ	Description
Nom du groupe de ressources	Nom principal affecté à un groupe de ressources GSO du domaine sécurisé. Le champ Nom du groupe de ressources peut être utilisé comme variable pour les requêtes portant sur le registre.
Description	Chaîne de texte décrivant les caractéristiques du groupe de ressources GSO. Le champ Description est une zone de saisie facultative et ses données ne sont pas utilisées par le registre.

Ajout d'un groupe de ressources GSO

Pour créer un groupe de ressources GSO :

1. Cliquez sur le bouton de commande **Nouveau**.

   Activez les zones de saisie **Nom du groupe de ressources** et **Description** dans la zone Données du groupe de ressources.
2. Tapez le nom du nouveau groupe de ressources dans le champ **Nom du groupe de ressources** et, éventuellement, entrez une description dans le champ **Description**.
3. Pour ajouter des ressources GSO au nouveau groupe de ressources GSO, faites glisser les icônes des ressources GSO désirées à partir de la fenêtre de la liste Ressources GSO vers la fenêtre Ressources GSO de la vue Données du groupe de ressources.

   Vous pouvez également utiliser les flèches de sélection pour déplacer les ressources dans ou hors du panneau Ressources GSO.
4. Cliquez sur le bouton de commande **Sauvegarde**.

   Une nouvelle entrée de groupe de ressources GSO apparaît dans la vue de la liste des groupes de ressources.

Création d'un droit d'accès de groupe de ressources GSO

Vous pouvez créer un droit d'accès unique pour toutes les ressources membres d'un groupe de ressources. Policy Director permet d'associer un unique droit d'accès à un groupe de ressources au lieu d'en affecter un séparément à chacune des ressources membres du groupe. Vous devez tout d'abord créer le groupe de ressources avant de créer le droit d'accès associé.

Une fois créée la définition du groupe de ressources GSO, pour créer le droit d'accès associé pour un utilisateur :

1. Sélectionnez l'onglet **Utilisateurs**, puis choisissez l'utilisateur à attacher au droit d'accès que vous allez créer.
2. Dans la vue Données utilisateur, sélectionnez l'onglet **Groupes de ressources** pour afficher la liste des groupes de ressources existants.
3. Sélectionnez le groupe de ressources auquel le droit d'accès s'applique.
4. Faites glisser le groupe de ressources choisi sur le panneau Groupe de ressources de la vue Données utilisateur.

   Les valeurs de l'ID de connexion et du mot de passe du compte de l'utilisateur deviennent automatiquement celles du nouveau droit d'accès.
5. Les valeurs de ce couple ID de connexion/mot de passe peuvent être modifiées en cliquant sur le bouton **ID de connexion** ou **Mot de passe**, puis en entrant les valeurs associées à l'utilisateur.
6. Cliquez sur le bouton de commande **Sauvegarde**.

Modification des données d'un groupe de ressources GSO

Pour modifier la composition ou le nom d'un groupe de ressources :

1. Sélectionnez un groupe de ressources dans la vue de la liste des groupes de ressources.

   Les propriétés du groupe de ressources choisi s'insèrent dans les champs de la vue Données du groupe de ressources.
2. Dans la zone Données du groupe de ressources, sélectionnez le champ à modifier (au choix **Nom du groupe de ressources** ou **Description**). Entrez les nouvelles valeurs.
3. Vous pouvez également ajouter d'autres ressources au groupe de ressources ou en supprimer.

   Dans la colonne Groupes de ressources, cliquez deux fois de suite sur l'icône d'un groupe de ressources. Faites glisser ensuite cette icône dans la fenêtre Ressources GSO de la vue Données du groupe de ressources. Vous pouvez également utiliser les flèches de sélection.
4. Cliquez sur le bouton de commande **Sauvegarde**.

Suppression d'un groupe de ressources GSO

Pour supprimer un groupe de ressources GSO :

1. Dans la vue de la liste des groupes de ressources, sélectionnez le nom du groupe de ressources GSO à supprimer.

   La liste des membres du groupe de ressources GSO apparaît dans la vue Données du groupe de ressources.
2. Sélectionnez une par une chaque ressource GSO, puis supprimez-la du groupe de ressources GSO.
3. Dans la vue de la liste des groupes de ressources GSO, sélectionnez le groupe de ressources GSO à supprimer.
4. Cliquez sur **Suppression** pour supprimer totalement l'entrée du groupe de ressources GSO.

Migration des données GSO

Si vous détenez des données GSO issues du produit IBM SecureWay Global Sign-on version 2.0.200, ou de versions antérieures, vous devrez migrer ces données pour les utiliser avec la version actuelle de Policy Director.

Les derniers outils et informations disponibles (notamment des utilitaires de migration) sont accessibles sur le site WEB d'IBM SecureWay Policy Director à l'adresse :

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

Modification du mot de passe d'un droit d'accès de ressource GSO

L'utilisateur peut mettre à jour le mot de passe d'une ressource GSO ou d'un groupe de ressources GSO à l'aide de l'utilitaire de gestion des mots de passe Web de Policy Director chpwd.exe. Vous ne pouvez utiliser cet outil qu'une fois le droit d'accès de ressource créé. Vous pouvez utiliser cet outil après la première modification du mot de passe.

Ce fichier se trouve dans le répertoire :

UNIX : `/opt/intraverse/www/docs/cgi-bin/chpwd`

Windows : `c:\Program Files\www\docs\cgi-bin\chpwd.exe`

Pour modifier le mot de passe du droit d'accès de ressource GSO à l'aide de l'utilitaire Web chpwd.exe :

1. Ouvrez une instance du navigateur sécurisé.
2. Entrez l'adresse URL suivante :

   `https: //`*`serveur WebSEAL`*`/cgi-bin/chpwd.exe`

   La variable serveur WebSEAL indique le nom attribué à votre serveur WebSEAL. Pour Windows, vous devez taper l'extension .exe à la fin de l'adresse URL.
3. Cliquez sur le nom de la ressource dans la colonne Nom de ressource, pour la sélectionner.
4. Tapez votre nom d'utilisateur dans le champ **ID utilisateur**.
5. Tapez votre nouveau mot de passe dans le champ **Nouveau mot de passe**. Pour le confirmer, tapez-le à nouveau dans le champ **Confirmation du nouveau mot de passe**.
6. Cliquez sur **Mise à jour**.

Chapitre 7. Principes du contrôle d'accès

Les ressources d'un domaine sécurisé peuvent être protégées. Pour cela, vous devez définir des règles spécifiques, puis les attacher ensuite aux objets représentant ces ressources. Ces règles spéciales sont appelées des modèles de règle. Policy Director reconnaît et utilise un type de modèle de règle appelé liste de contrôle d'accès (LCA). Les listes de contrôle d'accès permettent d'attacher les règles de sécurité de l'entreprise aux ressources affectées au domaine sécurisé.

Ce chapitre comprend les sections suivantes :

Espace des noms d'objet protégé

Le modèle de sécurité de Policy Director repose sur des règles, ou droits d'accès, pour protéger les ressource affectées au domaine sécurisé. Chaque série de droits d'accès constitue ce que l'on appelle un modèle de règle.

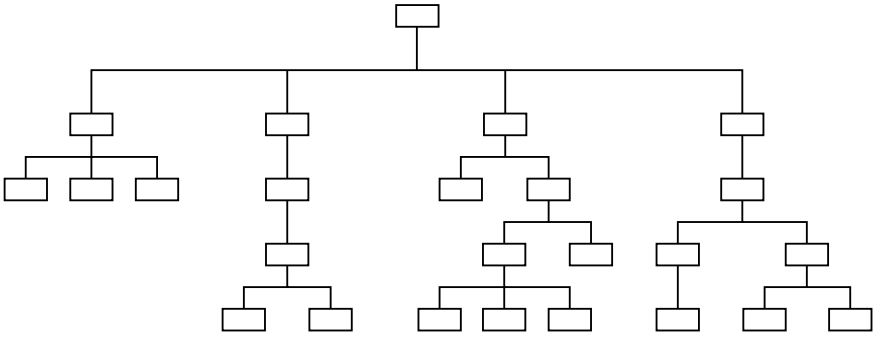
Une fois affecté à une ressource, le modèle de règle lui applique les règles de sécurité définies par l'entreprise. Pour créer ce modèle de sécurité, Policy Director utilise une représentation logique par objet de l'inventaire des ressources physiques du domaine sécurisé.

Pour protéger les véritables ressources physiques, vous devez attacher les modèles de règle aux objets logiques crées dans l'espace des noms. Le service d'autorisation de Policy Director décide d'accorder les autorisations après comparaison des droits d'accès de l'utilisateur, obtenus au cours de l'authentification, avec les autorisations définies dans les modèles.

L'espace des noms d'objet protégé de Policy Director est une représentation logique et hiérarchique des ressources d'un domaine sécurisé. Les objets apparaissant dans un espace des noms hiérarchisé représente les ressources physiques du réseau.

Ressource système
: Fichier physique, service de réseau ou application.

Objet protégé
: Représentation d'une ressource système utilisée par le service d'autorisation de Policy Director, la console de gestion et les autres utilitaires de gestion de Policy Director.



L'espace des noms d'objet protégé implique deux types d'objet :

Objets conteneurs
Les objets de type conteneur sont des désignations structurelles qui permettent d'organiser l'espace des noms de manière hiérarchique en plusieurs régions fonctionnelles. Les objets conteneurs peuvent contenir des objets de ressource.

Objets ressources
Les objets de ressource sont des représentations des véritables ressources de réseau (services, fichiers, programmes, etc.) affectées au domaine sécurisé.

Hiérarchie de l'espace des noms d'objet protégé

Le sommet structurel de l'espace des noms d'objet protégé est l'objet conteneur **racine**. Dans la console de gestion de Policy Director, le symbole de la racine est la barre oblique (/).

Les catégories d'espace des noms suivantes sont placées, du point de vue hiérarchique, sous l'objet racine :

Objets Web (conteneur /WebSEAL)
L'objet conteneur WebSEAL est la racine de l'espace Web logique du domaine sécurisé. Policy Director autorise toutes les requêtes HTTP portant sur les objets de cette sous-arborescence.

Les objets Web correspondent à toute entité pouvant être liée à une adresse URL (pages Web statiques, URL dynamiques, etc.). Les passerelles entre le Web et les applications peuvent convertir les pages Web statiques et les URL dynamiques en requêtes de base de données ou en un autre type d'appel d'application.

Objets applications de réseau (conteneur /NetSEAL)
L'objet conteneur NetSEAL est la racine de l'espace logique qui contient les services du domaine sécurisé protégés par NetSEAL. Ces objets représentent des applications TCP (telles que TELNET et FTP) qui se rattachent aux adresses de réseau TCP (les ports). L'application utilise ces ports.

Objets de gestion Policy Director (conteneur /Management)
L'objet conteneur Management (gestion) est la racine de l'espace logique qui contrôle toutes les opérations de gestion de Policy Director. Les objets de gestion représentent les services qui permettent de définir les utilisateurs et les règles de sécurité. Ces tâches s'effectuent au moyen de la console de gestion de Policy Director ou de l'utilitaire **ivadmin**.

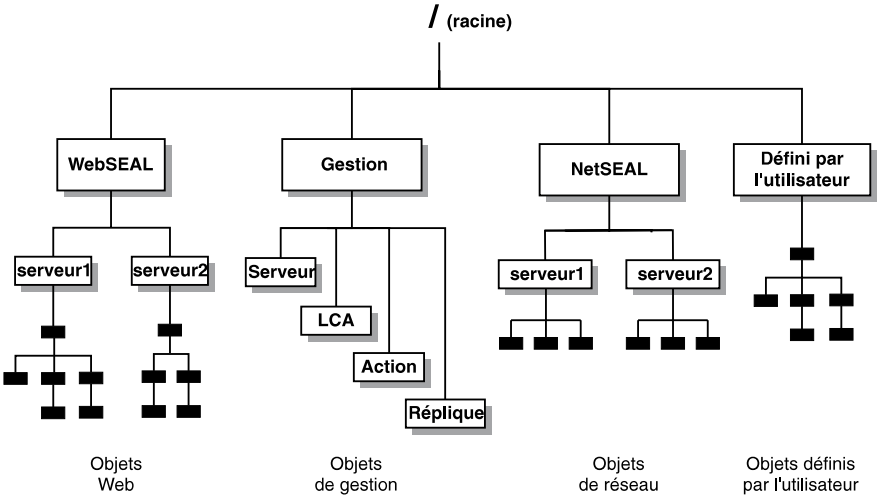
Les subdivisions de cette région comprennent :

- les tâches de gestion de serveurs (/Server) ;
- les tâches liées aux règles de sécurité (/ACL) ;
- le contrôle d'autorisation tiers (/Action) ;
- le contrôle de duplication de la base de données des autorisations (/Replica).

Policy Director permet de déléguer les activités de gestion et de limiter le droit d'un administrateur à créer des règles de sécurité à une partie définie de l'espace des noms.

Objets définis par l'utilisateur

Ces objets représentent les tâches ou les ressources de réseau protégées par des applications tiers utilisant le service d'autorisation de Policy Director (qui utilise pour sa part l'API d'autorisation).



Espaces des noms des applications tiers

Policy Director peut fournir des services d'autorisation à n'importe quel objet d'application défini par l'espace des noms d'objet protégé. Les applications de la famille des produits Policy Director comprennent WebSEAL (pour les applications Web) et NetSEAL (pour les applications TCP).

Policy Director et les applications tiers appellent le service d'autorisation de Policy Director par le biais de l'API d'autorisation de Policy Director. Pour intégrer une application tiers au service d'autorisation de Policy Director, procédez de la manière suivante :

1. Définissez l'espace des noms de l'application tiers.
2. Appliquez les droits d'accès appropriés aux objets de l'espace des noms demandant une protection.

Le cas échéant, vous pouvez aussi créer des objets conteneurs définis par l'utilisateur ; des régions de l'espace des noms d'objet protégé dans lesquelles vous pouvez créer des espaces de noms pour les applications tiers.

Dans l'espace des noms d'objet protégé, vous devez définir la racine (le point de jonction) sur laquelle commence cet espace des noms des applications tiers. Pour plus d'informations, reportez-vous à la section «Définition d'espaces de noms d'application tiers» à la page 133.

Vous devez ensuite utiliser la console de gestion ou l'utilitaire **ivadmin** pour créer et attacher des listes de contrôle d'accès aux objets de ce nouvel espace des noms, ou en supprimer.

Listes de contrôle d'accès

Une liste de contrôle d'accès (LCA) est un type de modèle de règle qu'utilise Policy Director pour protéger les ressources du domaine sécurisé.

Une liste de contrôle d'accès est une série de règles, ou d'autorisations, qui spécifient les conditions requises pour exécuter une opération sur une ressource protégée. Les listes de contrôle d'accès identifient les opérations autorisées sur les ressources protégées et répertorient les identités de ceux (utilisateurs, groupes, ou les deux) qui sont autorisés à les exécuter. Ceci concerne notamment les tâches suivantes :

- Définition des identités des utilisateurs et des groupes dans le registre de sécurité.
- Définition de l'espace des noms d'objet protégé et des modèles de règle dans la base de données des règles d'autorisation.

Comme n'importe quel modèle de règle, chaque liste de contrôle d'accès Policy Director possède un nom unique, ou étiquette, qui évoque les règles de sécurité qu'elle incarne. Vous devez appliquer les listes de contrôle d'accès aux objets représentant les ressources dans l'espace des noms d'objet protégé.

Une liste de contrôle d'accès se compose d'une ou de plusieurs entrées désignant des utilisateurs et des groupes ainsi que les autorisations dont ils disposent.

Entrées de liste de contrôle d'accès

Une liste de contrôle d'accès se compose d'une ou de plusieurs entrées désignant :

- les UUID des utilisateurs et des groupes dont l'accès aux objet est explicitement contrôlé ;
- les opérations autorisées pour chaque utilisateur, groupe ou fonction ;
- les opérations autorisées pour les catégories d'utilisateur spéciales “any” et “unauthenticated”.

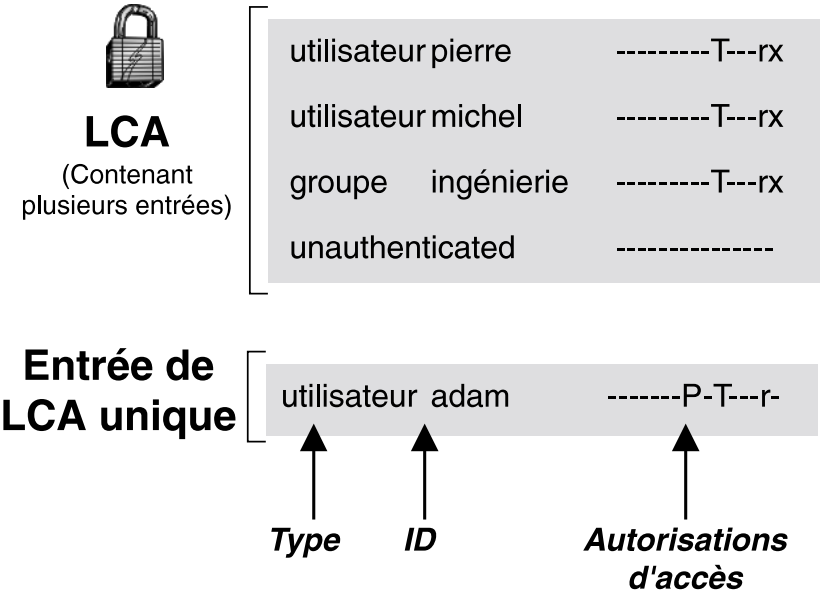
Le terme utilisateur, ou principal, désigne une identité authentifiée par le serveur de sécurité de Policy Director. Généralement, les utilisateurs sont des utilisateurs de réseau ou des serveurs d'applications.

Un groupe est un ensemble composé d'un ou plusieurs utilisateurs. L'administrateur de réseau peut utiliser des entrées de liste de contrôle d'accès de groupe pour affecter les mêmes droits d'accès à plusieurs utilisateurs. Les nouveaux utilisateurs obtiennent accès aux différents objets en devenant membres des groupes correspondants. Cette approche évite de devoir créer de nouvelles entrées de LCA pour chaque nouvel utilisateur. Les groupes définis dans le domaine sécurisé

peuvent refléter les divisions ou les services existant dans l'organisation de l'entreprise. Ils peuvent également servir pour la définition de rôles ou d'associations fonctionnelles.

Les utilisateurs et les groupes sont collectivement désignés sous le terme d'entités.

Les entrées des listes de contrôle d'accès peuvent être créées, modifiées ou supprimée à l'aide de la console de gestion de Policy Director (onglet de gestion **LCA**).



Listes de contrôle d'accès (modèles de règle)

La console de gestion permet de :

- créer une liste de contrôle d'accès ;
- enregistrer une LCA avec un étiquette ;
- appliquer une LCA à des objets de l'espace des noms.

Une fois définie, la liste de contrôle d'accès devient un modèle source ; elles est reproductible et modulable comme une formule ou une recette. La LCA contient les entrées qui assurent un niveau de protection adapté à tout objet auquel elle s'applique.

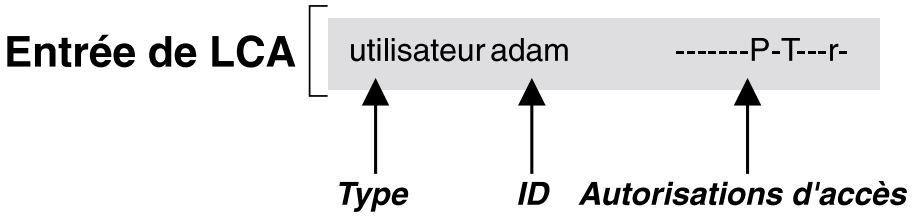
Voici un exemple de liste de LCA :

```
Nom de la LCA
default-management
default-netseal
default-replica
default-root
default-webseal
```

Un modèle de LCA prodigue les mêmes avantages qu'un style de mise en forme pour un document de traitement de texte. Si les règles de sécurité viennent à changer, il suffit de modifier la liste de contrôle d'accès. Policy Director répercute instantanément la nouvelle définition des règles de sécurité sur tous les objets auxquels la liste de contrôle d'accès s'applique.

Syntaxe des entrées de LCA

Une entrée de LCA contient deux ou trois attributs, selon son type, et se présente sous le format suivant :



Type La catégorie d'entité (utilisateur ou groupe) pour laquelle la liste de contrôle d'accès a été créée.

ID (identité) Identificateur (nom) unique de l'entité.

Les entrées de LCA de type any-authenticated (authentifié par une méthode quelconque) ou unauthenticated (non authentifié) ne demandent pas l'attribut ID.

Autorisations Série d'opérations autorisées sur l'objet pour cet utilisateur ou ce groupe.

La plupart des autorisations déterminent la capacité du client à réaliser une opération donnée sur la ressource. Toutefois, certaines autorisations imposent des conditions lorsqu'une action sur une ressource est autorisée. Ces conditions peuvent imposer, par exemple, le chiffrement des données, la protection de leur intégrité, l'enregistrement d'un état par le service d'audit, ou l'obtention d'une autorisation externe.

Dans cet exemple, l'utilisateur Adam (type=user, ID=adam) a l'autorisation de lire (afficher) l'objet associé à la liste de contrôle d'accès contenant cette entrée. Le droit de lecture (r pour read) permet cette opération. Le droit de chiffrement (P) oblige les canaux de communication à utiliser le chiffrement des données. Le droit de traversée (T) valide l'attribut de traversée.

Attribut de type

Le type indiqué dans une entrée de LCA désigne la catégorie d'entité quelle concerne. Il existe quatre types d'entité :

Type	Description

user (utilisateur)	Définit les autorisations d'un utilisateur dans le domaine sécurisé. Le type d'entrée user nécessite de spécifier un nom de compte (un ID). Le format de saisie est : `user ID autorisations`. Par exemple :
	`user`
	`gilles  -------------r-`

group (groupe)	Définit les autorisations des membres d'un groupe dans le domaine sécurisé. Le type d'entrée group nécessite de spécifier un nom de groupe (un ID). Le format de saisie est : `group ID autorisations`. Par exemple : `group ingénierie -------------r-`
any-authenticated	Définit les autorisations de tous les utilisateurs authentifiés (quelque soit la méthode). Spécifier l'ID de l'utilisateur n'est pas demandé. Le format de saisie est : `any-authenticated -------------r-`

unauthenticated	Définit les autorisations des utilisateurs non authentifiés par le serveur de sécurité. Spécifier l'ID de l'utilisateur n'est pas demandé. Le format de saisie est : `unauthenticated autorisations`. Par exemple :
	`unauthenticated ---------T---r-`
	
	Cette entrée de LCA est un masque (une opération avec opérateur "et") appliqué à l'entrée de LCA any-authenticated lors de la détermination du jeu d'autorisations. Par exemple, l'entrée de LCA unauthenticated suivante :
	`unauthenticated -------------r-`
	
	associée à cette entrée de LCA any-authenticated :
	`any-authenticated ---------T---r-`
	
	produit les autorisations suivantes :
	`-------------r-`
	`(lecture uniquement)`

Attribut ID

L'ID indiqué dans une entrée de LCA est l'identifiant unique, ou le nom, qui désigne l'utilisateur ou le groupe, respectivement pour le type user et group. Les ID doivent désigner des utilisateurs ou des groupes correctement définis dans le domaine sécurisé et enregistrés dans la base de données du registre.

Voici quelques exemples d'identifiant unique :

```
user michel
user gilles
group ingénierie
group documentation
group comptabilité
```

Remarque : N'utilisez pas l'attribut ID pour les types any-authenticated et unauthenticated.

Attributs des autorisations

Chaque entrée de la liste de contrôle d'accès contient une série d'autorisations définissant :

- les opérations que l'utilisateur ou le groupe peut réaliser sur l'objet ;
- les restrictions sur le type d'accès à l'objet, par exemple :
  - utilisation obligatoire de la confidentialité sur les canaux de communication ;
  - accès avec enregistrement d'un rapport d'audit ;
  - demande d'une autorisation externe (tiers).

Les listes de contrôle d'accès protègent les ressources sécurisées, notamment :

- la capacité de l'utilisateur à réaliser des opérations sur l'objet protégé ;
- la capacité de l'administrateur à modifier les règles du contrôle d'accès sur les objets et les sous-objet éventuels ;
- la capacité du serveur Policy Director à accorder des droits d'accès aux utilisateurs.

Ordre des autorisations

Les autorisations définies par les listes de contrôle d'accès sont réactives au contexte. En clair, ceci signifie que l'effet de certaines autorisations peut varier selon la région de l'espace des objets protégés où elle s'applique. Par exemple, l'autorisation m (modifier) a une portée différente selon qu'il s'agisse d'un objet WebSEAL ou d'un objet de gestion.

Les dix-sept autorisations standard se décomposent en quatre catégories et apparaissent dans l'ordre suivant dans une entrée de liste de contrôle d'accès :

Base	Générique	NetSEAL	WebSEAL
a A b c g I P T	d m s v	C p	l r x

La fenêtre de définition et saisie des listes de contrôle d'accès contient la liste des autorisations que vous pouvez choisir. Sélectionnez les cases à cocher situées à côté des autorisations désirées pour les choisir :

Base
  (a) Attach (attachement)
  (A) Audit (audit)
  (b) Browse (navigation)
  (c) Control (contrôle)
  (g) Delegation (délégation)
  (I) Integrity (intégrité)
  (P) Privacy (confidentialité)
  (T) Traverse (traversée)
Générique
  (d) Delete (suppression)
  (m) Modify (modification)
  (s) Server Admin (administration de serveur)
  (v) View (affichage)
NetSEAL
  (C) Connect (connexion)
  (p) Proxy (relais)
WebSEAL
  (l) List Directory (liste)
  (r) Read (lecture)
  (x) Execute (exécution)

Régions de l'espace des noms

Les objets conteneurs représentent des régions de l'espace des noms d'objet protégé et remplissent les fonctions de sécurité suivantes :

1. Vous pouvez utiliser la liste de contrôle d'accès de l'objet conteneur pour définir des règles de haute sécurité pour tous les sous-objets contenus dans la région, en l'absence d'autres listes de contrôle d'accès explicitement appliquées.
2. Vous pouvez instantanément interdire l'accès à tous les objets d'une région en supprimant le droit de traversée de la liste de contrôle d'accès de l'objet conteneur.

Droit de traversée

Le droit de traversée (traverse) est une autorisation générique qui s'applique dans l'ensemble de l'espace des noms d'objet protégé.

Droit de traversée :	Accès	Description
T	traversée	Permet à l'utilisateur de franchir le niveau hiérarchique de l'objet et de circuler dans la hiérarchie des objets pour atteindre celui qu'il demande. Cette autorisation ne donne pas d'autres types d'accès à l'objet franchi. Le droit de traversée est également requis pour l'objet demandé lui-même.

Conditions d'accès

Les conditions d'accès sont des autorisations génériques qui s'appliquent dans l'ensemble de l'espace des noms d'objet protégé.

Conditions d'accès pour tous les objets protégés :	Accès	Description
A	audit	Demande au serveur Policy Director d'enregistrer un rapport d'audit lors de chaque accès à l'objet. Toutes les tentatives d'accès sont consignées même si elles échouent.
I	intégrité	La protection de l'intégrité des données entre le client et le serveur Policy Director est indispensable pour accéder à cet objet.
P	confidentialité	Le chiffrement des données entre le client et le serveur Policy Director est indispensable pour accéder à cet objet.

Droit de contrôle

Le droit de contrôle est une autorisation importante qui confère la propriété de la liste de contrôle d'accès. Ce droit de contrôle donne la possibilité de modifier les entrées de la LCA, d'en créer, d'en supprimer, mais aussi d'accorder des autorisations ou d'en retirer.

Droit de contrôle :	Accès	Description
c	contrôle	Confère la propriété de la LCA ; permet de créer, supprimer et modifier ses entrées.

L'administrateur peut supprimer une liste de contrôle d'accès de la liste des modèles de LCA. L'administrateur doit être désigné dans une entrée de cette liste de contrôle d'accès pour la supprimer. Cette entrée doit également lui accorder le droit de contrôle.

Le droit de contrôle permet à son détenteur d'attribuer des droits d'administrateur à un autre utilisateur. Par exemple, vous pouvez ainsi attribuer le droit d'attacher une liste de contrôle d'accès à des objets. Cette dernière opération nécessite le droit d'attachement (a).

Dans la mesure où il confère la propriété de la LCA, il convient d'utiliser le droit de contrôle (c) avec prudence.

Objet conteneur racine

L'objet conteneur racine appelle les remarques suivantes s'agissant de la sécurité :

- L'objet racine est au sommet de la chaîne d'héritages des LCA pour l'ensemble de l'espace des noms d'objet protégé.
- Si vous n'appliquez aucune autre liste de contrôle d'accès, de manière explicite, l'objet racine détermine (par le jeu des héritages) les règles de sécurité applicables à l'ensemble de l'espace des noms.
- Pour accéder aux objets hiérarchiquement placés sous la racine, vous devez détenir le droit de traversée (T).

Région WebSEAL de l'espace des noms

L'objet conteneur /WebSEAL appelle les remarques suivantes s'agissant de la sécurité :

- L'objet WebSEAL est au sommet de la chaîne d'héritages des LCA pour la région WebSEAL de l'espace des noms.
- Si vous n'appliquez aucune autre liste de contrôle d'accès, de manière explicite, cet objet détermine (par le jeu des héritages) les règles de sécurité applicables à l'ensemble de l'espace Web.
- Pour accéder à cet objet et aux objets hiérarchiquement placés sous lui, vous devez détenir le droit de traversée (T).

/WebSEAL/host

Cette sous-arborescence contient l'espace Web d'un serveur WebSEAL Policy Director déterminé. Cet objet appelle les remarques suivantes s'agissant de la sécurité :

- Pour accéder aux objets hiérarchiquement placés sous cet objet, vous devez détenir le droit de traversée (T).
- Si vous n'appliquez aucune autre liste de contrôle d'accès, de manière explicite, cet objet détermine (par le jeu des héritages) les règles de sécurité applicables à l'ensemble de l'espace des noms du système.

/WebSEAL/host/file

Cette sous-arborescence correspond à l'objet ressource contrôlé pour l'accès HTTP. Les autorisations vérifiées dépendent de l'opération demandée.

Autorisations WebSEAL

Le tableau suivant décrit les autorisations applicables à la région WebSEAL de l'espace des noms :

Autorisations WebSEAL de l'espace des noms :	Accès	Description
r	lecture	Permet d'afficher l'objet HTTP.
x	exécution	Permet d'exécuter le programme CGI.
d	suppression	Permet de supprimer l'objet HTTP.
m	modification	Permet d'éditer (commande PUT) un objet HTTP dans la région WebSEAL de l'espace des noms.
l	liste	Permet d'afficher automatiquement le contenu d'un répertoire HTTP.
g	délégation	Permet de sécuriser un serveur WebSEAL pour le compte d'un client. Ce serveur agira pour le client et transmettra ses requêtes à un autre serveur WebSEAL lié au réseau via une jonction.

Région NetSEAL de l'espace des noms

L'objet /NetSEAL appelle les remarques suivantes s'agissant de la sécurité :

- L'objet NetSEAL est au sommet de la chaîne d'héritages des LCA pour la région NetSEAL de l'espace des noms.
- Si vous n'appliquez aucune autre liste de contrôle d'accès, de manière explicite, cet objet détermine (par le jeu des héritages) les règles de sécurité applicables à l'ensemble des services protégés par NetSEAL dans l'espace des noms.
- Pour accéder à cet objet et aux objets hiérarchiquement placés sous lui, vous devez détenir le droit de traversée (T).

/NetSEAL/host

Cette sous-arborescence contient tous les services protégés par NetSEAL sur la machine du serveur. Cet objet appelle les remarques suivantes s'agissant de la sécurité :

- Pour accéder aux ressources hiérarchiquement placées sous cet objet, vous devez détenir le droit de traversée (T).
- Si vous n'appliquez aucune autre liste de contrôle d'accès, de manière explicite, cet objet détermine (par le jeu des héritages) les règles de sécurité applicables à l'ensemble des services protégés par NetSEAL sur cette machine.

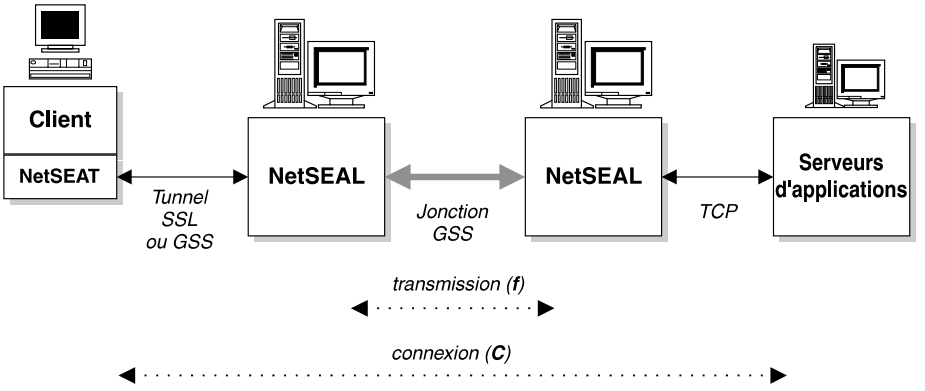
/NetSEAL/host/service

Cette sous-arborescence correspond à l'objet contrôlé pour l'accès au service protégé qu'il incarne. Les autorisations vérifiées dépendent de l'opération demandée.

Autorisations NetSEAL

Le tableau suivant décrit les autorisations applicables à la région NetSEAL de l'espace des noms :

Autorisations des objets protégés par NetSEAL :	Accès	Description
C	connexion	Permet de se connecter à un serveur NetSEAL.
f	transmission	Permet d'établir des connexions sortantes via une jonction NetSEAL (de franchir la jonction).



Région Management (gestion) de l'espace des noms

L'objet /Management appelle les remarques suivantes s'agissant de la sécurité :

- L'objet Management est au sommet de la chaîne d'héritages des LCA pour la région Management de l'espace des noms.
- Si vous n'appliquez aucune autre liste de contrôle d'accès, de manière explicite, cet objet détermine (par le jeu des héritages) les règles de sécurité applicables à l'ensemble de la région Management de l'espace des noms.
- Pour accéder à cet objet, vous devez détenir le droit de traversée (T).

/Management/server

L'objet conteneur /Management/server de l'espace des noms d'objet protégé de Policy Director permet à l'administrateur d'exécuter les tâches de gestion des serveurs (à condition d'avoir les autres autorisations requises).

Les contrôles de gestion des serveurs permettent de déterminer si un utilisateur a le droit de créer, modifier ou supprimer des définitions de serveur. Ces définitions contiennent des informations qui permettent aux serveurs Policy Director, en particulier le serveur de gestion ivmgrd, de localiser ces serveurs et de communiquer avec eux.

Vous pouvez créer une définition de serveur pour un gestionnaire de sécurité particulier (secmgrd) ou un serveur d'autorisations (ivacld) pendant la procédure d'installation. De plus, lorsque vous désinstallez un serveur, Policy Director supprime automatiquement sa définition.

La création et la suppression de la définition interviennent automatiquement ; l'administrateur d'installation n'a aucune action à entreprendre dans un cas comme dans l'autre. En revanche, l'administrateur doit détenir le droit de modification (m) sur l'objet /Management/Server pour pouvoir créer les définitions au cours de l'installation.

De même, il doit aussi détenir le droit de suppression (d) sur l'objet /Management/Server pour pouvoir supprimer ces définitions pendant la désinstallation.

Les autres opérations pouvant être conduites sur une définition de serveur sont notamment les suivantes :

- Afficher les définitions au moyen de l'utilitaire **ivadmin**. L'utilisateur doit détenir le droit d'affichage (v) sur l'objet serveur.

- Exécuter des opérations de gestion de serveur, comme initialiser, arrêter, suspendre et relancer les serveurs ou effacer les fichiers journaux. L'utilisateur doit détenir le droit d'administration de serveur (s) sur l'objet serveur.
- Modifier des sections d'une définition au moyen de la commande **ivadmin server modify**. L'utilisateur doit détenir le droit de modification (m) sur l'objet serveur.

Autorisations de gestion de serveur :	Accès	Description
s	serveur	Permet d'exécuter des tâches de gestion de serveur (initialiser, arrêter, suspendre, relancer les serveurs, etc.).
v	affichage	Permet d'afficher la liste des serveurs.
m	modification	Permet de créer une nouvelle définition de serveur.
d	suppression	Permet de supprimer une définition de serveur.

/Management/ACL

Cet objet permet aux administrateurs d'exécuter des tâches de gestion de liste de contrôle d'accès susceptibles d'affecter les règles de sécurité du domaine sécurisé.

Autorisations de gestion des LCA :	Accès	Description
b	navigation	Permet de visualiser le contenu de l'espace des noms hiérarchiquement placé sous l'objet.
a	attachement	Permet d'attacher des modèles de liste de contrôle d'accès aux objets ou de les retirer.
m	modification	Permet de créer un modèle de LCA.
d	suppression	Permet de supprimer un modèle de liste de contrôle d'accès. La LCA doit contenir une entrée donnant le droit de contrôle (c) au même utilisateur.
v	affichage	Permet d'afficher le contenu d'une LCA.

Vous devez définir les administrateurs de LCA dans l'objet de gestion des LCA par défaut. L'entrée de LCA de l'administrateur peut contenir n'importe laquelle des autorisations détaillées plus haut. Ces autorisations donnent à l'administrateur le droit de créer et de supprimer des modèles de liste de contrôle d'accès, et d'attacher les LCA aux objets.

Un administrateur de listes de contrôle d'accès ne peut pas modifier une LCA existante sauf si celle-ci contient une entrée lui donnant le droit de contrôle (c). Seul le propriétaire d'une liste de contrôle d'accès peut modifier ses entrées.

Notez que la première entrée d'une liste de contrôle contient obligatoirement le nom de son créateur, les autorisations abcT lui étant attribuées d'office.

Par exemple, si l'utilisateur `cell_admin` figure dans une entrée de la LCA de gestion par défaut, avec le droit de modification (m), cet utilisateur peut créer un nouveau modèle de LCA. L'utilisateur cell_admin figurera dans la première entrée de cette nouvelle LCA, avec les autorisations abcT. Le droit de contrôle (c) donne à cell_admin la propriété de la liste de contrôle d'accès et lui permet de la modifier. L'utilisateur cell_admin peut ensuite attribuer des droits administratifs à d'autres utilisateurs par le biais d'entrées adaptées dans la liste de contrôle d'accès.

Par défaut, la propriété de la LCA de gestion par défaut est attribuée à l'utilisateur `cell-admin` et au groupe `iv-admin`.

/Management/action

Cet objet permet aux administrateurs d'exécuter des tâches de gestion de LCA dans un espace des noms tiers. Les tâches et les autorisations concernées comprennent :

Autorisations de gestion des tâches (autorisation tiers) :	Accès	Description
m	modification	Permet de créer une nouvelle tâche.
d	suppression	Permet de supprimer une tâche.

Policy Director fournit des services d'autorisation aux applications. Les applications de la famille des produits Policy Director comprennent WebSEAL (pour les applications Web) et NetSEAL (pour les applications TCP).

Les applications tiers peuvent appeler le service d'autorisation de Policy Director par le biais de l'API d'autorisation de Policy Director. Deux actions sont nécessaires pour intégrer une application tiers au service d'autorisation de Policy Director :

- Définir l'espace des noms de l'application ;
- Appliquer les autorisations aux objets (ressources) demandant une protection.

L'administrateur de l'espace des noms d'une application tiers peut utiliser l'utilitaire **ivadmin** pour définir de nouvelles autorisations et actions. L'administrateur doit détenir les droits de gestion et d'action pour créer et supprimer ces autorisations et ces actions.

/Management/replica

L'objet conteneur /Management/Replica de l'espace des noms d'objet protégé de Policy Director contrôle la duplication de la base de données des autorisations. Les contrôles haut niveau sur cet objet ont une incidence sur le fonctionnement des gestionnaires de sécurité et du serveur de gestion dans le domaine sécurisé.

Les contrôles de gestion de la duplication permettent de déterminer quels processus sont autorisés à lire ou à mettre à jour la base de données primaire des règles d'autorisation pour que la duplication se fasse comme il se doit.

Les contrôle et les autorisations concernés comprennent :

Autorisations de gestion de la duplication :	Accès	Description
v	affichage	Permet de lire la base de données primaire des autorisations.
m	modification	Permet de modifier la ou les instances de la base de données.

Tous les serveurs de Policy Director gèrent une instance locale de la base de données des autorisations. Les serveurs concernés comprennent tous les gestionnaires de sécurité (secmgrd) et les serveurs d'autorisations de Policy Director (ivacld). Tous les serveurs Policy Director détiennent le droit d'affichage (v) sur l'objet /Management/Replica.

La duplication permet à ces processus d'afficher et d'accéder aux entrées de la base de données primaire des règles d'autorisation. Le programme d'installation de

Policy Director attribue automatiquement le droit de lecture (r) à tout serveur ayant besoin d'accéder à la base de données des règles d'autorisation.

Policy Director n'utilise actuellement pas le droit de modification (m). Pour modifier la base de données primaire des règles d'autorisation, vous devez utiliser la console de gestion ou l'utilitaire **ivadmin**. Ces outils sont soumis à d'autres contrôles plus restrictifs.

Recommandations pour créer un espace des noms sécurisé

Ces quelques recommandations vous aideront à concevoir un espace des noms sécurisé comme il convient :

- Définissez des règles de sécurité restrictives pour les objets conteneurs hiérarchiquement placés au sommet de l'espace des noms. Définissez des exceptions à ces règles au moyen d'une liste de contrôle d'accès explicite appliquée aux objets situés dans les niveaux inférieurs de la hiérarchie.
- Organisez votre espace des objets protégé de manière à ce que la plupart des objets soit protégés par des listes de contrôle d'accès héritées plutôt qu'explicites.

  Les LCA héritées simplifient la gestion de l'arborescence dans la mesure où elles réduisent le nombre de listes de contrôle d'accès présentes dans le domaine. Cette gestion allégée réduit aussi le risque d'erreurs pouvant compromettre les performances du réseau.
- Placez les nouveaux objets à l'emplacement de l'arborescence où ils hériteront des autorisations appropriées.

  Organisez l'arborescence des objets en sous-arborescences, chacune d'elles étant gouvernée par des règles d'accès spécifiques. De cette façon, vous pourrez déterminer ces conditions d'accès pour l'ensemble d'une sous-arborescence au moyen d'une liste de contrôle d'accès explicite appliquée à sa racine.
- Créez un jeu de modèles de LCA de base et réutilisez-les selon vos besoins.

  Dans la mesure où un modèle de LCA constitue une définition source unique, toute modification du modèle se répercute sur tous les objets auxquels il s'applique.
- Contrôlez les accès des utilisateurs au moyen de groupes.

  Une liste de contrôle d'accès peut ne contenir que des entrées de groupes. Pour contrôler individuellement comment les utilisateurs peuvent accéder aux ressources, ajoutez ou supprimez-les dans les groupes.

Modèles de LCA d'administration standard

Les modèles de LCA d'administration par défaut suivants constituent des bases de départ possibles pour sécuriser des régions déterminées du domaine sécurisé.

Vous pouvez créer des entrées pour les utilisateurs, les groupes et les entités authentifiées ou non authentifiées. Ces entrées offrent une gamme de contrôles élargie et répondent mieux aux besoins de votre espace des objets protégé.

Notez dans chaque LCA les utilisateurs et les groupes détenant le droit de contrôle (c). Les utilisateurs et les groupes ayant le droit de contrôle ont la propriété de la liste de contrôle d'accès et le droit de modifier ses entrées.

Racine

Les entrées fondamentales de la LCA par défaut de la racine (default-root) comprennent :

```
user cell_admin                 abcT
group iv-admin                  abcT
any-authenticated               T
unauthenticated                 T
```

La LCA de la racine est très simple. Chacun peut circuler dans l'espace des noms mais aucune autre action n'est permise. En principe, vous ne devez pas modifier ces entrées. Notez toutefois, que la LCA de la racine permet d'interdire rapidement l'accès à l'ensemble de l'espace des noms à un utilisateur ou un groupe donné.

Examinez l'entrée suivante de la LCA de la racine :

```
user jean
-----------------
```

La conséquence de cette entrée (aucune autorisation) est que `user jean` ne peut pas même franchir l'objet conteneur racine. Cet utilisateur n'a aucun accès à l'espace des objets protégé, quelles que soient les autorisations qui lui sont accordées dans les niveaux inférieurs de l'arborescence.

Vous pouvez appliquer cette même approche aux espaces des objets de WebSEAL et NetSEAL. Par exemple, vous pouvez supprimer le droit de traversée (T) à un utilisateur au niveau de l'objet conteneur /WebSEAL. Une fois ce droit supprimé, cet utilisateur ne peut plus accéder à l'espace des noms de WebSEAL quelles que soient les autorisations accordées sur les différents objets contenus dans cette région.

Espace des objets de WebSEAL

Les entrées fondamentales de la LCA de la région WebSEAL (default-webseal) comprennent :

```
user cell_admin                 abcTdmlrx
group iv-admin                  abcTdmlrx
group webseal-servers           gTdmlrx
group ivmgrd-servers            Tl
```

A l'installation, cette liste de contrôle d'accès par défaut s'attache à l'objet conteneur /WebSEAL dans l'espace des noms.

Le groupe `webseal-servers` contient une entrée pour chaque serveur WebSEAL existant dans le domaine sécurisé. Les autorisations par défaut permettent aux serveurs de répondre aux requêtes des navigateurs.

Le groupe `ivmgrd-servers` ne contient qu'une entrée qui définit les droits du serveur de gestion. La plupart des requêtes de gestion de la console de gestion partent du serveur de gestion vers le serveur WebSEAL de destination. Il en découle que le serveur de gestion doit avoir le droit d'adresser la requête au serveur de destination.

Le droit de traversée permet l'extension de l'espace Web tel que représenté dans la console de gestion. Le droit de liste permet à la console de gestion d'afficher le contenu de l'espace Web.

Espace des objets de NetSEAL

Les entrées fondamentales de la LCA de la région NetSEAL (default-netseal) comprennent :

```
user cell_admin                    abcTC
group iv-admin                     abcTC
```

A l'installation, cette liste de contrôle d'accès s'attache à l'objet conteneur /NetSEAL dans l'espace des noms. Vous devez attribuer le droit de contrôle (c) pour permettre l'accès à un service protégé.

Espace des objets de gestion

Les entrées fondamentales de la LCA de la région Management (default-management) comprennent :

```
user cell_admin                    abcTdmsv
group iv-admin                     abcTdmsv
group ivmgrd-servers               Ts
any-authenticated                  Tv
unauthenticated                    Tv
```

A l'installation, cette liste de contrôle d'accès s'attache à l'objet conteneur /Management dans l'espace des noms.

Objet de gestion des instances

Les entrées fondamentales de la LCA de gestion de la duplication (default-replica) comprennent :

```
group secmgrd-servers              dmv
group ivacld-servers               dmv
group ivmgrd-servers               m
group iv-admin                     abcTv
user cell_admin                    abcTv
```

Evaluation d'une liste de contrôle d'accès

Policy Director applique une procédure particulière pour déterminer les autorisations accordées à un utilisateur par une liste de contrôle d'accès.

Evaluation des requêtes authentifiées

Policy Director évalue un utilisateur authentifié selon la procédure suivante :

1. Policy Director recherche l'ID de utilisateur dans les entrées de type user de la LCA. Les autorisations accordées sont celles contenues dans l'entrée correspondant à cet ID, si elle existe.

   ```
   Entrée trouvée : l'évaluation prend fin. Aucune entrée trouvée : passage
   à l'étape suivante.
   ```

2. Policy Director détermine le ou les groupes auxquels l'utilisateur appartient et les recherche dans les entrées de type group de la liste de contrôle d'accès :

   Si plusieurs entrées de groupe correspondent, les autorisations réellement accordées résultent d'une combinaison logique "ou" (la moins restrictive) des autorisations définies dans chaque entrée trouvée.

   ```
   Entrée trouvée : l'évaluation prend fin.
   Aucune entrée trouvée : passage à l'étape suivante.
   ```

3. Policy Director attribue les autorisations définies dans l'entrée any-authenticated (si elle existe).

   ```
   Entrée trouvée : l'évaluation prend fin.
   Aucune entrée trouvée : passage à l'étape suivante.
   ```

4. S'il n'existe aucune entrée explicite du type any-authenticated dans la liste de contrôle d'accès, cette entrée est réputée exister implicitement mais n'accorder aucune autorisation (implicite ou explicite, l'entrée sera donc forcément trouvée).

   ```
   Entrée
   trouvée : aucune autorisation accordée.
   Fin du processus d'évaluation.
   ```

Evaluation des requêtes non authentifiées

Policy Director évalue les droits d'un utilisateur non authentifié d'après les autorisations définies dans l'entrée unauthenticated de la liste de contrôle d'accès.

L'entrée unauthenticated est un masque (une opération avec opérateur "et") appliqué à l'entrée any-authenticated lors de la détermination des autorisations. Une autorisation n'est accordée à une requête non authentifiée qu'à la condition de figurer également dans l'entrée any-authenticated (authentifié par une méthode quelconque).

Dans la mesure ou les droits des utilisateurs non authentifiés dépendent de l'entrée any-authenticated, il est illogique qu'une LCA contienne une entrée unauthenticated et pas d'entrée de type any-authenticated. Si cela se produit cependant, la réponse par défaut est de n'accorder aucune autorisation à l'utilisateur non authentifié.

Exemple d'entrées de liste de contrôle d'accès

Les autorisations des différents utilisateurs et/ou groupes se définissent à l'aide d'entrées du type approprié dans une liste de contrôle d'accès. Dans l'exemple suivant, le groupe `documentation` dispose d'un droit d'accès complet :

```
group documentation --bcg--TdmsvC-lrx
```

Vous pouvez réduire l'accès au domaine sécurisé pour les autres utilisateurs authentifiés (n'appartenant pas au groupe Documentation) à l'aide du type d'entrée any-authenticated (authentifié par une méthode quelconque) :

```
any-authenticated -------T-------rx
```

Vous pouvez encore réduire les droits d'accès pour les utilisateurs non membres du domaine sécurisé à l'aide du type d'entrée unauthenticated (non authentifié) :

```
unauthenticated -------T-------r-
```

Remarque : S'il n'existe pas d'entrée de LCA de type unauthenticated conférant quelques droits aux utilisateurs non authentifiés, ceux-ci ne peuvent accéder à aucun des documents sécurisés contenus dans le domaine sécurisé de Policy Director.

Modèle de LCA par héritage

Pour sécuriser les ressources d'un réseau dans un espace des objets protégé, vous devez associer une liste de contrôle d'accès à l'objet représentant chaque ressource.

Vous pouvez affecter une liste de contrôle d'accès à un objet de deux façons différentes :

- Attacher une liste de contrôle d'accès explicite à l'objet.
- Permettre que l'objet hérite sa liste de contrôle d'accès à partir des objets conteneurs de la hiérarchie.

Appliquer le principe d'héritage des listes de contrôle d'accès peut notablement réduire les tâches d'administration dans un domaine sécurisé. Cette section détaille les principes des LCA héritées (ou par analyse).

Présentation générale du modèle de LCA par analyse

L'avantage du système d'héritage des LCA repose sur le principe suivant : Tout objet dépourvu d'une liste de contrôle d'accès explicitement affectée hérite de la LCA explicitement définie pour l'objet conteneur le plus proche. En clair, tous les objets sans LCA explicitement attachée héritent des LCA des objets conteneurs avec une LCA explicitement attachée. Une chaîne d'héritages est rompue dès que vous attachez une LCA explicite à un objet de la hiérarchie.

L'héritage de LCA simplifie la définition et la gestion des contrôles d'accès dans un grand espace des objets protégé. Dans un espace des objets standard, il suffit d'attacher quelques listes de contrôle d'accès à des emplacements clés pour sécuriser l'ensemble de la hiérarchie. La présence de quelques listes de contrôle d'accès placées sur des positions clés indique qu'il s'agit d'un modèle de LCA par analyse.

Un espace des noms Policy Director standard commence par une unique liste de contrôle d'accès explicite attachée à l'objet conteneur de la racine. La LCA de la racine doit toujours exister et n'être jamais supprimée. Il s'agit, normalement, d'une LCA imposant peu de restrictions. Tous les objets hiérarchiquement situés en dessous héritent de cette liste de contrôle d'accès.

Lorsqu'une région, ou sous-arborescence, de l'espace des noms nécessite d'autres restrictions de contrôle d'accès, vous attachez une LCA explicite à la racine de cette sous-arborescence. Cette mesure brise la chaîne des LCA héritées de la racine de l'espace des noms primaire au niveau de la sous-arborescence. Une nouvelle chaîne d'héritages commence à partir de cette nouvelle liste de contrôle d'accès explicite.

Modèle de LCA de racine par défaut

Policy Director contrôle l'héritage en partant de la racine de l'espace des objets protégé. Si vous ne définissez pas explicitement d'autres listes de contrôle d'accès dans l'arborescence, l'ensemble de la hiérarchie hérite de la LCA de la racine.

Il existe toujours un modèle de LCA explicite défini sur la racine. L'administrateur peut remplacer cette LCA par une autre, contenant des entrées et des paramètres d'autorisation différents, mais la LCA de la racine ne peut jamais totalement disparaître.

Au cours de son installation et de sa configuration initiales, Policy Director définit explicitement le modèle de LCA de la racine dans la fenêtre de définition et de saisie des LCA :

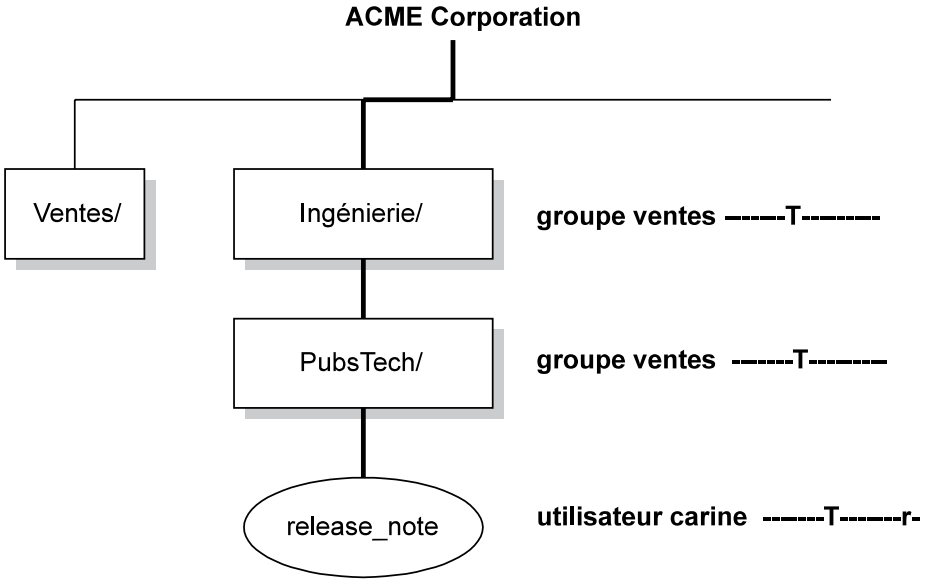
```
Nom
LCA    default-root
Description  LCA de racine par défaut
```

Droit de traversée

Le droit de traversée (T) permet à l'entité définie dans l'entrée de LCA de passer de l'autre côté des objets. L'entité a besoin de cette autorisation pour franchir un objet et accéder aux objets situés en dessous dans la hiérarchie. Le droit de traversée ne donne aucune autre autorisation sur l'objet auquel il s'applique. Vous devez aussi posséder le droit de traversée pour l'objet demandé lui-même.

L'illustration suivante montre le principe de fonctionnement du droit de traversée. Dans l'exemple de la société ACME, un répertoire Ingénierie contient un sous-répertoire appelé PubsTech. Carine (utilisateur carine) est membre du département Ventes et a besoin d'accéder au répertoire /Ingénierie/PubsTech pour examiner le fichier realease_note.

L'administrateur crée une entrée de LCA pour le groupe Ventes, avec le droit de traversée (T), sur les répertoires /Ingénierie et /PubsTech. Bien que l'utilisateur carine n'ai aucune aucune autorisation pour ces deux répertoires, il peut les traverser pour accéder au fichier release_note. Dans la mesure où ce fichier est assorti des droits traversée (T) et lecture (r) pour l'utilisateur carine, celui-ci peut lire le fichier.



Vous pouvez très facilement restreindre l'accès à la partie de la hiérarchie située en dessous d'un objet conteneur donné, ceci sans modifier les autorisations définies pour les objets concernés. Il suffit pour cela de supprimer le droit de traversée dans l'entrée de LCA appropriée. Supprimer ce droit de traversée sur un objet répertoire protège tous les objets placés plus bas dans la hiérarchie, même si ceux-ci sont attachés à des listes de contrôle d'accès moins restrictives.

Par exemple, le groupe Ventes doit avoir le droit de traversée (T) sur le répertoire Ingénierie. S'il ne l'avait pas, Carine, qui en est membre, ne pourrait pas accéder au fichier release_note, même si elle possède le droit de lecture (r) pour ce fichier.

Résolution d'une requête d'accès

L'héritage commence avec la LCA de la racine et s'applique à tous les objets de l'espace des noms jusqu'à ce qu'il existe un objet doté d'une liste de contrôle d'accès explicite. Une nouvelle chaîne d'héritages commence à partir de ce point.

Les objets placés sous un objet doté d'une liste de contrôle d'accès explicite héritent des contrôles d'accès définis dans cette liste. Si vous supprimez une LCA explicite, le contrôle d'accès pour tous les objets qu'elle gouvernait jusqu'alors redevient lié au répertoire ou à l'objet conteneur le plus proche qui en possède une.

Lorsqu'un utilisateur tente d'accéder à un objet sécurisé, Policy Director vérifie si cet utilisateur a les autorisations requises pour le faire. L'objet concerné peut être, par exemple, un document Web. Policy Director contrôle chaque objet présent dans la hiérarchie de l'objet pour déterminer les droits détenus par héritage ou explicitement définis.

Vous pouvez interdire à un utilisateur donné l'accès à un objet défini. Policy Director lui refusera l'accès si un objet conteneur ou répertoire quelconque des niveaux supérieurs de la hiérarchie n'accorde pas le droit de traversée (T) à cet utilisateur. Policy Director refusera également l'accès à l'objet cible si ses autorisations ne permettent pas l'opération demandée.

Pour satisfaire au contrôle d'accès, le demandeur doit posséder à la fois :

1. le droit de traverser le chemin menant à l'objet demandé ;
2. les autorisations requises pour utiliser l'objet demandé.

L'exemple suivant illustre comment Policy Director détermine si un utilisateur a le droit de lire (afficher) un objet :

```
/acme/ingénierie/projet_Y/courant/report.html
```

Policy Director contrôle :

1. le droit de traversée défini dans la LCA explicite de la racine (/) ;
2. le droit de traversée défini dans les listes de contrôle d'accès explicites des répertoires `acme`, `ingénierie`, `projet_Y` et `courant` ;
3. le droit de lecture défini pour le fichier lui-même (report.html).

Policy Director refuse l'accès à l'utilisateur si celui-ci ne satisfait pas au contrôle d'accès pour l'un de ces objets de la hiérarchie.

Application de modèles de LCA à différents types d'objet

Vous pouvez définir des autorisations dans un modèle de LCA pour divers types d'opération. Généralement, seules quelques opérations sont pertinentes pour un objet doté d'une liste de contrôle d'accès.

Cet aspect est lié aux deux outils qu'offre Policy Director pour faciliter l'administration d'un espace de noms :

- Les modèles de LCA ;
- L'héritage de LCA.

Les modèles de LCA permettent d'attacher la même définition de liste de contrôle d'accès à plusieurs objets dans l'espace des noms d'objet protégé. La définition de la LCA contient assez d'entrées pour répondre aux besoins de protection de tous les objets auxquels elle s'appliquera. Toutefois, seules quelques-unes de ces entrées ont un effet sur chaque objet.

Dans le système d'héritage de LCA, tout objet dépourvu d'une liste de contrôle d'accès explicite hérite de définitions de règle de sécurité. Ces définitions de règle de sécurité proviennent de la liste de contrôle d'accès appliquée à l'objet hiérarchiquement supérieur le plus proche.

En résumé, un modèle de LCA doit définir toutes les autorisations nécessaires pour tous les types d'objet auxquels il s'applique et non pas uniquement pour celui auquel il est attaché.

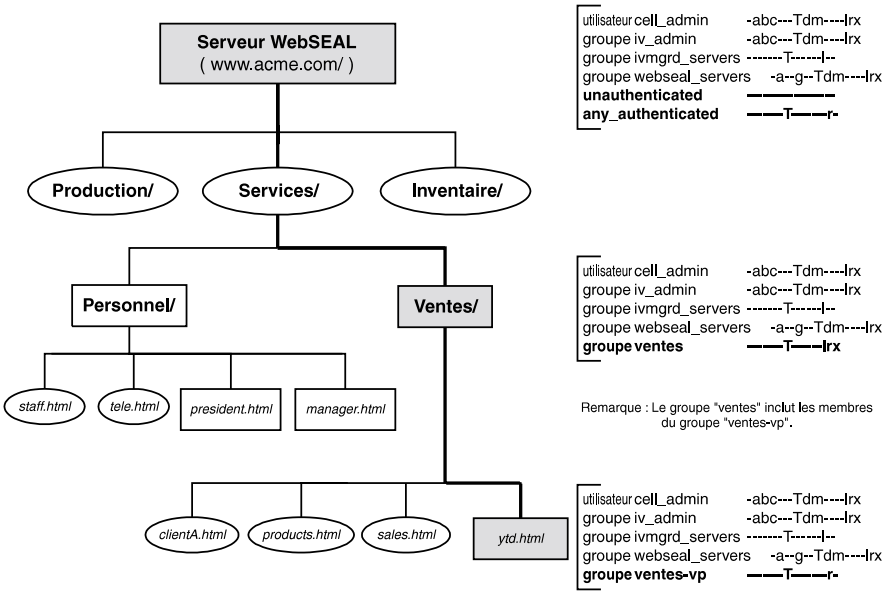
Exemple d'héritage de LCA

L'illustration suivante met en évidence le résultat d'une combinaison entre une LCA explicite et une LCA héritée dans un espace des noms.

Un espace des objets définit en général des règles de sécurité au niveau de l'objet `racine`. La racine est suivie de l'objet conteneur /WebSEAL et de sous-arbres individuellement gouvernés par les services qu'ils représentent.

Dans cet exemple, le groupe `ventes` a reçu la propriété de sa sous-arborescence. Notez que la LCA définie sur cette sous-arborescence n'utilise plus les entrées du type unauthenticated ou any-authenticated. Le fichier de ventes ytd.html possède une liste de contrôle d'accès explicite. Celle-ci accorde le droit de lecture (r) aux membres du groupe `ventes-vp` sachant que ceux-ci sont également membres du groupe `ventes`.

Remarque : Cette structure de LCA doit être modifiée ; des utilisateurs doivent être ajoutés ou retirés du domaine sécurisé. Les nouveaux utilisateurs sont simplement ajoutés à un ou plusieurs groupes appropriés. De même, des utilisateurs peuvent être exclus de ces groupes.



Délégation de la gestion des LCA

La répartition des responsabilités administratives au sein d'un domaine sécurisé est appelée la délégation de la gestion. La délégation de la gestion trouve généralement sa justification dans la croissance des demandes à laquelle un grand site, abritant plusieurs départements ou divisions de ressources, doit faire face.

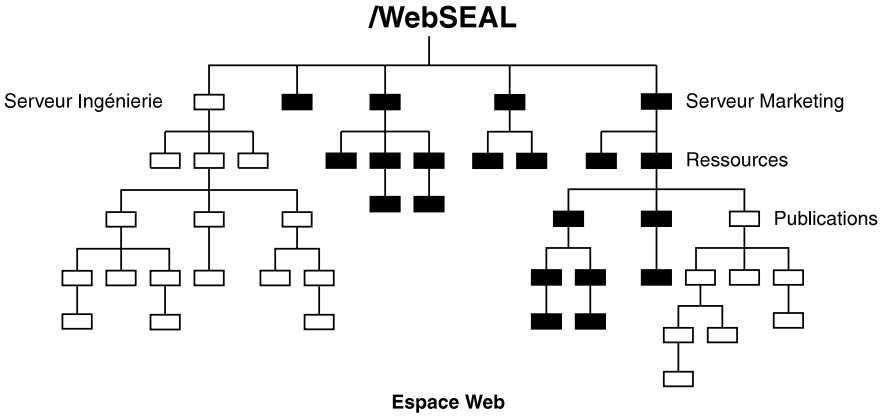
Généralement, un grand espace des objets peut être organisé en régions représentant ces départements ou divisions. Chaque région du domaine peut être organisée de façon plus adaptée mais aussi administrée par un responsable mieux informé des questions et besoins de son secteur.

Dans un domaine sécurisé de Policy Director, le compte cell_admin est au départ le seul doté d'autorisations d'administration. L'utilisateur cell_admin peut créer des comptes de gestionnaire et leur attribuer les autorisations requises pour des régions déterminées de l'espace des objets.

Structure de l'espace des noms pour la délégation de la gestion

Vous devez structurer votre espace des objets avec plusieurs régions, ou branches, distinctes, dans lesquelles des responsabilités de gestion intermédiaires pourront être assignées.

Dans l'exemple ci-dessous, les régions Ingénierie et Publications de l'espace des objets nécessitent un contrôle de gestion séparé. Le contrôle de ces régions commence à leur racine et couvre tous les objets hiérarchiquement inférieurs.



Utilisation d'utilisateurs et de groupes d'administration par défaut

Policy Director crée plusieurs groupes d'administration importants. Par défaut, ces utilisateurs et/ou groupes reçoivent des autorisations leur permettant de contrôler et de gérer toutes les opérations intervenant dans le domaine sécurisé. Ces règles de sécurité par défaut sont définies par les listes de contrôle d'accès au cours de l'installation.

Les sections qui suivent décrivent les rôles assignés à chacun de ces utilisateurs et groupes au moment de l'installation. L'administrateur peut par la suite adapter ces privilèges aux règles de sécurité de l'entreprise.

Utilisateur cell_admin

Cet utilisateur est l'administrateur du domaine sécurisé. Il possède tous les droits requis pour assurer l'ensemble des opérations possibles dans le domaine sécurisé.

Ces règles peuvent être modifiées à mesure que l'espace des objets grandit, notamment par le biais d'une délégation des droits de gestion à d'autres utilisateurs. Notez que certaines autorisations détenues par l'utilisateur cell_admin peuvent aussi lui être supprimées.

Groupe iv-admin

Ce groupe est celui des administrateurs. Comme cell_admin, tous les membres de ce groupe sont considérés par défaut comme étant des administrateurs du domaine sécurisé. Toutes les listes de contrôle d'accès par défaut accordent exactement les mêmes autorisations à l'utilisateur cell_admin et au groupe iv-admin.

Pour attribuer un rôle d'administrateur à un utilisateur, il suffit de l'ajouter au groupe iv-admin. Notez que cette procédure n'est cependant pas sans danger. Lorsqu'un utilisateur devient membre de ce groupe, il gagne automatiquement ses listes de contrôle d'accès par défaut. Pourvu de ces LCA par défaut, cet utilisateur détient désormais tous les droits sur n'importe quel objet de l'espace des noms.

Les règles par défaut appliquées au groupe iv-admin peuvent aussi être modifiées. Par exemple, vous pouvez les changer en déléguant des droits de gestion à d'autres utilisateurs, ou en révoquant tout ou partie des droits de gestion du groupe iv-admin.

Groupe ivmgrd-servers

Ce groupe contient le serveur de gestion. Policy Director restreint actuellement le serveur de gestion à une seule instance dans le domaine sécurisé. Il en découle que la définition de ce groupe ne contient que cette entrée.

La plupart des requêtes de gestion de la console de gestion partent du serveur de gestion vers le serveur Policy Director de destination. Le serveur de gestion doit donc avoir le droit d'adresser la requête au serveur de destination. Pour cette raison, ce groupe détient un droit d'administration de serveur (s) dans la LCA de gestion par défaut et un droit de liste (l) dans l'ensemble de l'espace Web.

Groupe webseal-servers

Ce groupe contient tous les serveurs WebSEAL existant dans le domaine sécurisé. La LCA WebSEAL par défaut fournit à ces serveurs le jeu complet des autorisations HTTP et le droit de délégation. Ces règles permettent notamment à tous les serveurs WebSEAL d'établir des jonctions entre eux. Vous pouvez modifier cette LCA pour accorder ces autorisations serveur par serveur.

Création d'utilisateurs administrateurs

Policy Director permet de créer des comptes d'administrateur dotés de niveaux de responsabilité variables. La responsabilité est déléguée aux administrateurs par le biais de LCA d'administration stratégiquement disposées dans la hiérarchie. La liste suivante détaille quelques-uns des rôles administratifs possibles :

Responsabilités de gestion des LCA

L'administrateur de LCA peut contrôler tout ou partie d'une région de l'espace des noms d'objet protégé, selon l'emplacement de la liste de contrôle d'accès d'administration. L'entrée de LCA de l'administrateur peut contenir les autorisations b, a et T, ainsi que d'autres droits adaptés aux opérations exécutées sur les objets de cette région.

L'administrateur de LCA peut utiliser la console de gestion pour attacher des listes de contrôle d'accès aux objets de l'espace des noms dont il a la charge. A cet égard, il peut utiliser le jeu de modèles de LCA existant mais doit posséder l'autorisation d'attacher (a). Notez que cet administrateur n'a pas le droit de créer, modifier ou supprimer les modèles de LCA.

Responsabilités des règles de LCA

L'administrateur des règles de LCA est en principe chargé de contrôler la création et la modification de tous les modèles de LCA utilisés dans le domaine sécurisé. Il doit recevoir les autorisations d, b, m et v sur l'objet /Management ou /Management/ACL.

Cet administrateur des règles de LCA peut créer de nouveaux modèles de LCA puisqu'il détient l'autorisation de les modifier (m). Etant son créateur, l'administrateur figure, par défaut, dans la première entrée du nouveau

modèle de LCA et reçoit les autorisations abcT. Le droit de contrôle (c) lui donne la propriété effective de la liste de contrôle d'accès et lui permet de la modifier.

Etant son propriétaire, l'administrateur peut aussi utiliser le droit de suppression (d) que lui accorde la LCA de gestion. Il peut dès lors utiliser ce droit pour supprimer la LCA de la liste des modèles. Notez que seul le propriétaire d'un modèle de LCA peut le supprimer.

Responsabilités de gestion des serveurs
Cet administrateur reçoit les autorisations d, m, s et v sur l'objet /Management/Server. Il peut exécuter des opérations impliquant les serveurs de Policy Director.

Responsabilités des tâches d'autorisation
Cet administrateur reçoit les autorisations (d) et (m) sur l'objet /Management/Action. Il peut créer toutes les autorisations requises pour les applications tiers ou les supprimer.

Reportez-vous à la section «Région Management (gestion) de l'espace des noms» à la page 92 pour plus d'informations sur l'espace des noms Management.

Exemple de modèle de LCA d'administration

L'exemple suivant explique comment un utilisateur obtient des droits d'administrateur.

- La LCA suivante définie sur l'objet /WebSEAL accorde des droits d'administrateur à l'utilisateur `user adam` :

```
user cell_admin                 abcTdmlrx
group iv-admin                  abcTdmlrx
group webseal-servers           gTdmlrx
group ivmgrd-servers            Tl
user adam                       abcTdmlrx
any-authenticated               Trx
unauthenticated                 Trx
```

- La LCA suivante définie sur l'objet /NetSEAL accorde des droits d'administrateur à l'utilisateur `user adam` :

```
user cell_admin                         abcTC
group iv-admin                          abcTC
user adam                               abcTC
any-authenticated                       TC
unauthenticated                         TC
```

Exemple de délégation de la gestion

Un grand espace des objets peut nécessiter plusieurs administrateurs pour gérer les différentes sous-branches. Dans cette situation, les LCA des répertoires du chemin de chacune de ces branches doivent contenir des entrées pour chaque compte, leur accordant le droit de traversée. Pour un site doté de plusieurs administrateurs, les LCA peuvent contenir une longue liste d'entrées correspondant à ces comptes d'administrateur.

Le problème que pose l'existence simultanée de nombreuses entrées de LCA pour les administrateurs peut être résolu par la technique suivante :

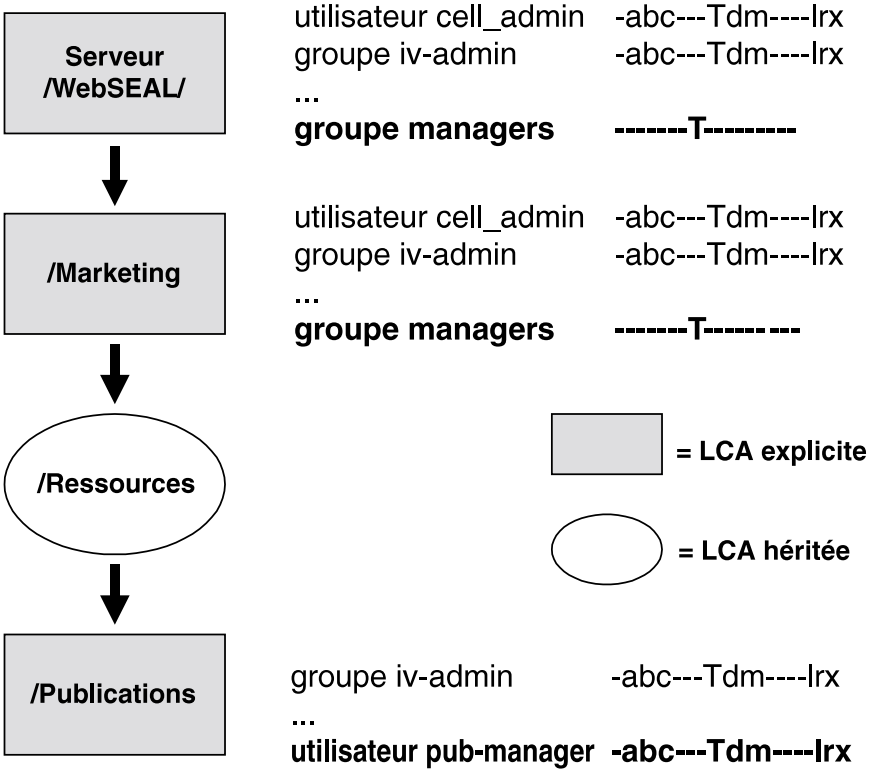
1. Créez un compte de groupe d'administrateurs.

2. Ajoutez tous les nouveaux administrateurs à ce groupe.
3. Ajoutez ce groupe sous la forme d'une entrée de LCA (avec droit de traversée) au niveau des répertoires menant aux différentes sous-branches demandant une délégation de la gestion.
4. Dans chaque LCA de racine de branche, ajoutez l'entrée d'administrateur appropriée (avec les autorisations b, c, T, plus d'autres droits appropriés).
5. L'administrateur en chef peut à présent supprimer l'entrée de LCA du groupe d'administrateurs (et toute autre entrée) au niveau de la racine de l'espace des objets.

   Désormais, seul cet utilisateur détient le contrôle total de la racine et de tous les objets de la hiérarchie.

Dans l'exemple ci-dessous, le groupe `managers` a été créé pour accueillir tous les utilisateurs administrateurs. L'utilisateur `pub-manager` est un membre de ce groupe et possède donc le droit de traversée requis pour naviguer jusqu'au répertoire Publications.

La liste de contrôle d'accès du répertoire Publications comprend une entrée pour l'utilisateur `pub-manager`. L'utilisateur `pub-manager` est l'administrateur délégué de cette branche et possède les autorisations appropriées pour la gérer. En qualité d'administrateur délégué, `pub-manager` peut supprimer l'entrée du groupe `manager` (et toute autre entrée) de la liste de contrôle d'accès du répertoire Publications. En supprimant l'entrée du groupe et toutes les autres entrées de LCA, l'administrateur délégué obtient le contrôle absolu de cette branche de l'espace Web.



Chapitre 8. Application du contrôle d'accès

Vous pouvez protéger les ressources d'un domaine sécurisé au moyen de modèles de règle. Les modèles de règle contiennent des autorisations qui contrôlent l'utilisation des ressources. Vous devez attacher ces modèles de règle aux objets représentant ces ressources dans l'espace des noms.

Policy Director reconnaît et utilise un type de modèle de règle appelé liste de contrôle d'accès (LCA). Les listes de contrôle d'accès permettent d'attacher les règles de sécurité de l'entreprise aux ressources affectées au domaine sécurisé.

Ce chapitre aborde les tâches usuelles à exécuter pour gérer l'espace des objets et appliquer le contrôle d'accès.

Ce chapitre comprend les sections suivantes :

Présentation générale de la gestion des LCA

Les modèles de LCA se créent, se modifient ou se suppriment à l'aide du panneau des tâches de gestion des LCA de la console de gestion de Policy Director.

1. Connectez-vous à la console de gestion sous un ID d'administrateur de LCA tel que `cell_admin`.
2. Cliquez sur l'onglet de tâches **LCA**.

   Le panneau de tâches de gestion des LCA apparaît.

Boutons de commande des tâches de gestion des LCA

Les boutons de commande du panneau **LCA** exécutent des opérations de gestion sur les listes de contrôle d'accès. Le tableau suivant décrit les tâches de chaque bouton de commande :

Bouton de commande	Description
Nouvelle LCA	Permet de créer un modèle de LCA.
Nouvelle entrée	Ajoute une nouvelle entrée dans le modèle de LCA sélectionné.
Sauvegarde	Enregistre le modèle de LCA. La liste de contrôle d'accès apparaît dans la vue de la liste des noms de LCA.
Suppression	Supprime le modèle de LCA sélectionné.
Extraction	Récupère les informations liées au modèle de LCA désigné et renseigne les champs de sa vue détaillée. Insère le nom de la LCA dans le champ Nom LCA de la section Définition de LCA.
Liste	Régénère l'affichage de la liste.
Utilisation par	Affiche la liste complète des objets protégés disposés à l'emplacement où le modèle de LCA est attaché. Ces informations apparaissent dans la section Tableau d'informations de la console de gestion.

Tâches de gestion des LCA

Vous pouvez exécuter les tâches de gestion de LCA suivantes :

- Création d'un modèle de LCA
- Ajout d'une entrée de LCA
- Modification des autorisations définies dans une entrée de LCA
- Suppression d'un modèle de LCA

Création d'un modèle de LCA

Pour créer un modèle de LCA, vous pouvez utiliser l'un des modèles de LCA par défaut proposés comme base de départ et l'adapter à vos besoins.

1. A partir de la liste **Nom LCA**, faites glisser vers le Tableau d'informations l'icône du modèle de LCA à utiliser comme base de départ pour créer la nouvelle liste de contrôle d'accès.
2. Cliquez sur le bouton de commande **Nouvelle LCA**.

   Les informations initialement présentes dans la zone Définition de LCA disparaissent dans l'attente des nouvelles entrées.

   Par défaut, votre ID de connexion occupe la première entrée, avec les autorisations abcT. Le droit de contrôle (c) vous donne la propriété de cette liste de contrôle d'accès.
3. Tapez le nom de la liste de contrôle d'accès dans le champ **Nom LCA**.
4. Passez au champ **Description** et décrivez la finalité de cette liste de contrôle d'accès (comment et/ou pourquoi vous la créez).
5. Faites glisser l'icône **LCA** par défaut du Tableau d'informations vers la zone Entrée de LCA de la zone de définition.

   La nouvelle liste de contrôle d'accès contient à présent les entrées de la LCA par défaut.
6. Modifiez les entrées à votre convenance.
7. Cliquez sur **Sauvegarde**.

Ajout d'une entrée de LCA

Pour ajouter une entrée de LCA :

1. A partir de la liste **Nom LCA**, sélectionnez un modèle de LCA.
2. Cliquez sur le bouton de commande **Nouvelle entrée**.

   Les données de la zone Entrée de LCA disparaissent dans l'attente d'une nouvelle entrée.
3. Cliquez sur le champ **Type** et maintenez le bouton de la souris enfoncé.

   Un menu déroulant apparaît.
4. Sélectionnez le type user, group, any-authenticated ou unauthenticated.
5. Cliquez sur le champ **ID** et entrez l'ID approprié.

   Vous pouvez également prendre/déposer des icônes d'utilisateur et de groupe à partir de la vue **Gestion des comptes**. Cliquez sur l'onglet de tâches **Comptes** et déplacez la vue **Gestion des comptes** dans le panneau inférieur de la console.
6. A l'aide des cases à cocher, sélectionnez les autorisations appropriées pour cette entrée.
7. Cliquez sur le bouton **Sauvegarde** pour valider l'entrée dans la liste de contrôle d'accès.

Modification des autorisations définies dans une entrée de LCA

Pour modifier les autorisations définies dans une entrée de LCA :

1. Sélectionnez l'entrée à modifier dans la zone Définition de LCA.
2. Dans la zone Entrée de LCA, sélectionnez les autorisations appropriées au moyen des cases à cocher associées.
3. Cliquez sur le bouton **Sauvegarde** pour valider les modifications.

Suppression d'un modèle de LCA

Pour supprimer un modèle de LCA :

1. Dans la liste **Nom LCA**, sélectionnez le modèle de LCA à supprimer.
2. Cliquez sur le bouton **Suppression**.

   Un message d'avertissement apparaît.
3. Cliquez sur **OK**

   Notez que la console de gestion refuse de supprimer une liste de contrôle d'accès encore appliquée à un objet. Dans cette situation, un message d'avertissement apparaît dans la barre d'état pour vous en informer.

Exemple :

Vous avez appliqué une liste de contrôle d'accès conçues pour les membres du groupe `webtest`. Le groupe `webtest` comprend des personnes chargées de développer et de tester de nouvelles pages HTML. Une fois ces pages validées, vous pouvez supprimer cette LCA explicite pour les rendre accessibles aux autres membres du domaine sécurisé.

Procédure type de création d'un modèle de LCA

Pour créer un modèle de LCA :

1. Cliquez sur le bouton de commande **Nouvelle LCA**.

   Les informations initialement présentes dans la zone Définition de LCA disparaissent dans l'attente des nouvelles entrées.

   Par défaut, votre ID de connexion occupe la première entrée, avec les autorisations abcT.
2. Tapez le nom de la liste de contrôle d'accès dans le champ **Nom LCA**.
3. Passez au champ **Description** et décrivez la finalité de cette liste de contrôle d'accès (comment et/ou pourquoi vous la créez).
4. Cliquez sur le bouton **Sauvegarde** pour valider la nouvelle liste de contrôle d'accès et la faire entrer dans la liste des LCA.
5. Cliquez sur le bouton de commande **Nouvelle entrée**.

   Les données de la zone Entrée de LCA disparaissent dans l'attente d'une nouvelle entrée.
6. Cliquez sur le champ **Type** et maintenez le bouton de la souris enfoncé.

   Un menu déroulant apparaît.
7. Cliquez sur **unauthenticated** et n'entrez aucune autorisation.
8. Cliquez sur le bouton **Sauvegarde**.

   L'entrée apparaît dans la zone Définition de LCA.
9. Suivez la même procédure pour ajouter une entrée any-authenticated sans définir d'autorisations.
10. Cliquez sur l'onglet de tâches **Comptes**.

Le panneau de gestion des comptes apparaît dans le panneau supérieur.

11. Cliquez sur le bouton **Déplacer tâche en bas** pour positionner le panneau de gestion des comptes dans la partie inférieure de la console.
12. Pour créer une entrée de groupe, cliquez sur **Nouvelle entrée** dans le panneau LCA.
13. A partir de la liste **Groupes** du panneau Comptes, faites glisser une icône **group** vers le champ **ID** de la zone Entrée de LCA.

    Les données correspondantes s'insèrent dans les champs **Type** et **ID**.
14. Sélectionnez les autorisations désirées.
15. Cliquez sur le bouton **Sauvegarde** pour valider l'entrée dans la liste de contrôle d'accès.

Présentation générale de la gestion de l'espace des objets

Le panneau de tâches de gestion Espace objets, dans la console de gestion, permet d'associer des listes de contrôle d'accès aux objets de l'espace des noms ou d'en supprimer.

1. Connectez-vous à la console de gestion sous un ID doté de droits d'administrateur de LCA tel que `cell_admin`.
2. Cliquez sur l'onglet de tâches **Espace objets**.

   Le panneau de tâches de gestion Espace objets apparaît.

Boutons de commande des tâches de gestion du panneau Espace objets

Les boutons de commande du panneau **Espace objets** permettent d'exécuter des opérations de gestion de l'espace des objets. Le tableau suivant décrit les tâches de chaque bouton de commande :

Bouton de commande	Description
Attacher LCA	Affecte une LCA à un objet.
Supprimer LCA	Supprime une LCA attachée à un objet.
Rechercher LCA	Recherche tous les objets explicitement attachés à une LCA déterminée. Les objets concernés apparaissent dans le panneau inférieur de la console.
Enregistrer LCA	Enregistre les modifications apportées à une LCA dans la vue Edition LCA.
Liste	Régénère la vue de l'arborescence de l'espace des objets.

Tâches de gestion du panneau Espace objets

Vous pouvez exécuter les tâches de gestion de l'espace des objets suivantes :

- Application d'une LCA à un objet
- Suppression d'une LCA explicite attachée à un objet

Application d'une LCA à un objet

L'application de listes de contrôle d'accès aux objets, comme leur suppression, requiert les droits de gestion appropriés. Vous devez en particulier posséder le droit d'attachement (a) pour appliquer une liste de contrôle d'accès à des objets.

1. Positionnez le panneau de tâches de gestion LCA dans la partie inférieure de la console.
2. Cliquez sur le panneau Espace objets dans le panneau supérieur de la console.
3. Développez la région désirée de l'arborescence de l'espace des objets et sélectionnez l'objet auquel vous voulez appliquer une liste de contrôle d'accès explicite.
4. Faites glisser l'icône du modèle de LCA désiré à partir de la liste **Nom LCA** jusque sur l'objet sélectionné dans l'arborescence de l'espace des objets.

Suppression d'une LCA explicite attachée à un objet

L'application de listes de contrôle d'accès aux objets, comme leur suppression, requiert les droits de gestion appropriés. Vous devez en particulier posséder le droit d'attachement (a) pour appliquer une liste de contrôle d'accès à des objets.

1. Cliquez sur l'onglet de tâches **Espace objets**.
2. Développez la région désirée de l'arborescence de l'espace des objets et sélectionnez l'objet auquel vous voulez retirer sa liste de contrôle d'accès explicite.
3. Cliquez sur le bouton **Supprimer LCA**.

Chapitre 9. Gestion des utilisateurs relais

La solution IBM SecureWay FirstSecure (FirstSecure) comprend le produit de sécurité IBM SecureWay Boundary Server pour Windows NT et AIX (Boundary Server). Si LDAP est votre registre des utilisateurs par défaut, vous pouvez utiliser Policy Director conjointement avec Boundary Server pour créer une solution intégrée de gestion des utilisateurs relais comprenant IBM Firewall et Policy Director.

Pour plus d'informations sur le produit FirstSecure et ses composants, contactez le site Web :

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

Principes de la sécurisation des limites

Comme Policy Director, Boundary Server est l'un des produits fournis avec le progiciel de sécurité IBM SecureWay FirstSecure. Vous pouvez également acheter Boundary Server ou Policy Director séparément puis les utiliser de manière autonome (sans acheter l'ensemble du progiciel FirstSecure).

La sécurisation des limites de votre réseau ne fait pas que protéger celui-ci en plus des applications et des informations qu'il héberge mais étend également l'accessibilité de vos ressources. Une sécurité des limites efficace implique que vous devez contrôler à la fois qui et quelles informations pénètrent dans votre réseau et en sortent. Boundary Server offre des fonctions de pare-feu, de sécurité et de réseau privé virtuel (RPV). Boundary Server établit une limite, ou frontière, entre votre réseau et l'Internet. Cette limite vous permet de bloquer les virus potentiellement dangereux, les scripts Java, les applets, les contrôles ActiveX et même les courriers électroniques indésirables (SPAM).

Reportez-vous au manuel IBM SecureWay Boundary Server - Guide de configuration et d'utilisation, fourni avec ce dernier produit, pour plus d'informations sur la planification, l'installation, la configuration, l'utilisation et la résolution des incidents du produit Boundary Server.

Boundary Server est un progiciel comprenant plusieurs modules qui réunissent les meilleures technologies de sécurité sous la forme d'une solution intégrée. Cette solution intègre les services d'assistance IBM disponibles en option.

Le progiciel Boundary Server comprend notamment le produit IBM SecureWay Firewall Version 4.1 (Firewall).

Intégration d'IBM Firewall

L'objectif d'un pare-feu est d'empêcher les communications non désirées ou non autorisées de pénétrer dans le réseau sécurisé ou d'en sortir. Un pare-feu fait respecter une sorte de blocus entre un ou plusieurs réseaux privés internes sécurisés et les autres réseaux (non sécurisés) ou l'Internet publique.

IBM Firewall est un programme de sécurité de réseau. IBM SecureWay Firewall Version 4.1 comprend les nouvelles fonctions suivantes :

- Améliorations du serveur relais de messagerie sécurisée
- Améliorations du protocole Socks version 5
- Service d'accès à distance (SAD)

- Serveur relais HTTP

Le serveur relais HTTP gère les requêtes des navigateurs au moyen du pare-feu SecureWay Firewall, ceci éliminant le besoin d'un serveur de sockets pour la navigation sur le Web. Les utilisateurs peuvent accéder aux informations de l'Internet sans menacer la sécurité de leurs réseaux internes ni nécessiter l'installation d'un serveur relais HTTP dans leurs environnements clients.

Avant d'installer SecureWay Firewall, vérifiez que le matériel et les logiciels requis sont disponibles, installés et configurés. Vous devez également définir des interfaces sécurisées, déterminer et organiser vos règles de sécurité et définir les objets du réseau. Les objets de réseau clés suivants doivent impérativement être définis :

- Les interfaces sécurisées du pare-feu ;
- Les interfaces non sécurisées du pare-feu ;
- Un réseau sécurisé ;
- Chaque sous-réseau du réseau sécurisé ;
- Un objet de réseau système hôte pour héberger les serveurs Security Dynamics et les serveurs de domaine Windows NT, le cas échéant.

Pour plus d'informations sur l'installation et la configuration du pare-feu IBM Firewall, reportez-vous au manuel IBM SecureWay Boundary Server - Guide de configuration et d'utilisation fourni avec Boundary Server.

Description des types d'utilisateur

Les administrateurs d'IBM Firewall ont la charge de créer, configurer et modifier les définitions des utilisateurs relais mais ne peuvent ni créer, ni modifier les définitions des autres administrateurs de pare-feu.

Les administrateurs de pare-feu ont la responsabilité des tâches suivantes :

- Déclaration des utilisateurs sur le pare-feu IBM Firewall afin de leur permettre d'accéder aux hôtes résidant hors du réseau protégé.
- Modification des attributs des utilisateurs parvenant au pare-feu.
- Suppression des définitions des utilisateurs n'ayant plus besoin de sortir de leur réseau.

Dans le cadre d'une solution intégrant IBM Firewall et Policy Director, la gestion des utilisateurs relais est du ressort de l'administrateur de Policy Director.

Utilisateurs du pare-feu

Les utilisateurs d'un réseau sécurisé peuvent accéder à un réseau non sécurisé au moyen d'un système de mise en réseau (serveur Socks ou relais). Pour permettre aux utilisateurs sécurisés de votre réseau d'accéder à un réseau non sécurisé (relais), vous devez établir et configurer des connexions adaptées à ce type de transaction.

Les services effectivement disponibles dépendent des décisions prises au moment de la planification. Mettre en oeuvre un service implique souvent d'établir et de configurer des connexions propres à servir ce type de transaction. Par exemple, pour permettre aux utilisateurs de naviguer sur le Web à l'aide d'un serveur relais HTTP, vous devez configurer le démon HTTP Proxy, sur le pare-feu mais également les connexions requises pour les transactions HTTP.

Si vous pensez avoir besoin d'une procédure d'authentification pour des fonctions telles que les connexions Web sortantes, déclarez les utilisateurs concernés sur le pare-feu IBM Firewall.

Utilisateurs relais

L'administrateur de Policy Director peut prévoir de gérer les utilisateurs relais dans le prolongement de la gestion des utilisateurs de Policy Director. Pour une solution intégrant Policy Director et IBM Firewall, les utilisateurs doivent être définis comme utilisateurs relais de Policy Director.

Un utilisateur relais est une personne qui utilise des services du pare-feu, tels que le serveur relais HTTP, pour accéder à des sites Web à partir d'un réseau d'entreprise. Les utilisateurs relais peuvent utiliser des services en franchissant le pare-feu mais ne peuvent ni accéder à distance à la machine du pare-feu ni s'y connecter localement.

Gestion des utilisateurs relais - Activation

Avant de passer à la phase de gestion des utilisateurs relais, vous devez activer cette fonction dans la console de gestion. Pour activer la fonction Utilisateur relais, vous devez éditer le fichier console.properties.

Le fichier console.properties file se trouve dans le répertoire :

Windows : `C:\Program Files\IBM\IVConsole\console.properties`

UNIX : `/opt/intraverse/ivconsole/console.properties`

Pour configurer la gestion des utilisateurs relais :

1. Ouvrez le fichier console.properties à l'aide d'un éditeur de texte.
2. Supprimez le symbole de commentaire (#) au début de la ligne suivante :
   ```
   #6, ProxyUsersTaskView            = IV.ProxyUserTask.ProxyUsersTaskView
   ```
3. Réamorcez la console de gestion pour activer la fonction de gestion Utilisateur relais.

Présentation de la gestion des utilisateurs relais

Dans le contexte de Policy Director, les utilisateurs du pare-feu sont appelés des utilisateurs relais. La console de gestion de Policy Director permet de gérer ces utilisateurs relais.

Les administrateurs de Policy Director ont la responsabilité des tâches suivantes :

- Définition des utilisateurs comme utilisateurs relais pour leur permettre d'utiliser les services du pare-feu.
- Modification des attributs des utilisateurs relais utilisant les services du pare-feu.
- Suppression des utilisateurs relais n'ayant plus besoin des services du pare-feu.

Les administrateurs de pare-feu pourront se reporter à la documentation d'IBM Firewall pour plus d'informations sur ces tâches d'administration.

Utilisation du panneau de gestion Utilisateurs relais

Le panneau de tâches de gestion Utilisateurs contient une vue arborescente titrée **Utilisateurs** et une vue détaillée intitulée **Utilisateur relais**.

Utilisation des boutons de commande du panneau de gestion des utilisateurs relais

Les boutons de commande de la vue **Utilisateur relais** permettent d'exécuter des tâches de gestion sur les utilisateurs relais. Le tableau suivant décrit les tâches de chaque bouton de commande :

Bouton de commande	Description
Sauvegarde	Crée un nouvel utilisateur relais si vous avez sélectionné un utilisateur Policy Director dans la vue arborescente des utilisateurs, ou, modifie un utilisateur relais existant si vous en avez sélectionné un dans la vue arborescente des utilisateurs.
Suppression	Supprime l'utilisateur relais sélectionné.

Utilisation des champs de définition des utilisateurs relais

Le tableau suivant décrit les champs de la vue **Données utilisateur relais** de la console de gestion :

Champ	Description
Utilisateur relais	Nom affecté à l'utilisateur défini pour l'accès par serveur relais. Il s'agit du nom d'utilisateur qu'utilisera cette personne pour se connecter au serveur TELNET ou FTP du pare-feu IBM Firewall. Cet utilisateur n'a aucun droit administratif.
Domaine relais	Nom du domaine du serveur relais du pare-feu.
Mot de passe	Mot de passe utilisé pour se connecter au domaine du serveur relais du pare-feu.
Description	Chaîne de texte décrivant les caractéristiques de l'utilisateur relais. Le champ Description est une zone de saisie facultative et ses données ne sont pas utilisées par le registre.
Shell distant	Indique le shell de connexion à distance à utiliser pour l'utilisateur relais. Au choix : **/bin/restrict.sh**, **/bin/csh**, **/bin/ksh /bin/bsh**, **/bin/oneact.sh**, ou une chaîne vide.
Shell local	Indique le shell de connexion local à utiliser pour l'utilisateur relais. Au choix : **/bin/restrict.sh**, **/bin/csh**, **/bin/ksh /bin/bsh**, **/bin/oneact.sh**, ou une chaîne vide.
Groupe par défaut	Indique le groupe par défaut auquel l'utilisateur relais appartient. L'administrateur peut sélectionner ce groupe dans la liste des groupes dont l'utilisateur relais est membre.
Authentification FTP sécurisée	Indique le niveau d'authentification requis pour que cet utilisateur puisse utiliser FTP pour accéder au pare-feu à partir du réseau sécurisé. Au choix : **Mot de passe du pare-feu**, **Tout autoriser**, **Tout interdire**, **Carte SecurID**, **Mot de passe NT**, **Défini par l'utilisateur 1**, **Défini par l'utilisateur 2**, **Défini par l'utilisateur 3**, **Mot de passe AIX**, ou une chaîne vide.

Authentification FTP à distance	Indique le niveau d'authentification requis pour que cet utilisateur puisse utiliser FTP pour accéder au pare-feu à partir du réseau non sécurisé. Au choix : **Mot de passe du pare-feu**, **Tout autoriser**, **Tout interdire**, **Carte SecurID**, **Mot de passe NT**, **Défini par l'utilisateur 1**, **Défini par l'utilisateur 2**, **Défini par l'utilisateur 3**, **Mot de passe AIX**, ou une chaîne vide.
Authentification Telnet sécurisée	Indique si l'identité de cet utilisateur doit être authentifiée par une procédure ad-hoc, s'il tente de se connecter à partir du réseau sécurisé. Au choix : **Mot de passe du pare-feu**, **Tout autoriser**, **Tout interdire**, **Carte SecurID**, **Mot de passe NT**, **Défini par l'utilisateur 1**, **Défini par l'utilisateur 2**, **Défini par l'utilisateur 3**, **Mot de passe AIX**, ou une chaîne vide.
Authentification Telnet à distance	Indique si l'identité de cet utilisateur doit être authentifiée par une procédure ad-hoc, s'il tente de se connecter à partir du réseau non sécurisé. Au choix : **Mot de passe du pare-feu**, **Tout autoriser**, **Tout interdire**, **Carte SecurID**, **Mot de passe NT**, **Défini par l'utilisateur 1**, **Défini par l'utilisateur 2**, **Défini par l'utilisateur 3**, **Mot de passe AIX**, ou une chaîne vide.
Authentification SOCK sécurisée	Spécifie la méthode d'authentification Socks V5 pour les connexions des clients Socks provenant de côté sécurisé du pare-feu. Au choix : **Mot de passe du pare-feu**, **Tout autoriser**, **Tout interdire**, **Carte SecurID**, **Mot de passe NT**, **Défini par l'utilisateur 1**, **Défini par l'utilisateur 2**, **Défini par l'utilisateur 3**, **Mot de passe AIX**, ou une chaîne vide.
Authentification SOCK à distance	Spécifie la méthode d'authentification Socks V5 pour les connexions des clients Socks provenant de côté non sécurisé du pare-feu. Au choix : **Mot de passe du pare-feu**, **Tout autoriser**, **Tout interdire**, **Carte SecurID**, **Mot de passe NT**, **Défini par l'utilisateur 1**, **Défini par l'utilisateur 2**, **Défini par l'utilisateur 3**, **Mot de passe AIX**, ou une chaîne vide.
Authentification HTTP sécurisée	Spécifie la méthode d'authentification par couple ID utilisateur/mot de passe pour les requêtes sortantes utilisant le serveur relais HTTP. Au choix : **Mot de passe du pare-feu**, **Tout autoriser**, **Tout interdire**, **Carte SecurID**, **Mot de passe NT**, **Défini par l'utilisateur 1**, **Défini par l'utilisateur 2**, **Défini par l'utilisateur 3**, **Mot de passe AIX**, ou une chaîne vide.
Authentification locale	Spécifie la méthode d'authentification locale. Au choix : **Mot de passe du pare-feu**, **Tout autoriser**, **Tout interdire**, **Carte SecurID**, **Mot de passe NT**, **Défini par l'utilisateur 1**, **Défini par l'utilisateur 2**, **Défini par l'utilisateur 3**, **Mot de passe AIX**, ou une chaîne vide.
Délai avant déconnexion	Indique le délai d'inactivité maximal autorisé avant la déconnexion d'office de l'utilisateur.
Délai avant avertissement	Indique la durée de la période de préavis avant la déconnexion de l'utilisateur.

Validation du mot de passe	Indique si un message doit demander à l'utilisateur d'entrer un mot de passe. Le pare-feu IBM Firewall demandera un mot de passe pour cet utilisateur.
Mot de passe verrouillé	Indique si le mot de passe doit être verrouillé. L'administrateur peut affecter la valeur yes à ce champ pour empêcher l'utilisateur d'utiliser l'authentification par mot de passe.

Création d'un utilisateur relais

Pour créer un utilisateur relais :

1. Cliquez sur l'onglet de tâches **Utilisateur relais**.
2. Développez la région appropriée de l'arborescence **Utilisateurs** et sélectionnez l'utilisateur Policy Director dont vous voulez faire un utilisateur relais.
3. Renseignez les champs de la vue **Données utilisateur relais**.
4. Cliquez sur le bouton **Sauvegarde**.

Modification des propriétés d'un utilisateur relais

Pour modifier les propriétés d'un utilisateur relais :

1. Cliquez sur l'onglet de tâches **Utilisateur relais**.
2. Développez la région appropriée de l'arborescence **Utilisateurs** et sélectionnez un utilisateur relais dans la liste.

   La zone Données utilisateur relais affiche les propriétés de l'utilisateur relais sélectionné.
3. Entrez-y les nouvelles données.
4. Cliquez sur le bouton **Sauvegarde**.

Suppression d'un utilisateur relais

Pour supprimer un utilisateur relais :

1. Cliquez sur l'onglet de tâches **Utilisateur relais**.
2. Développez la région appropriée de la vue arborescente **Utilisateurs** et sélectionnez un utilisateur relais dans la liste.
3. Cliquez sur le bouton **Suppression**.

Utilisation des commandes ivadmin policy pour la gestion des utilisateurs relais

L'utilitaire **ivadmin** propose des commandes de gestion des règles de sécurité spécialement adaptées aux utilisateurs relais de Policy Director. Ces commandes **ivadmin policy** permettent de gérer les règles générales applicables aux utilisateurs de Policy Director et aux utilisateurs relais. L'administrateur peut gérer les attributs de règle de sécurité suivants :

- «Gestion des règles de sécurité des connexions» à la page 119.
- «Gestion des règles de sécurité des mots de passe» à la page 119

Les règles de sécurité définissent les contraintes appliquées aux comptes utilisateur et aux mots de passe pour améliorer la sécurité globale du système. Ces contraintes peuvent s'imposer d'une manière générale (globalement à tous les utilisateurs présents dans le système) ou spécifique (uniquement à un utilisateur déterminé). Dans le cas de règles de sécurité spécifiquement appliquées à un utilisateur, ces règles sont prioritaires par rapport aux règles générales

éventuellement définies par ailleurs. Cette priorité s'applique, que les règles spécifiques soient plus restrictives que les règles générales ou non.

Gestion des règles de sécurité des connexions

Les commandes **ivadmin policy** suivantes permettent à l'administrateur du produit IBM SecureWay Boundary Server de gérer les règles de sécurité en relation avec les sessions de connexion.

Les tâches de gestion des règles de sécurité des connexions permettent de créer des règles de sécurité pour les connexions. Ces règles de sécurité s'appliquent à tous les utilisateurs.

S'agissant des tâches de gestion des règles de sécurité des connexions, Policy Director définit l'heure relative sous la forme JJJ-hh:mm:ss, et l'heure absolue sous la forme AAAA-MM-JJ-hh:mm:ss.

Commande	Description
policy {set | get} disable-time-interval [valeur]	

	Définit la durée (en secondes) pendant laquelle un compte doit être désactivé s'il atteint le nombre maximal de tentatives de connexion infructueuses autorisé.
	
	L'argument valeur définit cette durée en secondes.
	
	Exemples :
	`ivadmin> policy set disable-time-interval 3`
	
	Ou :
	`ivadmin> policy get disable-time-interval`

policy {set | get} max-login-failures [valeur]	

	Crée une nouvelle règle de sécurité, ou affiche une règle existante, déterminant le nombre maximal de tentatives de connexion infructueuses autorisé. Ce nombre est défini par l'argument valeur.
	
	Exemples :
	`ivadmin> policy set max-login-failures 5`
	
	Ou :
	`ivadmin> policy get max-login-failures`

Gestion des règles de sécurité des mots de passe

Les commandes **ivadmin policy** suivantes permettent à l'administrateur du produit IBM SecureWay Boundary Server de gérer les règles de sécurité en relation avec les mots de passe.

S'agissant des tâches de gestion des règles de sécurité des mots de passe, Policy Director définit l'heure relative sous la forme JJJ-hh:mm:ss.

Commande	Description
policy {set | get} max-password-age [heure relative]	

	Définit la durée maximale d'utilisation d'un mot de passe après laquelle son changement devient obligatoire. L'argument heure relative exprime cette durée en jours, heures et minutes selon le format `JJJ-hh:mm:ss`
	
	Exemples :
	`ivadmin> policy set max-password-age 031-08:30:00`
	
	Ou :
	`ivadmin> policy get max-password-age`

policy {set | get} max-password-repeated-chars [valeur]	

	Définit le nombre maximal de caractères pouvant être répétés à la suite dans un mot de passe d'utilisateur.
	
	Exemples :
	`ivadmin> policy set max-password-repeated-chars 3`
	
	Dans cet exemple, avec au plus trois caractères répétés, le mot de passe `deptfff` peut être adopté puisqu'il ne dépasse pas la limite de trois caractères "f" répétés. En revanche, le mot de passe `deptffff` ne peut pas être défini puisqu'il contient quatre caractères "f" alors que la limite est de trois.
	
	Ou :
	`ivadmin> policy get max-password-repeated-chars`

policy {set | get} min-password-alphas [valeur]	

	Définit le nombre minimal de caractères alphanumériques devant être contenus dans un mot de passe d'utilisateur.
	
	Exemples :
	`ivadmin> policy set min-password-alphas 5`
	
	Dans cet exemple, un mot de passe doit contenir au moins cinq caractères alphanumériques.
	
	Ou :
	`ivadmin> policy get min-password-alphas`

policy {set | get} min-password-non-alphas [valeur]	

	Définit le nombre minimal de caractères non alphanumériques pouvant être compris dans un mot de passe d'utilisateur.
	
	Exemples :
	`ivadmin> policy set min-password-non-alphas 1`
	
	Dans cet exemple, un mot de passe doit contenir au moins un caractère non alphanumérique.
	
	Ou :
	`ivadmin> policy get min-password-non-alphas`

policy {set | get} min-password-different-chars [valeur]	

	Définit le nombre minimal de caractères différents devant être compris dans un mot de passe d'utilisateur.
	
	Exemples :
	`ivadmin> policy set min-password-different-chars 3`
	
	Dans cet exemple, un mot de passe doit contenir au moins trois caractères différents. Si vous entrez le mot de passe `ddddyyyy`, celui-ci sera rejeté puisqu'il ne contient que deux caractères différents (d et y).
	
	Ou :
	`ivadmin> policy get min-password-different-chars`

policy {set | get} min-password-length [valeur]	

	Définit la longueur minimale, en caractères, d'un mot de passe. L'argument valeur indique cette longueur.
	
	Exemples :
	`ivadmin> policy set min-password-length 8`
	
	Ou :
	`ivadmin> policy get min-password-length`

policy {set | get} min-password-reuse-num [valeur]	

	Définit le nombre minimum de modifications d'un mot de passe avant qu'un ancien mot de passe puisse être réutilisé.
	
	Exemples :
	`ivadmin> policy set min-password-reuse-num 3`
	
	Ou :
	`ivadmin> policy get min-password-reuse-num`

policy {set | get} min-password-reuse-time [heure relative]	

	Définit le délai minimal avant réutilisation d'un mot de passe.
	
	L'argument heure relative exprime ce délai minimal en jours, heures et minutes dans le format (`JJJ-hh:mm:ss`). Selon cette règle, un utilisateur ne peut pas réutiliser le même mot de passe avant un délai déterminé (dans cet exemple, 60 jours ou `060-00:00:00`).
	
	Exemples :
	`ivadmin> policy set min-password-reuse-time 060-00:00:00`
	
	Ou :
	`ivadmin> policy get min-password-reuse-time`

policy {set | get} password-expiry-date [heure relative]	

	Définit la date et l'heure de l'expiration du mot de passe.
	
	Exemples :
	`ivadmin> policy set password-expiry-date 031-08:30:00`
	
	Ou :
	`ivadmin> policy get password-expiry-date`

policy {set | get} password-expiry-warn [valeur]	

	Définit le délai de préavis d'expiration du mot de passe. L'argument valeur indique le nombre de jours précédant la date d'expiration pendant lesquels les avertissements s'afficheront (par exemple, sur les quatre jours avant l'expiration du mot de passe).
	
	Exemples :
	
	`ivadmin> policy set password-expiry-warn 4`
	
	Ou :
	
	`ivadmin> policy get password-expiry-warn`

Chapitre 10. Gestion des serveurs de Policy Director

Ce chapitre détaille les tâches générales d'administration et de configuration des serveurs de Policy Director. Les fichiers de configuration de chaque serveur sont également décrits.

Ce chapitre comprend les sections suivantes :

Présentation des serveurs de Policy Director

Le serveur Policy Director met en oeuvre les processus (démons) de serveur suivants :

- Serveur de sécurité (secd)
- Gestionnaire de sécurité (secmgrd)
- Serveur d'autorisations (ivacld)
- Serveur de gestion (ivmgrd)
- Répartiteur des services de répertoire (RSR)

Ces serveurs se configurent automatiquement au cours de l'installation du produit.

Le **serveur de sécurité (secd)** de Policy Director est un serveur DCE exclusivement. Le serveur de sécurité fournit des services d'authentification et administre une base de données de registre centralisée. Le registre des utilisateurs peut être géré par un serveur LDAP ou DCE. Dans le deuxième cas, la base de données de registre centralisée contient les données des comptes de tous les utilisateurs membres du domaine sécurisé.

Le **gestionnaire de sécurité (secmgrd)** contient les serveurs de sécurité WebSEAL et NetSEAL.

Le **serveur d'autorisations (ivacld)** de Policy Director répond aux requêtes d'autorisation des applications tiers qui utilisent l'API d'autorisation de Policy Director en mode distant. Généralement, le serveur d'autorisations implique une configuration et une administration peu importantes.

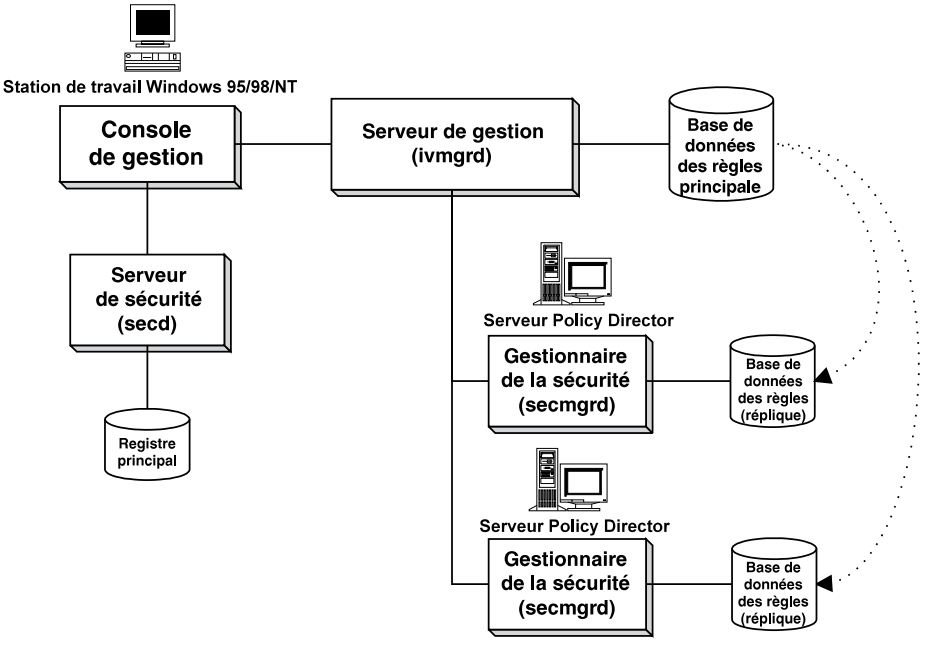
Le **serveur de gestion (ivmgrd)** administre la base de données primaire des LCA et gère les données d'emplacement des autres serveurs WebSEAL et NetSEAL du domaine sécurisé. Généralement, le serveur de gestion implique une configuration et une administration limitées.

Le **répartiteur des services de répertoire (RSR)** fait partie du progiciel du serveur de gestion (IVMgr). La console de gestion nécessite 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.

Conditions pour l'installation des serveurs

Les conditions requises pour l'installation des serveurs de Policy Director sont les suivantes :

- Un domaine sécurisé ne doit contenir qu'une seule instance du serveur de gestion et de la base de données primaire des autorisations (LCA).
- Le serveur de gestion duplique sa base de données des LCA pour tous les autres serveurs Policy Director du domaine sécurisé.
- Un gestionnaire de sécurité, avec demandes d'alerte WebSEAL et NetSEAL, réside sur chaque serveur Policy Director.
- Chaque gestionnaire de sécurité applique les règles de contrôle d'accès d'après les données d'une instance de la base de données des autorisations ou LCA.



Présentation générale des outils d'administration des serveurs

Les tâches d'administration de serveur s'effectuent au moyen des interfaces suivantes :

- L'utilitaire **ivadmin** ;
- L'utilitaire **wandmgr** (WebSEAL uniquement) ;
- Les scripts UNIX ;
- Le panneau de configuration des services Windows NT.

Ce chapitre décrit comment utiliser chacune de ces interfaces.

Les utilitaires **ivadmin**, **wandmgr**, et les scripts de démarrage, proposent des interfaces de ligne de commande. Ces interfaces permettent notamment d'automatiser les tâches d'administration de serveur dans des scripts shell.

La console de gestion et les utilitaires ivadmin et wandmgr peuvent être utilisés localement ou à distance. Les scripts de démarrage doivent être gérés localement.

Lors de la résolution d'incidents, les utilitaires de ligne de commande peuvent fournir des données d'état et permettent de contrôler individuellement les serveurs.

Utilitaire ivadmin

L'utilitaire de ligne de commande **ivadmin** permet de réaliser des tâches de gestion de serveur plus avancées. Vous pouvez utiliser **ivadmin** pour :

- conduire toutes les tâches de la console de gestion détaillées dans la section précédente ;
- afficher l'état des serveurs.

Utilitaire wandmgr

L'utilitaire de ligne de commande **wandmgr** est un outil de Policy Director WebSEAL qui permet de conduire des tâches avancées de gestion de la mémoire cache et d'autorisation des clients Web, notamment pour :

- afficher l'état des caches des objets Web ;
- supprimer de la mémoire les caches des objets Web.

Scripts UNIX

Policy Director utilise des scripts pour arrêter et démarrer automatiquement les serveurs pendant l'amorçage du système et pour afficher leur état. Vous pouvez exécuter ces scripts manuellement pour :

- arrêter des serveurs ;
- afficher l'état des serveurs ;
- démarrer des serveurs.

Panneau de configuration des services Windows NT

Utilisez le panneau de configuration des services Windows NT pour :

- démarrer un serveur ;
- arrêter un serveur ;
- suspendre un serveur ;
- relancer un serveur suspendu ;
- afficher la liste des serveurs configurés.

Fichiers de configuration des serveurs

Les serveurs Policy Director utilisent des fichiers de configuration pour assurer leur fonctionnement.

Nom du serveur	Processus	Fichier de configuration

Gestionnaire de sécurité	**secmgrd**	**UNIX :**
		`/opt/intraverse/secmgr/lib/secmgrd.conf`
		
		Windows :
		`\Program Files\ibm\Policy Director\secmgr\lib\secmgrd.conf`

Serveur de gestion	**ivmgrd**	**UNIX :**
		`/opt/intraverse/ivmgrd/lib/ivmgrd.conf`
		
		Windows :
		`\Program Files\ibm\Policy Director\ivmgrd\lib\ivmgrd.conf`

Serveur d'autorisations	**ivacld**	**UNIX :**
		`/opt/intraverse/ivacld/lib/ivacld.conf`
		
		Windows :
		`\Program Files\ibm\Policy Director\ivacld\lib\ivacld.conf`

Les fichiers de configuration sont des fichiers ASCII qui peuvent être modifiés à l'aide d'un éditeur de texte conventionnel. Les entrées de ces fichiers ont le format suivant :

```
paramètre=valeur
```

L'installation initiale d'un serveur Policy Director définit des valeurs par défaut pour la plupart des paramètres. Certains de ces paramètres sont statiques (ne changent pas) tandis que d'autres sont ajustés ou ajoutés pour configurer la fonctionnalité du serveur et optimiser ses performances.

Remarque : Après avoir modifié un fichier de configuration, vous devez arrêter le serveur Policy Director, puis le relancer pour activer les modifications.

Chaque fichier contient des sections, ou **strophes**, contenant des paramètres liés à un aspect spécifique de la configuration. Les étiquettes des strophes apparaissent entre crochets [ ].

Par exemple, la strophe `[intraverse]` que contient le fichier iv.conf définit les paramètres généraux de la configuration de Policy Director pour l'ensemble du domaine sécurisé. La strophe `[wand-mime-types]` contient les définitions des types MIME pris en charge par Policy Director WebSEAL sur le système local.

Chaque fichier contient des commentaires expliquant l'utilisation des différents paramètres. Si vous devez modifier des paramètres de configuration, éditez les fichiers comme il convient pour préserver leur intégrité.

UNIX : Démarrage et arrêt des serveurs Policy Director

Le démarrage et l'arrêt des processus de serveur se font généralement au moyen de scripts automatisés qui s'exécutent au moment de l'amorçage et de l'arrêt du système.

L'administrateur peut également utiliser des scripts pour démarrer ou arrêter les processus des serveurs. Cette technique s'apprécie notamment pour personnaliser une installation ou résoudre des incidents. Les scripts ne peuvent s'exécuter que sur une machine locale. Pour démarrer ou arrêter des serveurs à distance, vous devez utiliser la console de gestion ou l'utilitaire **ivadmin**.

Vous pouvez démarrer ou arrêter des serveurs Policy Director collectivement ou individuellement. En général, il convient de les démarrer et de les arrêter dans un ordre déterminé.

Le traitement des requêtes des services de répertoire de cellules (SRC) pour le compte de clients NetSEAT nécessite l'intervention du répartiteur des services de répertoire (RSR) (la version Windows de la console de gestion utilise le client NetSEAT).

Arrêt des serveurs par le script iv

Vous pouvez utiliser le script iv pour arrêter tous les serveurs Policy Director sur une machine donnée dans un ordre déterminé :

AIX :

```
# /etc/iv/iv stop
```

Solaris :

```
# /etc/init.d/iv stop
```

Ce script arrête les serveurs dans l'ordre suivant : ivacld, secmgrd, puis ivmgrd. Le script attend que tous les serveurs soient arrêtés avant de réafficher l'invite de ligne de commande.

Arrêt manuel

Les serveurs peuvent également être arrêtés individuellement à l'aide de la commande **kill** :

`# kill <pid>`	Oblige le serveur à s'arrêter une fois terminés les processus en cours.
`# kill -9 <pid>`	Oblige le serveur à s'arrêter instantanément.

Arrêtez les serveurs Policy Director dans l'ordre suivant :

1. Répartiteur des services de répertoire (RSR)
2. Serveur d'autorisations (ivacld)
3. Gestionnaire de sécurité (secmgrd)
4. Serveur de gestion (ivmgrd)

Démarrage des serveurs par le script iv

Vous pouvez utiliser le script iv pour démarrer tous les serveurs Policy Director sur une machine donnée dans un ordre déterminé :

AIX :

```
# /etc/iv/iv start
```

Solaris :

```
# /etc/init.d/iv start
```

Ce script démarre les serveurs dans l'ordre suivant : ivmgrd, secmgrd, puis ivacld. Le script attend que tous les serveurs aient démarré avant de réafficher l'invite de ligne de commande.

Démarrage manuel

Vous pouvez démarrer chaque serveur individuellement et directement. Dans une première phase, le serveur s'initialise lui-même, puis exécute son démon si l'initialisation réussit.

Notez que seul un utilisateur administrateur (root ou ivmgr) a le droit d'exécuter les commandes de lancement. Démarrez les serveurs Policy Director dans l'ordre suivant :

1. Serveur de gestion (ivmgrd) :
   ```
   # /opt/intraverse/ivmgrd/bin/ivmgrd
   ```
2. Gestionnaire de sécurité (secmgrd) :
   ```
   # /opt/intraverse/secmgr/bin/secmgrd
   ```
3. Serveur d'autorisations (ivacld) :
   ```
   # /opt/intraverse/ivacld/bin/ivacld
   ```
4. Répartiteur des services de répertoire (RSR) :
   ```
   # /opt/intraverse/broker/bin/dsb
   ```

Affichage de l'état des serveurs

Pour savoir si un serveur est actif, utilisez la commande suivante :

AIX :

```
# /etc/iv/iv status
```

Solaris :

```
# /etc/init.d/iv status

Serveurs DCE :
Serveur                     Activé                  Actif
dced                        yes                     yes
secd                        -                       yes
cdsd                        -                       yes
dtsd                        -                       yes
rsr                         -                       yes

Serveurs Policy Director :
Serveur                     Activé                  Actif
ivmgrd                      yes                     yes
secmgrd                     yes                     yes
ivacld                      yes                     yes
```

Windows : Démarrage et arrêt des serveurs Policy Director

Vous devez utiliser le panneau de configuration des services de Windows NT pour démarrer et arrêter les processus des serveurs manuellement. Cette technique s'apprécie notamment pour personnaliser une installation ou résoudre des incidents. Notez que vous devez détenir des privilèges d'administrateur pour employer cet utilitaire.

Vous pouvez démarrer ou arrêter des serveurs Policy Director collectivement ou individuellement. En général, il convient de démarrer et d'arrêter les serveurs dans un ordre déterminé.

Le service AutoStart de Policy Director démarre automatiquement chacun des serveurs de Policy Director lorsque vous réamorcez le système. Une fois les serveurs lancés, le service AutoStart s'arrête de lui-même.

Utilisez le panneau de configuration des services de Windows NT pour démarrer et arrêter individuellement et manuellement les serveurs Policy Director :

1. Ouvrez le panneau de configuration de Windows.
2. Cliquez deux fois de suite sur l'icône **Services**.

   La boîte de dialogue Services apparaît. Voici quelques-uns des services qui peuvent s'afficher :

   ```
   Service                                 Status          Startup
   Director Services Broker                Started         Automatic
   Policy Director Authorization Server    Started         Manual
   Policy Director Auto-Start Service      Started         Automatic
   Policy Director Management Server       Started         Manual
   Policy Director Security Manager        Started         Manual
   Policy Director X.509 Authorization Server  Started     Manual
   ```
3. Sélectionnez dans la liste les serveurs Policy Director selon l'ordre indiqué dans les étapes 4 et 5.
4. Arrêtez les serveurs dans l'ordre suivant :
   - Gestionnaire de sécurité
   - Serveur de gestion
   - Répartiteur des services de répertoire
5. Démarrez les serveurs dans l'ordre suivant :
   - Répartiteur des services de répertoire

- Serveur de gestion
- Gestionnaire de sécurité
- Serveur d'autorisations

6. Cliquez sur le bouton approprié parmi ceux proposé sur le côté droit de la fenêtre (**Démarrer, Arrêter, Démarrage**).
7. Pour empêcher le lancement automatique d'un serveur Policy Director par le service AutoStart, utilisez le bouton d'option **Démarrage**. Ce bouton affecte l'état Désactivé au serveur Policy Director sélectionné.

Automatisation du démarrage des serveurs à l'amorçage du système

La strophe [intraverse] du fichier de configuration iv.conf contient des paramètres qui déterminent si le lancement du serveur doit être automatisé ou non.

Lors de l'installation vous pouvez configurer le démon du serveur de sécurité (secmgrd) pour qu'il s'exécute automatiquement après chaque redémarrage du système.

```
[intraverse]
boot-start-secmgrd = yes
```

Pour empêcher le démarrage automatique de secmgrd, entrez :

```
boot-start-secmgrd
= no
```

Lors de l'installation du module IVMgr, le démon du serveur de gestion de Policy Director (ivmgrd) s'exécute automatiquement après chaque redémarrage du système.

```
[intraverse]
boot-start-ivmgrd = yes
```

Pour empêcher le démarrage automatique de ivmgrd, entrez :

```
boot-start-ivmgrd
= no
```

Remarque : Chaque domaine sécurisé (cellule) nécessite exactement un démon de serveur de gestion Policy Director. N'installez et n'exécutez pas **ivmgrd** sur plus d'un seul serveur par cellule.

Lors de l'installation du module IVAcld, le démon du serveur d'autorisations de Policy Director s'exécute automatiquement après chaque redémarrage du système.

```
[intraverse]
boot-start-ivacld = yes
```

Pour empêcher le démarrage automatique de **ivacld**, entrez :

```
boot-start-ivacld = no
```

Configuration des unités d'exécution d'agent RPC

Le nombre d'unités d'exécution d'agent configurées détermine le nombre de requêtes entrantes que le serveur peut satisfaire simultanément. Lorsque tous les agents sont occupés, Policy Director met en mémoire tampon les nouvelles demandes de connexion jusqu'à ce qu'une unité d'exécution d'agent se libère.

Vous pouvez définir le nombre d'unités d'exécution disponibles pour servir les connexions entrantes. Définissez ce nombre avec soin en raison des effets possibles sur les performances.

Les paramètres de configuration n'imposent pas de limite supérieure au nombre de connexions simultanées. Ils ne font que spécifier le nombre d'unités d'exécution mises à disposition pour traiter une file d'attente de travaux potentiellement illimitée.

Le nombre idéal d'unités d'exécution d'agent dépend de la quantité et du type des transactions intervenant dans votre réseau.

Plus ce nombre augmente, plus le temps moyen de traitement des requêtes est supposé diminuer. D'un autre côté, augmenter le nombre d'unités d'exécution accroît aussi la charge de travail du serveur et peut provoquer une augmentation de ce délai moyen.

Chacun des fichiers de configuration des serveurs secmgrd, ivmgrd et ivacld contient les paramètres suivants pour configurer les unités d'exécution d'agent RPC (appel de processus à distance) :

- Nombre maximum d'unités d'exécution d'agent RPC
- Port TCP utilisé pour l'écoute des RPC entrants
- Port UDP utilisé pour l'écoute des RPC entrants

Nom du serveur	Processus	Fichier de configuration
Gestionnaire de sécurité	**secmgrd**	secmgrd.conf
Serveur de gestion	**ivmgrd**	ivmgrd.conf
Serveur d'autorisations	**ivacld**	ivacld.conf

Définition du pool d'unités d'exécution d'agent RPC

Les serveurs Policy Director utilisent des unités d'exécution d'agent RPC pour traiter :

- les requêtes RPC entrantes des clients NetSEAT ;
- les mises à jour de base de données induites par les tâches administratives réalisées à partir de la console de gestion.

Le paramètre définissant le nombre maximum d'unités d'exécution d'agent RPC, contenu dans le fichier de configuration de chaque serveur, a la valeur par défaut suivante :

```
max-rpc-worker-threads = 10
```

Vous pouvez augmenter cette valeur lorsque le serveur Policy Director administre un grand nombre de clients NetSEAT.

Configuration des serveurs pour les requêtes RPC entrantes

Le tableau suivant présente les numéros et valeurs des ports définis par défaut pour chaque serveur, pour l'écoute des appels de processus à distance (RPC) entrants.

Serveur	Fichier de configuration	Paramètre de port et valeurs par défaut
secmgrd	secmgrd.conf	`rpc-tcp-port = 6052 rpc-udp-port = 0`
ivmgrd	ivmgrd.conf	`tcp-rpc-port = 6032 udp-rpc-port = 0`

ivacld	ivacld.conf	`tcp-rpc-port = 6031 udp-rpc-port = 0`

La valeur de port (0) désactive l'écoute des RPC sur le port concerné. Il est fortement recommandé d'utiliser l'écoute TCP. N'activez les ports UDP qu'en cas d'absolue nécessité.

Vous pouvez définir différents ports selon vos besoins.

Exemple pour secmgrd :

```
rpc-udp-port = 6052
```

Les protocoles TCP et UDP fonctionnent à présent sur le même port d'écoute.

Chapitre 11. Gestion du service d'autorisation

Le service d'autorisation de Policy Director met en application les règles de sécurité d'un réseau en contrôlant le processus de décision d'attribution des autorisations. Vous pouvez développer les possibilités d'autorisation de Policy Director de plusieurs manières : En définissant et en intégrant des espaces de noms supplémentaires, en définissant de nouveaux droits de contrôle d'accès ou en intégrant des services d'autorisation externes tiers. Ce chapitre détaille les tâches à accomplir pour configurer, administrer et développer le service d'autorisation de Policy Director.

Ce chapitre comprend les sections suivantes :

Définition d'espaces de noms d'application tiers

Les règles de sécurité d'un domaine sécurisé par Policy Director sont déterminées par les facteurs suivants :

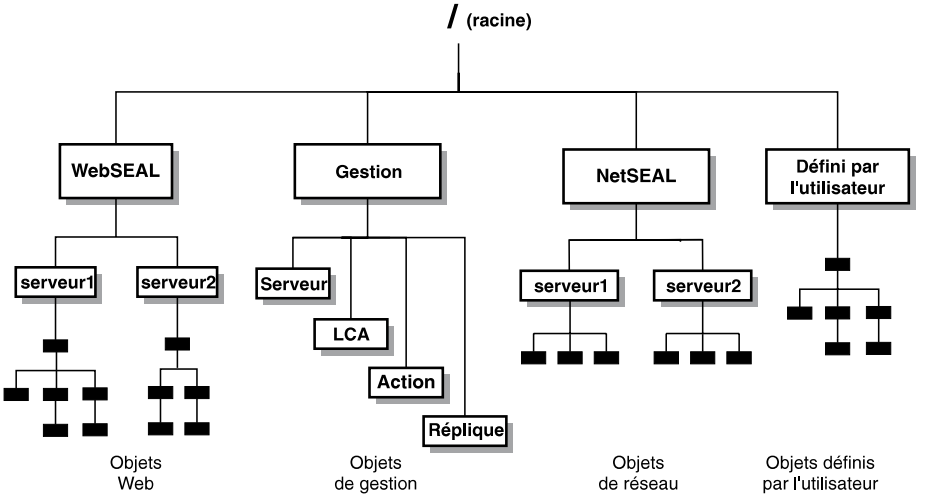
- Qui peut accéder au domaine sécurisé ?
- Quels objets doivent être protégés ?
- Quelles règles doivent protéger ces objets ?

L'espace des noms d'objet protégé de Policy Director est une représentation logique et hiérarchique des ressources du domaine sécurisé. Les objets contenus dans l'espace des noms représentent les ressources du système devant être protégées (par exemple, les fichiers et les ports). Pour protéger les ressources du domaine sécurisé, vous devez appliquer des modèles de règle, ou listes de contrôle d'accès, aux objets les représentant.

L'espace des noms d'objet protégé implique deux types d'objet :

Objets conteneurs
Les objets de type conteneur sont des désignations structurelles qui permettent d'organiser l'espace des noms de manière hiérarchique en plusieurs régions fonctionnelles. Les objets conteneurs peuvent contenir des objets de ressource.

Objets ressources
Les objets de ressource sont des représentations des véritables ressources du système (services, fichiers, programmes, etc.) affectées au domaine sécurisé.



Policy Director permet d'utiliser ses services d'autorisation pour protéger les objets appartenant à un espace de noms tiers. L'intégration d'un espace des noms tiers dans Policy Director nécessite les deux tâches suivantes :

- Définir l'espace des noms de l'application tiers dans Policy Director.
- Appliquer les modèles de règle (ou listes de contrôle d'accès) aux objets de l'espace des noms demandant une protection.

La description dans Policy Director du contenu d'un espace des noms tiers se fait au moyen d'un fichier de mappage spécial. Ce fichier répertorie les objets ressources appartenant à cet espace des noms et indique leur relation hiérarchique.

De plus, vous devez définir l'objet conteneur racine qui contient cet espace des noms tiers. Le nom de l'objet conteneur racine apparaîtra dans l'espace des noms de Policy Director lorsque vous l'afficherez au moyen de la console de gestion (onglet Espace objets). Les objets conteneurs standard de Policy Director comprennent /WebSEAL, /NetSEAL et /Management.

Le fichier de configuration du serveur de gestion (ivmgrd.conf) définit le nom de l'objet conteneur tiers et l'emplacement du fichier de mappage.

Nom de l'objet conteneur racine et emplacement du fichier de mappage

La strophe `[object-spaces]` du fichier de configuration du serveur de gestion (ivmgrd.conf) définit :

- le nom de l'objet conteneur racine de l'espace des noms tiers ;
- l'emplacement du fichier de mappage.

Chaque entrée a le format suivant :

```
racine de l'espace objets =
fichier de mappage
```

Où :

racine de l'espace objets — Nom de l'objet conteneur contenant l'espace des noms tiers.

fichier de mappage	Nom de chemin absolu du fichier de mappage. Le fichier de mappage peut être installé n'importe où.

L'exemple suivant définit un objet conteneur tiers appelé `Notes` et l'emplacement du fichier de mappage `notemap.txt` :

UNIX : `/Notes = /opt/intraverse/lib/notemap.txt`

Windows : `/Notes = C:\Program Files\IBM\Policy Director\lib\notemap.txt`

Remarque : Vous devez arrêter, puis redémarrer le serveur de gestion pour activer les modifications du fichier ivmgrd.conf.

Format du fichier de mappage

Le fichier de mappage, qui décrit l'espace des noms tiers, est un fichier texte ASCII. Chaque ligne du fichier contient un nom de chemin d'accès absolu correspondant à un objet ressource de l'espace des noms. Le fichier de mappage ne répertorie que les objets ressources ; Policy Director déduit les objets conteneurs d'après les noms de chemin.

Les autres règles régissant un fichier de mappage sont les suivantes :

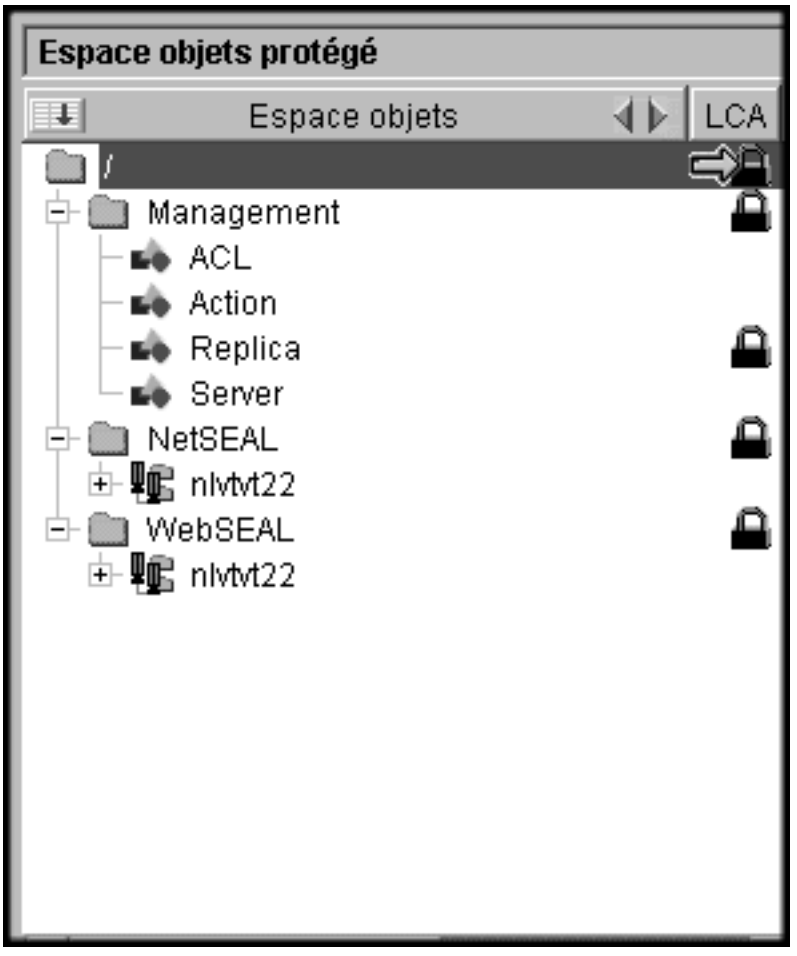
- Chaque ligne contient un seul objet et nom de chemin.
- Les noms de chemin des objets commencent toujours par une barre oblique (/).

Exemple de fichier de mappage

```
/Forum/public/courrier
/Forum/public/référence
/Forum/public/dialogue
/Forum/documents/style
/Forum/documents/guide
/Forum/documents/manuel
/Forum/privé/courrier
/Forum/privé/notes
/Forum/privé/bulletins
```

Affichage hiérarchique dans la console de gestion

La vue de la console de gestion suivante résulte du fichier de mappage pris comme exemple dans la section «Format du fichier de mappage».



Définition d'autorisations de LCA personnalisées

Policy Director utilise des modèles de règle pour spécifier les conditions requises pour exécuter une opération sur un objet protégé. Policy Director utilise un type de modèle de règle particulier appelé liste de contrôle d'accès (LCA).

Entrées de liste de contrôle d'accès

Vous avez la possibilité d'attacher une liste de contrôle d'accès à un objet. Une fois la LCA attachée, ses entrées déterminent quelles opérations Policy Director autorise sur cet objet et qui peut les réaliser. Une entrée de LCA comprend les éléments suivants :

- Le type user (utilisateur) ou group (groupe).

  Il existe encore deux autres types, unauthenticated et any-authenticated, qui correspondent respectivement aux utilisateurs non authentifiés et authentifiés par une méthode quelconque.
- L'identité unique (ID) de l'utilisateur ou du groupe.
- Les autorisations détenues.

Autorisations

Policy Director utilise un jeu d'autorisations standard qui couvre une large part des opérations possibles. Ces autorisations sont représentées sous la forme de caractères ASCII. Dans la console de gestion (onglet **LCA**), Policy Director affiche

chaque autorisation avec une étiquette qui décrit l'opération qu'elle gouverne. De plus, Policy Director regroupe les LCA dans des catégories selon leur utilisation (restreinte à une région spécifique de l'espace des noms ou permise dans l'ensemble de l'espace des noms). Ainsi les LCA peuvent appartenir à la catégorie des LCA de base, génériques, WebSEAL ou NetSEAL.

Opérations sur les objets

Les logiciels d'application impliquent souvent une ou plusieurs opérations sur des objets protégés. Ces applications font appel au service d'autorisation avant de lancer l'opération proprement dite. Cet appel s'effectue par le biais de l'API d'autorisation de Policy Director, pour Policy Director comme pour les applications tiers.

Les données de contrôle d'accès sont contenues dans la LCA qui protège l'objet. Le service d'autorisation se base sur ces informations pour répondre par `oui` ou `non` à la question : Cet utilisateur ou groupe a-t-il le droit de lire (par exemple) l'objet demandé ?

Il est important de noter que le service d'autorisation ignore tout de l'opération qui demande cette autorisation de lecture (r). Seule lui importe la présence (ou l'absence) de ce droit. L'autorisation de lecture (r pour read) est ou n'est pas mentionnée dans l'entrée de LCA liée à l'utilisateur ou au groupe à l'origine de la requête.

Cette fonction représente un aspect important du service d'autorisation de Policy Director. Le service est complètement indépendant des opérations demandées, ce qui explique pourquoi ses avantages peuvent être facilement étendus aux applications tiers.

Conditions de création des autorisations personnalisées

L'ensemble des autorisations standard de Policy Director peut être utilisé pour les applications tiers. Une application tiers peut également utiliser avec profit une autorisation Policy Director. Dans ce contexte, l'opération réalisée par l'application tiers devra être très proche de celle normalement conduite par Policy Director. Par exemple, une opération demandant un accès en lecture seule à un objet protégé ne doit utiliser que le droit de lecture (r).

Remarque : Une application tiers peut utiliser une autorisation standard de Policy Director pour une opération sans rapport, sans que quiconque le sache ou s'en préoccupe. Ceci n'est pas sans poser des difficultés à un administrateur qui désire distinguer deux usages distincts d'une même autorisation.

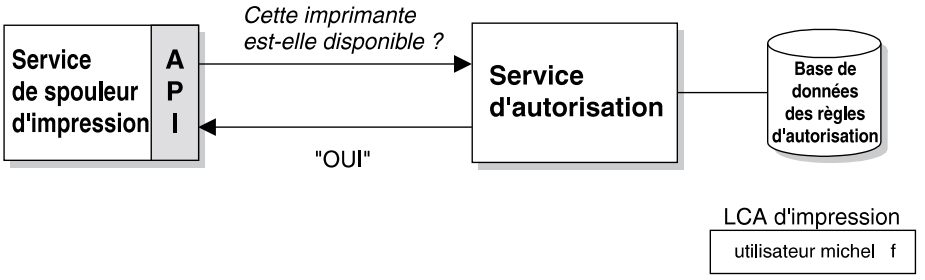
Une application tiers peut également exécuter une opération non prévue par le jeu d'autorisations standard. Dans ce contexte, Policy Director permet de définir une nouvelle autorisation. Cette application peut alors utiliser l'autorisation dans un but reconnu par le service d'autorisation.

Exemple :

L'objectif, dans cet exemple, est de protéger une imprimante contre une utilisation non autorisée. Un service de spoulage d'impression tiers est créé au moyen de l'API d'autorisation de Policy Director. Ce service de spoulage d'impression va appeler le service d'autorisation qui va contrôler les requêtes d'impression à l'aide des LCA.

Les autorisations standard de Policy Director ne comprennent pas d'autorisation pour la protection des imprimantes. La nouvelle autorisation d'impression créée dans cet exemple va donc protéger l'imprimante.

Une liste de contrôle d'accès est à présent attachée à l'objet de la ressource imprimante. Si un utilisateur demande à utiliser l'imprimante protégée, il doit figurer dans une entrée de LCA contenant aussi le droit d'impression. Si le service d'autorisation trouve son ID et cette autorisation, il retourne une réponse favorable et l'opération d'impression peut aboutir. Dans le cas contraire, la demande d'impression est rejetée.



Gestion des autorisations

En qualité d'administrateur de Policy Director, vous pouvez gérer les autorisations par les procédure suivantes :

- Ajout d'autorisations personnalisées
- Suppression d'autorisations personnalisées
- Affichage des autorisations existantes

Création d'une autorisation personnalisée

Les commandes **ivadmin action** permettent de créer, supprimer et afficher les autorisations. Vous devez être connecté en qualité d'administrateur Policy Director pour accéder à l'utilitaire **ivadmin**.

Utilisez la commande suivante pour créer une autorisation personnalisée :

```
ivadmin> action create nom description
type d'action
```

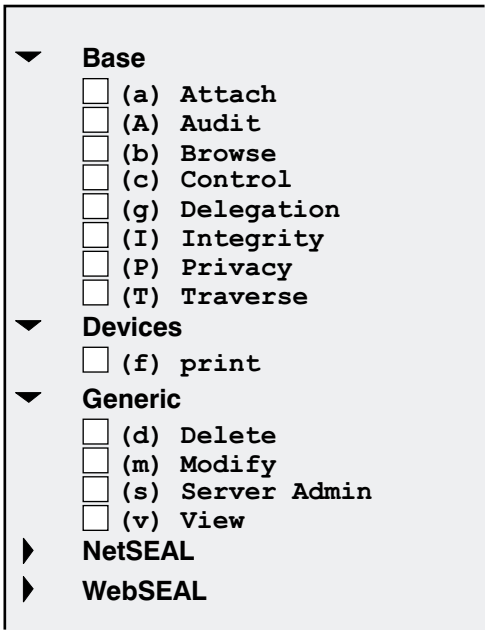
Où :

`nom`	Caractère ASCII représentant l'autorisation.
`description`	Etiquette descriptive apparaissant à la droite du caractère dans l'écran de la console de gestion (onglet LCA).
`type d'action`	Catégorie dans laquelle l'autorisation apparaît dans l'écran de la console de gestion (onglet LCA).

Par exemple, la commande :

```
ivadmin> action create f imprimante Unités
```

fait apparaître cette entrée dans le panneau de gestion des LCA de la console de gestion.



Suppression d'une autorisation personnalisée

Utilisez la commande suivante pour supprimer une autorisation personnalisée :

```
ivadmin> action delete nom
```

Par exemple :

```
ivadmin> action delete f
```

Affichage des autorisations existantes

Utilisez la commande suivante pour afficher la liste complète des autorisations existantes :

```
ivadmin> action list
```

La liste d'autorisations affichée peut ressembler à ceci :

```
p "Proxy" (relais) NetSEAL
r "Read" (lecture) WebSEAL
v "View" (affichage) Générique
x "Execute" (exécution) WebSEAL
A "Audit" (audit) Base
a "Attach" (attachement) Base
b "Browse" (navigation) Base
c "Control" (contrôle) Base
C "Connect" (connexion) NetSEAL
d "Delete" (suppression) Générique
f "Print" (impression) Unités
g "Delegation" (délégation) Base
I "Integrity" (intégrité) Base
l "List Directory" (liste) WebSEAL
m "Modify" (modification) Générique
P "Privacy" (confidentialité) Base
s "Server Admin" (administration de serveur) Générique
T "Traverse" (traversée) Base
...
```

Définition de services d'autorisation externes

Un service d'autorisation externe permet d'imposer des contrôles d'autorisation et des conditions supplémentaires pour compléter le processus d'autorisation standard de Policy Director. Un programme de serveur d'autorisations séparé administre ces contrôles et conditions supplémentaires.

Le service d'autorisation de Policy Director intègre automatiquement la fonction d'autorisation externe. Si vous configurez ce type de service, le service d'autorisation de Policy Director ajoute simplement les nouveaux contrôles et les nouvelles conditions à son processus d'évaluation.

La configuration d'un service d'autorisation externe implique les étapes suivantes :

1. Conception d'un programme de serveur pouvant être appelé au cours du processus de décision d'autorisation.

   Reportez-vous au manuel Policy Director - Guide de programmation et de référence.
2. Enregistrement du service d'autorisation externe dans le registre de Policy Director.

   Reportez-vous à la section «Enregistrement d'un service d'autorisation externe».

Une fois le service enregistré, un nouveau droit d'accès lui correspondant apparaît dans la console de gestion de Policy Director. Vous pouvez ensuite faire figurer ce droit d'accès dans une entrée de liste de contrôle d'accès.

Lorsque Policy Director rencontre ce droit d'accès au cours d'un contrôle d'autorisation, il appelle le service d'autorisation externe pour la prise de décision d'autorisation correspondante.

Pour plus d'informations, reportez-vous à la section «Fonction d'autorisation externe» à la page 50.

Enregistrement d'un service d'autorisation externe

La commande **ivadmin server register** informe le service d'autorisation de Policy Director de l'existence et de l'emplacement d'un service d'autorisation externe.

La syntaxe est la suivante :

```
ivadmin> server register externauth nom de serveur emplacement esp.noms
nom principal
         car. action nom action
```

Où :

nom de serveur	Nom (ou étiquette) du service d'autorisation externe. Ce nom apparaît dans l'écran de l'espace des objets dans la console de gestion et dans la commande ivadmin server list.
emplacement espace de noms	Entrée RPC de l'espace des noms du SRC dans laquelle le serveur d'autorisation externe exporte ses liaisons RPC.
nom principal	Nom LDAP ou nom de principal DCE associé au processus du serveur d'autorisation externe.
caractère de l'action	Caractère d'autorisation utilisé dans une liste de contrôle d'accès pour contrôler l'utilisation de ce service d'autorisation externe pour les décisions d'autorisation externe.
nom de l'action	Etiquette descriptive apparaissant à la droite du caractère dans l'écran de la console de gestion (onglet LCA).

Cette commande génère une catégorie de LCA par défaut appelée autorisation externe (external authorization). La console de gestion utilise la catégorie de LCA par défaut lors de l'affichage des listes de contrôle d'accès. Les autorisations définies pour tous les services d'autorisation externes apparaissent dans cette catégorie.

Par exemple, la commande :

```
ivadmin> server register externauth
timechecker /.:/subsys/timechk
         t-checker k time-check
```

enregistre un serveur d'autorisation externe nommé `timechecker` dans le service d'autorisation. L'entrée RPC de l'espace des noms du SRC dans lequel timechecker exporte ses liaisons RPC est `/.:/subsys/timechk`. Le nom de principal de DCE affecté au serveur est `t-checker`. L'autorisation associée à ce service est le droit de contrôle d'heure ″k″ (time-check).

L'autorisation définie pour ce serveur d'autorisation externe apparaît dans la console de gestion sous l'aspect suivant :

```
Base
  (a) Attach (attachement)
  (A) Audit (audit)
  (b) Browse (navigation)
  (c) Control (contrôle)
  (g) Delegation (délégation)
  (I) Integrity (intégrité)
  (P) Privacy (confidentialité)
  (T) Traverse (traversée)
Générique
  (k) time-check (contrôle horaire)
Générique
  (d) Delete (suppression)
  (m) Modify (modification)
  (s) Server Admin (administration de serveur)
  (v) View (affichage)
NetSEAL
WebSEAL
```

Suppression d'un serveur d'autorisation externe

Utilisez la commande **ivadmin server delete** pour supprimer un service d'autorisation externe enregistré. La syntaxe est la suivante :

```
ivadmin> server delete /ExternAuthzn/nom de serveur
```

Où :

`nom de serveur`	Nom (ou étiquette) du service d'autorisation externe. Ce nom apparaît dans l'écran de l'espace des objets dans la console de gestion.

Par exemple :

```
ivadmin> server delete /ExternAuthzn/timechecker
```

Exemple 1 :

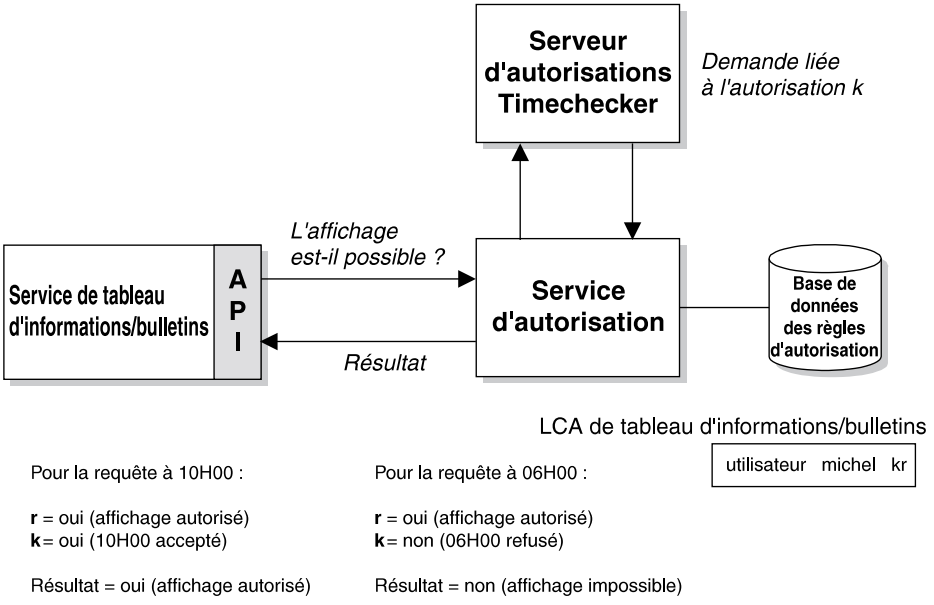
Les opérations d'un service tiers de tableau d'informations et de bulletins sont soumises à des contraintes horaires. Les utilisateurs peuvent visualiser les

informations proposées par ce service entre 08h00 et 17h00 exclusivement. Un service d'autorisation externe est créé pour vérifier l'heure des requêtes adressées au service d'informations.

Utilisez la commande **ivadmin** pour créer le service d'autorisation externe.

L'illustration qui suit met en évidence les différentes formes que peut prendre le processus d'autorisation. L'utilisateur doit détenir le droit de lecture pour afficher le tableau d'informations et les bulletins. La LCA attachée au service d'informations contient également le droit de contrôle horaire (k). Le droit de contrôle horaire (k) indique au service d'autorisation de Policy Director qu'il doit se reporter au serveur d'autorisations externe Timechecker pour la décision finale.

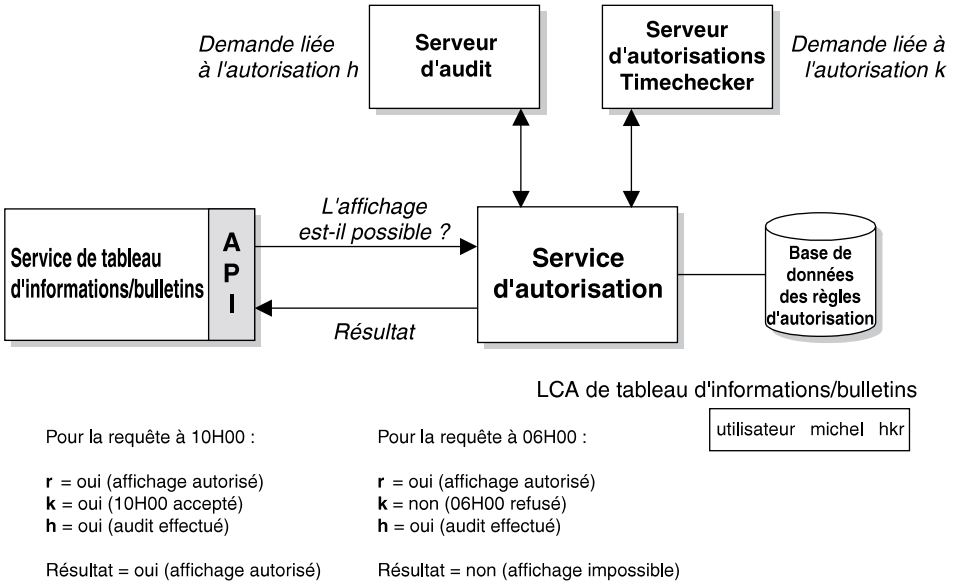
Policy Director base sa décision finale d'accorder ou non l'autorisation sur la somme des décisions prises par l'ensemble des serveurs d'autorisations consultés.



Exemple 2 :

Dans cet exemple proche du premier, un deuxième service d'autorisation externe contrôle l'activité du service d'informations.

Notez que si le service d'autorisation Timechecker refuse l'affichage, l'audit de l'activité se fait quand même. La présence de l'autorisation **h** (avec ″yes″) déclenche l'audit du serveur d'autorisations pendant le contrôle de LCA.



Administration du serveur de gestion

Le serveur de gestion (ivmgrd) de Policy Director administre la base de données primaire des règles d'autorisation. Il gère également les données d'emplacement des autres serveurs WebSEAL et NetSEAL du domaine sécurisé. Généralement, le serveur de gestion implique une configuration et une administration limitées. Cette section détaille les tâches confiées à l'administrateur.

Définition du nombre d'unités d'exécution de notification de mise à jour

Le serveur de gestion (ivmgrd) gère la base de données primaire des règles d'autorisation. Le gestionnaire de sécurité (secmgrd) et le serveur d'autorisations (ivacld) sont responsables de la duplication de la base de données primaire.

La synchronisation de toutes les instances de la base de données présentes dans le domaine sécurisé est du ressort du serveur de gestion. Lorsque la base de données primaire est mise à jour, des unités d'exécution notifient le changement à toutes ses instances. Chacune d'elle peut alors télécharger les nouvelles données de la base de données primaire.

Le fichier de configuration du serveur de gestion, ivmgrd.conf, contient un paramètre qui permet de définir le nombre maximum d'unités d'exécution de notification de mise à jour. Ce pool d'unités d'exécution permet de notifier simultanément la mise à jour à toutes les instances de la base de données primaire.

Par exemple, pour notifier une mise à jour de la base de données primaire à 30 instances, définissez un pool d'au moins 30 unités d'exécution. S'il existe plus de 30 instances de la base de données, un deuxième lot de notifications s'exécute (dans cet exemple, 30 à la fois). Toutes les instances reçoivent la notification, quelque soit la valeur de ce paramètre.

Le nombre d'unités d'exécution choisi doit conduire à notifier la mise à jour aux instances le plus rapidement possible. En général, on choisit une valeur égale au nombre d'instances de la base de données primaire. Le simple fait de définir cette

valeur crée l'avantage de voir un unique pool d'unités d'exécution simultanément notifier la mise à jour à toutes les instances.

La valeur définie par défaut est :

```
[ivmgrd]
max-notifier-threads = 10
```

Chapitre 12. Journalisation et audit de l'activité du serveur

Policy Director propose un certain nombre de fonctions d'audit et de journalisation. Des fichiers journaux consignent les messages d'erreur et d'avertissement générés par les serveurs Policy Director et les serveurs DCE (environnement informatique partagé). De plus, des fichiers d'audit permettent de suivre l'activité de Policy Director et des serveurs DCE.

Ce chapitre comprend :
- une présentation générale des principes de la journalisation et de l'audit ;
- une explication de chaque type de fichier journal ;
- une explication de chaque type de fichier d'audit.

Présentation générale de la journalisation et de l'audit

Le contenu des fichiers journaux et des fichiers d'audit peut constituer une source d'informations appréciable. Ils permettent notamment de surveiller les activités des serveurs du DCE et de Policy Director, de rechercher l'origine des incidents et de les résoudre.

Fichiers journaux

Les serveurs DCE et Policy Director utilisent des fichiers journaux pour stocker les messages d'erreur et d'avertissement. Tous les fichiers journaux sont au format texte.

Policy Director utilise les fichiers journaux suivants :
- Fichiers journaux des serveurs Policy Director

  Reportez-vous à la section «Fichiers journaux des serveurs Policy Director» à la page 146.
- Fichiers journaux des serveurs DCE

  Reportez-vous à la section «Fichiers journaux des serveurs DCE» à la page 147.
- Messages de mise en service DCE

  Reportez-vous à la section «Messages de mise en service DCE» à la page 147.
- Fichiers journaux HTTP standard

  Reportez-vous à la section «Journalisation HTTP standard» à la page 148.

Fichiers d'audit

Les serveurs DCE et Policy Director utilisent des fichiers d'audit pour stocker les rapports d'activité des serveurs. Le terme rapport désigne la sortie d'un événement de serveur. Un fichier d'audit regroupe plusieurs rapports fournissant des informations sur l'activité du serveur. La plupart des fichiers d'audit sont au format ASCII. Les fichiers d'audit des serveurs DCE sont, pour leur part, au format binaire. Pour visualiser le contenu de ces fichiers, utilisez l'utilitaire **dcecp**.

Les fichiers d'audit qui suivent fournissent des informations sur les événements en rapport avec l'activité des serveurs DCE et Policy Director :
- Fichier d'audit des trois serveurs Policy Director suivants (audit.log) :
  - Serveur de gestion (ivmgrd)
  - Gestionnaire de sécurité (secmgrd)
  - Serveur d'autorisations (ivacld)

Reportez-vous à la section «Fichiers d'audit des autorisations de Policy Director» à la page 151.

- Fichier d'audit de WebSEAL (wand_audit_log)

  Reportez-vous à la section «Fichier d'audit de WebSEAL» à la page 154.
- Fichier d'audit des activités de gestion de Policy Director

  Reportez-vous à la section «Fichier d'audit des commandes de gestion de Policy Director» à la page 155.
- Fichiers d'audit DCE

  Reportez-vous à la section «Fichiers d'audit des serveurs DCE» à la page 157.

Convention d'usage de la variable chemin_installation

La variable chemin_installation utilisée tout au long de ce chapitre s'interprète de la manière suivante selon les systèmes d'exploitation :

UNIX :

```
/opt/intraverse/
```

Windows :

```
C:\Program Files\IBM\
```

UNIX ne permet pas de modifier ce nom de chemin qui reste invariable.

Windows permet de définir la valeur de la variable chemin_installation pendant l'installation du logiciel Policy Director.

Fichiers journaux des serveurs Policy Director

Chaque serveur Policy Director génère des messages d'erreur et d'avertissement qui sont dirigés vers la sortie d'erreur standard, puis enregistrés dans des fichiers journaux définis.

Serveur	Processus	Emplacement du fichier journal
Serveur de gestion	**ivmgrd**	Défini dans ivmgrd.conf : log-file=*chemin_installation*/ivmgrd/log/ivmgrd.log
Gestionnaire de sécurité	**secmgrd**	Défini dans secmgrd.conf: log-file=*chemin_installation*/secmgr/log/secmgrd.log
Serveur d'autorisations	**ivacld**	Défini dans ivacld.conf : log-file=*chemin_installation*/ivacld/log/ivacld.log
Répartiteur des services de répertoire	**nsid**	*chemin_installation*/broker/nsid.log

Activation et désactivation des fichiers journaux des serveurs

Policy Director active la journalisation dès lors qu'un fichier journal a été défini dans le fichier de configuration.

Exemple de secmgrd.log

Le contenu du fichier secmgrd.log a l'aspect suivant :

```
1998-09-22-21:56:36.898-04:00I----- secmgrd FATAL ivc general
exec.c 344 0x00000006
Détecté signal (15)
1998-09-22-21:56:37.309-04:00I----- secmgrd ERROR ivc rpc
```

```
IVServer.cpp 1039 0x00000001
Impossible d'annuler l'exportation des liaisons vers le serveur de noms
(/.:/subsys/ibm/secmgr/server/sun,0x16c9a093
1998-09-22-21:56:37.354-04:00I----- secmgrd ERROR ivc rpc
IVServer.cpp 1048 0x00000001
Impossible d'annuler l'enregistrement des extrémités RPC (0x16c9a042)
```

Fichiers journaux des serveurs DCE

Chaque serveur DCE génère des messages d'erreur et d'avertissement qui sont dirigés vers la sortie d'erreur standard, puis enregistrés dans des fichiers journaux définis. Ces fichiers journaux peuvent constituer une précieuse source d'informations lors de la recherche de l'origine d'un incident.

Les fichiers journaux des serveurs DCE comprennent :

Serveur de sécurité :

UNIX : `/opt/dcelocal/var/security/secd.log`

Windows : `\Program Files\IBM\dcelocal\var\security\secd.log`

Serveur DCE :

UNIX : `/opt/dcelocal/var/dced/dced.log`

Windows : `\Program Files\IBM\dcelocal\var\dced\dced.log`

Messages de mise en service DCE

Le fichier de routage contrôle les messages de mise en service du DCE :

UNIX : `/opt/dcelocal/var/svc/routing`

Windows : `\Program Files\IBM\NetSEAT\var\svc\routing`

Remarque : Pour les systèmes Windows, le chemin d'installation peut être défini pendant l'installation : `\Program Files\IBM\NetSEAT\`. La variable d'environnement (%NETSEAT%) prend la valeur du chemin défini.

Entrées par défaut du fichier de routage

Les entrées de ce fichier de configuration déterminent le type d'informations journalisées. Le fichier de routage contient les entrées par défaut suivantes :

UNIX :

```
FATAL:STDERR:-;FILE:/opt/dcelocal/var/svc/fatal.log
ERROR:STDERR:-;FILE:/opt/dcelocal/var/svc/error.log
WARNING:STDERR:-;FILE:/opt/dcelocal/var/svc/warning.log
```

Windows :

```
FATAL:STDERR:-;FILE:%NETSEAT%\var\svc\fatal.log
ERROR:STDERR:-;FILE:%NETSEAT%\var\svc\error.log
WARNING:STDERR:-;FILE:%NETSEAT%\var\svc\warning.log
```

Les messages de type NOTICE fournissent des informations supplémentaires sur l'activité du serveur. Par défaut, Policy Director n'active pas (aucune entrée n'existe dans le fichier) les messages NOTICE.

Pour activer les messages NOTICE (et les diriger vers la sortie d'erreur standard), ajoutez la ligne NOTICE suivante à la fin du fichier de routage.

UNIX :

```
FATAL:STDERR:-;FILE:/opt/dcelocal/var/svc/fatal.log
ERROR:STDERR:-;FILE:/opt/dcelocal/var/svc/error.log
WARNING:STDERR:-;FILE:/opt/dcelocal/var/svc/warning.log
NOTICE:STDERR:-;FILE:/opt/dcelocal/var/svc/notice.log
```

Windows :

```
FATAL:STDERR:-;FILE:%NETSEAT%\var\svc\fatal.log
ERROR:STDERR:-;FILE:%NETSEAT%\var\svc\error.log
WARNING:STDERR:-;FILE:%NETSEAT%\var\svc\warning.log
NOTICE:STDERR:-;FILE:%NETSEAT%\var\svc\notice.log
```

Mode de débogage pour l'acheminement des messages vers la sortie standard

En principe, Policy Director réoriente les messages d'erreur et d'avertissement, ceci comprenant les messages NOTICE, vers les fichiers journaux appropriés.

Pour envoyer ces messages vers la sortie standard (le terminal), utilisez l'option de commande **-debug** lors du démarrage d'un serveur. Cette option permet d'exécuter le programme serveur en avant-plan (le démon du serveur ne s'exécute pas). Policy Director envoie les messages d'erreur et d'avertissement vers la sortie standard.

Par exemple, pour démarrer le gestionnaire de sécurité (secmgrd) en mode débogage, utilisez la commande suivante :

```
# /opt/intraverse/secmgr/bin/secmgrd -debug
```

Vous pouvez également utiliser la commande UNIX **tee** pour enregistrer la sortie du serveur dans un fichier.

L'exemple suivant illustre comment démarrer le gestionnaire de sécurité de Policy Director dans ce mode :

```
# secmgrd -debug 2>&1 | tee /tmp/secmgrd.log
```

Remarques sur le débogage

Lors d'un débogage, n'oubliez pas les aspects suivants :

1. Une fois obtenues les informations relatives à l'activité du serveur, n'oubliez pas de restaurer le fichier de routage dans son état initial. Supprimez notamment l'entrée NOTICE. L'entrée NOTICE génère une grande quantité d'informations qui peuvent rapidement s'accumuler.
2. Vous pouvez utiliser la combinaison de touches **Ctrl + c** pour arrêter un processus de serveur lancé en mode débogage. Le processus de serveur s'arrête.

Journalisation HTTP standard

Le serveur WebSEAL Policy Director administre également trois fichiers journaux HTTP conventionnels qui consignent l'activité plutôt que les messages :

wand_request_log

Reportez-vous à la section «Affichage du fichier journal wand_request_log» à la page 150.

wand_agent_log
Reportez-vous à la section «Affichage du fichier journal wand_agent_log» à la page 151.

wand_referer_log
Reportez-vous à la section «Affichage du fichier journal wand_referer_log» à la page 151.

Par défaut, Policy Director enregistre ces fichiers journaux dans le répertoire suivant :

UNIX : `/opt/intraverse/www/log`

Windows : `\Program Files\IBM\Policy Director\www\log`

Configuration de la journalisation HTTP standard

La strophe `[wand]` du fichier de configuration iv.conf contient des paramètres qui déterminent la configuration de la journalisation HTTP standard.

Le tableau suivant illustre la relation entre les fichiers journaux HTTP et les paramètres du fichier de configuration.

Fichiers journaux	Paramètre d'emplacement	Paramètre d'activation/désactivation (= yes ou no)
wand_request_log	reqlog =	logreqs =
wand_referer_log	reflog =	logrefs =
wand_agent_log	agentlog =	logagents =

Par exemple, l'entrée du fichier iv.conf définissant l'emplacement par défaut du fichier **wand_request_log** se présente comme suit :

```
reqlog = log/wand_request_log
```

Le répertoire racine de cet emplacement est :

UNIX : `/opt/intraverse/www/`

Windows : `\Program Files\IBM\Policy Director\www\`

Activation et désactivation de la journalisation HTTP

Par défaut, Policy Director active tous les fichiers de journalisation HTTP :

```
[wand]
logreqs = yes
logrefs = yes
logagents = yes
```

Pour désactiver la journalisation, entrez :

```
<paramètre d'activation> = no
```

Définition du type d'horodate

Les horodates apparaissant dans les fichiers journaux peuvent s'exprimer en temps GMT (Greenwich Mean Time) au lieu du temps local. Par défaut, Policy Director utilise l'heure locale.

```
[wand]
loggmttime = no
```

Pour utiliser des horodates GMT, entrez :

```
loggmttime = yes
```

Remarque : La synchronisation horaire des fichiers journaux et des fichiers d'audit des applications liées à la sécurité facilite leur lecture.

Définition de la taille maximale d'un fichier journal

La taille maximale des fichiers journaux HTTP est définie par défaut :

```
[wand]
logsize = 2000000
```

Policy Director crée une sauvegarde du fichier journal lorsque celui-ci atteint cette taille.

Notez que ce paramètre s'applique également au fichier d'audit de Policy Director **wand_audit_log**.

Vérifiez régulièrement la taille des fichiers journaux pour qu'ils ne deviennent pas trop volumineux. Archivez-les à l'occasion des opérations de maintenance périodique du système.

Utilisation du format de fichier journal HTTP standard

Chaque réponse (réussite ou échec) renvoyée par le serveur Policy Director est enregistrée dans une entrée d'une ligne dans le format de fichier journal HTTP standard suivant :

```
hôte - utilisateur
[date] requête état octets
```

Où :

hôte	Adresse IP (protocole Internet (IP))) de la machine adressant la requête.
utilisateur	Valeur de l'en-tête **From :** (De :) de la requête HTTP réceptionnée. En outre, ce champ contient aussi une requête RPC sécurisée en définissant la valeur sur `dce-rpc`. Ce champ reste vide dans le cas d'un utilisateur non authentifié.
date	Date et heure de la requête.
requête	Première ligne de la requête telle qu'elle a été transmise par le client.
état	Code d'état HTTP renvoyé à la machine ayant adressé la requête.
octets	Nombre d'octets renvoyés à la machine ayant adressé la requête (autrement dit, la longueur du document renvoyé).

Affichage du fichier journal wand_request_log

Le fichier wand_request_log assure la journalisation standard des requêtes HTTP. Sont notamment journalisées les données des URL demandées et celles du client (par exemple, son adresse IP) à l'origine de la requête.

Le contenu du fichier wand_request_log a l'aspect suivant :

```
130.105.1.90 - - [Tue, 23 Apr 1996 17:23:33 EDT]
  "GET /~smith/private_html/ HTTP/1.0" 403 77
130.105.1.90 - - [Tue, 23 Apr 1996 17:23:47 EDT]
  "GET /icons HTTP/1.0" 302 93
130.105.1.90 - - [Tue, 23 Apr 1996 17:23:59 EDT]
  "GET /icons/ HTTP/1.0" 403 77
130.105.1.90 - - [Tue,  23 Apr 1996 17:24:04 EDT]
  "GET /~smith/private_html/ HTTP/1.0" 403 77
```

```
130.105.1.90 - - [Tue, 23 Apr 1996 17:24:11 EDT]
  "GET /~smith/ HTTP/1.0" 403 77
dce-rpc - - [Tue, 23 Apr 1996 17:24:51 EDT]
  "GET / HTTP/1.0" 200 919
```

Affichage du fichier journal wand_agent_log

Le fichier wand_agent_log enregistre le contenu de l'en-tête `User_Agent :` de la requête HTTP. Ce fichier journal contient des informations sur le navigateur (architecture, numéro de version, etc.) utilisé pour chaque requête.

L'exemple suivant donne un aperçu du contenu d'un fichier wand_agent_log :

```
Mozilla/4.01 [en] (WinNT; U)
Mozilla/4.01 [en] (WinNT; U)
Mozilla/4.01 [en] (WinNT; U)
Mozilla/4.01 [en] (WinNT; U)
```

Affichage du fichier journal wand_referer_log

Le fichier wand_referer_log enregistre l'en-tête principal de la requête HTTP. Pour chaque requête, le fichier journal consigne le document qui contenait le lien au document demandé.

Le fichier journal utilise le format suivant :

```
référent ->
objet
```

Ces informations permettent de surveiller les liens renvoyant aux documents de votre espace Web. Le fichier journal révèle que la source désignée par `référent` contient un lien à un objet page. Ceci permet de repérer les liens obsolètes et de savoir qui crée des liens renvoyant à vos documents.

L'exemple suivant donne un aperçu du contenu d'un fichier wand_referer_log :

```
http://manuel/maybam/index.html -> /pics/ibm_logo.gif
http://manuel/maybam/ivdl/index.html -> /pics/ibm_logo.gif
http://manuel/maybam/ -> /ivdl/index.html
http://manuel/maybam/ -> /ivdl/index.html
http://manuel/maybam/ivdl/index.html -> /pics/ibm_logo.gif
http://manuel/maybam/ -> /ivdl/index.html
```

Fichiers d'audit des autorisations de Policy Director

Chaque serveur Policy Director peut consigner des événements contrôlables lorsqu'une opération de sécurité pouvant être auditée intervient. Policy Director enregistre ces événements contrôlables sous la forme d'un rapport d'audit qui renseigne sur les opérations conduites. Une fois réunis, ces rapports d'audit constituent le fichier d'audit proprement dit.

Le tableau suivant illustre la relation entre chaque serveur Policy Director et son fichier d'audit :

Serveur	Processus	Fichier d'audit des autorisations
Serveur de gestion	**ivmgrd**	Défini dans ivmgrd.conf : audit-file= *chemin_installation*/ivmgrd/log/audit.log
Gestionnaire de sécurité	**secmgrd**	Défini dans secmgrd.conf : authzn-audit-file= *chemin_installation*/secmgr/log/audit.log
Serveur d'autorisations	**ivacld**	Défini dans ivacld.conf : audit-file= *chemin_installation*/ivacld/log/audit.log

Policy Director enregistre les données des autorisations dans le fichier d'audit approprié chaque fois que vous accordez le droit d'audit (A) à un utilisateur ou un groupe dans une liste de contrôle d'accès. Toutes les tentatives d'accès sont consignées même si elles échouent.

Administration des fichiers d'audit

Le droit d'audit (A) contenu dans une entrée de LCA déclenche l'enregistrement des données d'activité de Policy Director dans les fichiers d'audit. L'activation du processus d'audit par le biais du droit d'audit est facile à réaliser.

La gestion des fichiers d'audit d'autorisation doit répondre aux conditions suivantes :

- L'objet auquel la LCA est attachée détermine lequel des trois fichiers audit.log consigne les données.

  Par exemple, vous pouvez attacher la liste de contrôle d'accès contenant le droit d'audit dans une ou plusieurs entrées à l'objet /Management de l'espace des noms d'objet protégé. Dans ce cas, les données seront consignées dans le fichier audit.log associé au serveur de gestion (ivmgrd). Le serveur de gestion contrôle la base de données des règles d'autorisation (LCA) et sa duplication (les répliques).
- Les informations relatives aux opérations ne sont consignées que pour les utilisateurs et/ou les groupes lorsque vous définissez le droit d'audit (A) dans les entrées de LCA appropriées.

  Par exemple, vous pouvez associer ce droit à une entrée unauthenticated dans une liste de contrôle d'accès attachée à une page HTML. Avec ce droit, le fichier audit.log du gestionnaire de sécurité collecte des données sur toutes les tentatives d'accès à l'objet ayant été rejetées.

Exemple : La liste de contrôle d'accès suivante représente la LCA default-webseal. L'entrée de l'utilisateur `cell_admin` et l'entrée `unauthenticated` accordent le droit d'audit (A).

```
user cell_admin                 aAbcTdmlrx
group iv-admin                  abdTdmlrx
group ivmgrd-servers            Tl
group webseal-servers           gTdmlrx
any-authenticated               Tr
unauthenticated                 ATr
```

Attacher une LCA à l'objet /WebSEAL signifie plus précisément l'appliquer à la racine de la région WebSEAL de l'espace des noms d'objet protégé. Dans cette

situation, Policy Director enregistrera dans le journal d'audit audit.log du gestionnaire de sécurité les opérations impliquant ce serveur (WebSEAL et NetSEAL).

Si l'espace des noms de WebSEAL ne contient pas d'autres listes de contrôle d'accès explicites modifiant les conditions d'autorisation, l'audit couvrira toutes les requêtes, quelque soit l'objet de l'espace Web qu'elles concernent.

Le fichier d'audit enregistre exclusivement les opérations déclenchées par l'utilisateur cell_admin et les tentatives d'accès non authentifiées.

Toute liste de contrôle d'accès explicite appliquée sous l'objet /WebSEAL aura pour effet de rompre la chaîne d'héritage de LCA. Si les entrées de cette LCA explicite ne contiennent pas de droits d'audit, le processus d'audit ne couvrira pas l'objet associé, ni ceux hiérarchiquement inférieurs.

Remarque : Vous devez impérativement spécifier le droit d'audit dans les entrées appropriées des listes de contrôle d'accès explicitement attachées aux objets situés sous l'objet /WebSEAL dans la hiérarchie si vous voulez couvrir ces objets.

Exemple de fichier d'audit de serveur de gestion

Le contenu d'un fichier d'audit de serveur de gestion a l'aspect suivant :

```
START RECORD
  Objet protégé : /WebSEAL
  Autorisations demandées : 0x00000100
  Principaux :
principal 0: principal DCE 00000064-35ee-21d2-a000-0800207b48c5
niveau de protection : aucun    résultat : autorisé
END RECORD

START RECORD
  Objet protégé : /WebSEAL/sun
  Autorisations demandées : 0x00000100
  Principaux :
principal 0: principal DCE 00000064-35ee-21d2-a000-0800207b48c5
niveau de protection : aucun    résultat : autorisé
END RECORD

START RECORD
  Objet protégé : /WebSEAL/sun/icons
  Autorisations demandées : 0x00000100
  Principaux :
principal 0: principal DCE 00000064-35ee-21d2-a000-0800207b48c5
niveau de protection : aucun    résultat : autorisé
END RECORD

START RECORD
  Objet protégé : /WebSEAL
  Autorisations demandées : 0x00000100
  Principaux :
principal 0: principal DCE 00000064-35ee-21d2-a000-0800207b48c5
niveau de protection : aucun    résultat : autorisé
END RECORD
```

Fichier d'audit de WebSEAL

Vous pouvez également surveiller l'activité du serveur WebSEAL. Policy Director enregistre ces événements contrôlables sous la forme d'un rapport d'audit qui renseigne sur les opérations conduites. Une fois réunis, ces rapports d'audit constituent le fichier d'audit proprement dit.

Audit de WebSEAL

La strophe [wand] du fichier de configuration iv.conf contient des paramètres qui déterminent la configuration des fichiers d'audit du serveur WebSEAL.

Le tableau suivant illustre la relation entre WebSEAL et le fichier d'audit :

Serveur	Fichier d'audit
WebSEAL	Défini dans iv.conf: auditlog= *chemin_installation*/www/log/wand_audit_log

Activation et désactivation de l'audit de WebSEAL

Par défaut, l'audit du serveur WebSEAL est désactivé :

```
[wand]
logaudit = no
```

Pour activer, l'audit, entrez :

```
logaudit = yes
```

Remarque : Aucun espace ne doit suivre yes ou no lorsque vous éditez ce paramètre dans le fichier de configuration iv.conf.

Définition de l'emplacement du fichier d'audit

L'emplacement par défaut du fichier d'audit de WebSEAL est :

```
[wand]
auditlog = log/wand-audit-log
```

Définition de la taille maximale d'un fichier journal

Policy Director définit une taille maximale par défaut pour le journal d'audit :

```
[wand]
logsize = 2000000
```

Policy Director crée une copie de sauvegarde du fichier d'audit lorsque celui-ci atteint cette taille. Un nouveau fichier journal vide prend la place du journal d'audit par défaut. Notez que ce paramètre s'applique également aux fichiers journaux HTTP standard suivants :

- wand_request_log
- wand_referer_log
- wand_agent_log

Syntaxe du fichier d'audit de WebSEAL

Chaque réponse (réussite ou échec) renvoyée par le serveur WebSEAL est enregistrée dans une entrée d'une ligne dans le format suivant :

```
hôte type_appel uri code_état_iv [date] uuid liste_uuid_groupes
```

hôte (et point d'arrivée)	Données de l'adresse IP et du point d'arrivée du système hôte distant. Affiche ″[-]″ à défaut de données de point d'arrivée.

type_appel	0 pour une connexion TCP, 1 pour UNAUTH RPC et 2 pour AUTH RPC
uri	Désigne l'identifiant de requête universel (Universal Request Indicator) de la requête.
code_état_iv	Code d'état de ce sous-ensemble des fonctions d'audit standard de Policy Director.
date	Date et heure de la requête.
uuid (indiqué avec l'attribut **-p**)	UUID du client. N'affiche rien en l'absence d'UUID identifié.
liste_uuid_groupes (indiqué avec l'attribut **-g**)	Liste des UUID des groupes. N'affiche rien en l'absence d'UUID de groupe identifié.

Exemple de contenu d'un fichier d'audit

Le contenu d'un fichier d'audit a l'aspect suivant :

```
204.30.81.188[33380] 2 /audit_report.html 0x18a2141a
[21/Aug/1997:14:36:23 -0700]
-p 00000064-0f4c-21d1-9300-00c078500371
-g 0000000c-0f4c-21d1-9301-00c078500371
-g 0000044c-0f4c-21d1-8601-00c078500371
-g 0000044d-0f4c-21d1-8601-00c078500371
```

Détail :

hôte :	204.30.81.188
point d'arrivée :	[33380]
type_appel :	2
uri :	/audit_report.html
code_état_iv :	0x18a2141a
date :	[21/Aug/1997:14:36:23 -0700]
uuid :	-p 00000064-0f4c-21d1-9300-00c078500371
liste_uuid_groupes :	-g 0000000c-0f4c-21d1-9301-00c078500371 -g 0000044c-0f4c-21d1-8601-00c078500371 -g 0000044d-0f4c-21d1-8601-00c078500371

Remarque : La chaîne de l'URI peut apparaître sous la simple forme d'un tiret (-). Cette situation peut notamment résulter d'une fin prématurée de la requête ou d'un défaut dans la syntaxe de la chaîne de la requête.

Fichier d'audit des commandes de gestion de Policy Director

Chaque serveur Policy Director peut consigner des événements contrôlables lorsqu'une opération de gestion pouvant être auditée intervient. Policy Director enregistre ces événements contrôlables sous la forme d'un rapport d'audit qui renseigne sur les opérations conduites. Une fois réunis, ces rapports d'audit constituent le fichier d'audit proprement dit.

Le tableau suivant illustre la relation entre chaque serveur Policy Director et son fichier d'audit :

Serveur	Processus	Fichier d'audit de gestion

Serveur de gestion	**ivmgrd**	Défini dans ivmgrd.conf : mgr-audit-file= *chemin_installation*/ivmgrd/log/mgraudit.log

Le serveur de gestion a notamment pour mission d'administrer la base de données primaire des règles d'autorisation.

Cette base de données comprend :

- la description de l'espace des noms d'objet protégé du domaine sécurisé ;
- les modèles de règle ;
- les données d'emplacement des listes de contrôle d'accès.

A partir de la console de gestion, ou par le biais de l'utilitaire **ivadmin**, vous pouvez consigner tous les événements liés aux commandes de gestion dans le fichier mgraudit.log.

Contenu des rapports d'audit

Les rapports d'audit sont enregistrés sous forme de chaînes encadrées par des crochets de style XML. Un événements d'audit comporte les informations suivantes :

ID du processus source
Fourni d'après le descripteur du client RPC entrant et indiqué sous la forme d'une liste d'UUID ou la chaîne `unauthenticated`, selon les cas.

Code : `P`

ID d'événement
Nombre qui identifie de manière unique une commande de gestion, défini dans l'en-tête ../ivmgrd/cmdConst.h.

Code : `I`

Sortie de la commande
Nombre correspondant au code d'état retourné au programme appelant.

Code : `O`

Horodate
Indique la date et l'heure à laquelle la commande a abouti, dans le format utilisé pour l'audit des listes de contrôle d'accès.

Code : `D`

Vecteur d'arguments de la commande
Représente les arguments d'entrée de la commande entrée.

Codes : `V` et `A`

Exemple de fichier d'audit du serveur de gestion

Le contenu du fichier d'audit du serveur de gestion a l'aspect suivant :

```
<E><D>Fri May 30 00:00:00 1999<\D><I>3008</I><O>0</O><P>[1]
069d9fb6-943e-11cd-a35c-0000c08adf56</P><V><A> argument
1</A><A>argument 2</A></V></E>
```

Fichiers d'audit des serveurs DCE

Les fichiers d'audit des serveurs DCE suivants utilisent le service d'audit du DCE. Les fichiers sont au format binaire. Pour visualiser le contenu de ces fichiers, utilisez l'utilitaire **dcecp**.

1. Fichier d'audit du service de sécurité du DCE (secd)
   /opt/dcelocal/var/security/sec_audit_trail
   /opt/dcelocal/var/security/sec_audit_trail.md_index
2. Fichier d'audit du service d'audit du DCE (auditd)
   /opt/dcelocal/var/security/central_trail
   /opt/dcelocal/var/security/central_trail.md_index
3. Fichier d'audit du service horaire du DCE (dtsd)
   /opt/dcelocal/var/security/dts_aud_trail
   /opt/dcelocal/var/security/dts_aud_trail.md_index

Exemple du fichier sec_audit_trail

```
dcecp> login cell_admin
Enter Password:
dcecp>

--- Event Record number 261 ---
o Event Information:
   - Event Number:          0x101 /* 257 */
   - Event Name:          AS_Request
   - Event Outcome:          success
o Server:          /.:/hosts/eggman
o Client:          /.../eggman_cell/cell_admin
o Number of groups:          0
o Authorization Status:          Authorized with a name
o Date and Time recorded: 1998-10-20-10:42:56.248-04:00I-----
--- End of Event record number 261 ---
```

Chapitre 13. WebSEAL - Configuration de l'authentification

Policy Director WebSEAL prend en charge les méthodes d'authentification par clé secrète LDAP ou Kerberos, et par clé privée et clé publique. L'un des aspects importants du processus d'authentification est l'acquisition des droits d'accès. Les droits d'accès, qui s'obtiennent au cours de l'autorisation des requêtes, permettent d'accéder aux ressources protégées.

Ce chapitre comprend les sections suivantes :

Présentation générale de l'authentification WebSEAL

Cette section explique comment WebSEAL gère les fonctions suivantes :

- Communication sécurisée par protocole SSL
- Méthodes d'authentification
- Méthodes de soumission des données d'identité
- Extension des méthodes d'authentification standard

Support SSL

WebSEAL gère les communications sécurisées par le biais du protocole SSL. Les sections qui suivent détaillent les processus de communication sécurisée utilisant le protocole SSL :

- «Configuration de WebSEAL pour SSL» à la page 160.
- «Définition d'un certificat de côté serveur pour WebSEAL» à la page 163.

Méthodes d'authentification

L'authentification est un processus qui consiste à identifier une personne qui tente de se connecter à un domaine sécurisé. WebSEAL gère les méthodes d'authentification suivantes :

- Clé secrète LDAP
- Kerberos version 5
- Paire de clés publique/privée

Données d'identité du client

Le processus d'authentification demande au client de fournir des données d'identité au cours de la procédure de connexion. WebSEAL prend en charge les méthodes de présentation d'identité suivantes :

1. L'authentification par nom d'utilisateur et mot de passe (LDAP et Kerberos) :
   - L'authentification de base
   - La connexion par formulaires

Reportez-vous à la section «Méthodes d'authentification par nom d'utilisateur et mot de passe» à la page 168.

2. L'authentification par certificat côté client X.509 (utilisée par la méthode avec clés privée/publique).

   Reportez-vous à la section «Méthode d'authentification par certificat X.509» à la page 173.

Acquisition des droits d'accès

Vous pouvez utiliser un service d'acquisition de droits d'accès (SAD) pour étendre les méthodes d'authentification prises en charge par WebSEAL. Reportez-vous à la section «Configuration du service d'acquisition de droits d'accès de Policy Director» à la page 174.

Configuration de WebSEAL pour SSL

Le serveur WebSEAL Policy Director gère les communications sécurisées avec les navigateurs utilisant le protocole SSL.

S'ils utilisent ce protocole, les clients peuvent choisir entre deux méthodes pour transmettre leurs données d'identité à WebSEAL :

- Nom d'utilisateur et mot de passe
- Certificat numérique côté client X.509

Dans les deux modes, WebSEAL s'authentifie auprès du client au moyen de son certificat numérique de côté serveur. Ce certificat X.509 lui est délivré par une autorité de certification (AC). Policy Director enregistre le certificat et la clé privée associée dans un fichier au format PEM ou PKCS#12.

Dans le cas du format PEM, Policy Director enregistre dans des fichiers séparés la clé privée du serveur et sa clé publique signée. Avec le format PKCS#12, les paires de clés générées sont enregistrées ensemble dans un même fichier.

Le nom commun (CN) contenu dans le certificat de serveur devrait être identique au nom d'hôte complet du serveur WebSEAL.

Bien que cela ne soit pas obligatoire, la plupart des navigateurs vérifient que le certificat d'un serveur a été délivré par une autorité de certification homologuée. Cette vérification se fait par le biais de la base de données des autorités de certification racine. Si le signataire du certificat ne figure dans aucune entrée de cette base de données, un message d'avertissement apparaît. Il revient alors à l'utilisateur de refuser ou d'accepter la connexion à ce serveur.

Reportez-vous à la section «Définition d'un certificat de côté serveur pour WebSEAL» à la page 163 pour plus d'informations sur l'obtention et l'installation d'un certificat X.509 de côté client pour WebSEAL.

En mode certificat de côté client, WebSEAL s'authentifie auprès du client au moyen de son certificat numérique côté serveur, comme décrit plus haut. De plus, WebSEAL demande un certificat d'AC racine X.509 à une autorité de certification pouvant valider le certificat de côté client. Une requête client adressée avec le certificat de côté client permet une véritable authentification réciproque.

Utilisation des certificats de côté client et des certificats d'AC racine

Un certificat X.509 de côté serveur permet d'identifier un serveur WebSEAL donné auprès d'un client. Policy Director enregistre les certificats de côté client au format PEM ou PKCS#12, de la manière suivante :

- Dans le cas du format PEM, Policy Director enregistre dans des fichiers séparés la clé privée du serveur et sa clé publique signée.
- Dans le cas du format PKCS#12, un unique fichier contient la clé publique et la clé privée du serveur.

Remarque : Le serveur WebSEAL ne peut contenir et gérer qu'un seul certificat de serveur à la fois. WebSEAL ne permet pas d'installer plusieurs instances logiques d'un serveur Web sur une même machine.

Un certificat d'AC racine identifie une autorité de certification (AC) déterminée. WebSEAL demande un certificat d'AC racine pour valider un certificat de côté client. WebSEAL peut administrer une liste de certificats d'AC racine au format PEM , PKCS#12, ou une combinaison des deux formats, de la manière suivante :

- Pour le format PEM, les certificats de racine sont contenus dans un unique fichier.
- Pour le format PKCS#12, Policy Director les enregistre dans des fichiers séparés regroupés dans un répertoire commun.

Stockage des certificats

Le fichier de configuration secmgrd.conf définit les paramètres de stockage des certificats. Ces paramètres varient selon qu'on les emploie pour UNIX ou pour Windows.

Paramètre	Description
Pour UNIX : `ca-directory = /opt/intraverse/lib/certs` **Pour Windows :** `ca-directory = C:\Program Files\ibm\Policy Director\lib\certs`	
	Répertoire de base des certificats stockés.
Pour UNIX : `ca-cert-file = /lib/certs/cacert.pem` **Pour Windows :** `ca-cert-file = C:\Program Files\ibm\Policy Director\lib\certs\cacert.pem`	
	Certificat X.509 d'AC racine d'une autorité de certification reconnue, au format PEM. WebSEAL accepte les certificats X.509 de côté client d'une autorité de certification sécurisée, au format PEM. Vous pouvez ajouter les certificats de racine d'autres autorités de certification dans ce fichier.
Pour UNIX : `ca-cert-p12-dir = /opt/intraverse/lib/certs/ca_p12` **Pour Windows :** `ca-cert-p12-dir = C:\Program Files\ibm\Policy Director\lib\certs\ca_p12`	
	Répertoire désigné pour stocker un fichier contenant le certificat de racine X.509 d'une autorité de certification reconnue, au format PKCS#12. WebSEAL accepte les certificats X.509 de côté client d'une autorité de certification sécurisée, au format PKCS#12. Vous pouvez stocker les fichiers des certificats de racine d'autres autorités de certification dans ce répertoire.
Pour UNIX : `certificate-file = /opt/intraverse/lib/certs/svrcert.pem` **Pour Windows :** `certificate-file = C:\Program Files\ibm\Policy Director\lib\certs\svrcert.pem`	

	Certificat de serveur X.509 délivré par l'AC, au format PEM. Ce certificat est présenté aux clients utilisant le protocole SSL. Le certificat type contenu dans ce fichier doit être remplacé par un certificat valide fourni par une autorité de certification sécurisée.
Pour UNIX : `key-file = /opt/intraverse/lib/certs/srvkey.pem` **Pour Windows :** `key-file = C:\Program Files\ibm\Policy Director\lib\certs\srvkey.pem`	
	Clé privée du serveur, au format PEM. La clé par défaut contenue dans ce fichier à l'installation doit être remplacée par une autre, que vous devez créer.
Pour UNIX: `certificate-file = /opt/intraverse/lib/certs/svrcert.p12` **Pour Windows :** `certificate-file = C:\Program Files\ibm\Policy Director\lib\certs\svrcert.p12`	
	Certificat de serveur X.509 délivré par l'AC, au format PKCS#12. Le fichier contient la clé privée. Le certificat et la clé par défaut contenus dans ce fichier doivent être remplacés par un certificat et une clé valides délivrés par une autorité de certification sécurisée.
Pour UNIX et Windows: **pass-key =**phrase clé	
	Mot de passe clé (phrase clé) utilisé pour déverrouiller le fichier de la clé privée.

Configuration de la gestion des certificats

La strophe `[wand]` du fichier de configuration iv.conf contient un paramètre qui permet de définir le mode de gestion des certificats X.509 de côté client. Pour choisir comment WebSEAL doit gérer ces certificats, vous devez définir la valeur du paramètre **verify-clients**. Les valeurs qu'admet ce paramètre sont les suivantes :

Valeur	Description
never	Ne demande pas de certificats X.509 aux clients. Oblige les clients à fournir un nom d'utilisateur et un mot de passe pour avoir accès au domaine.
optional	Demande aux clients un certificat X.509 et utilise l'authentification par certificat s'il l'obtient. Dans le cas contraire, oblige les clients à utiliser l'authentification de base.
required	Demande aux clients un certificat X.509 et utilise l'authentification par certificat uniquement. Si le client ne le fournit pas, n'autorise pas la connexion.

Par défaut, WebSEAL ne demande pas de certificats de côté client.

```
[wand]
verify-clients = never
```

Définition du délai d'expiration du cache de session SSL

La strophe `[ssl]` du fichier de configuration contient un paramètre qui permet de définir le délai d'expiration du cache des sessions SSL statiques.

WebSEAL place les données de droit d'accès dans un cache interne. Ce paramètre de délai d'expiration des droits d'accès détermine la durée pendant laquelle les données de droits d'accès restent en mémoire au niveau de WebSEAL.

Ce paramètre ne définit pas un délai d'expiration pour inactivité. Il définit une "durée de vie de droit d'accès" plutôt qu'un "délai d'expiration de droit d'accès". Son objectif est de renforcer la sécurité en obligeant l'utilisateur à s'authentifier à nouveau une fois atteint le délai défini.

Le délai d'expiration par défaut du cache (en secondes) est :

```
[ssl]
ssl-cache-timeout = 3600
```

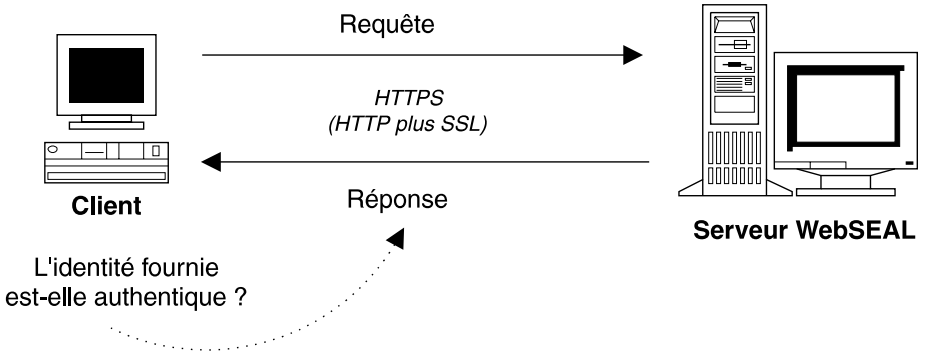
Ajustez cette valeur au mieux pour équilibrer les performances du serveur et la facilité d'emploi en fonction du nombre de requêtes SSL que le serveur doit traiter.

Remarque : Certains navigateurs renégocient leur session de manière automatique. Dans cette situation, ce paramètre est sans effet.

Définition d'un certificat de côté serveur pour WebSEAL

Vous pouvez configurer un serveur WebSEAL Policy Director de manière à permettre aux clients utilisant SSL de vérifier son authenticité. Cette section vous guide à travers les tâches administratives requises pour définir un certificat de côté serveur au format PEM.

En particulier, vous devez enregistrer le serveur auprès d'une autorité de certification homologuée ou d'un programme de création de certificats contrôlé en interne. Vous devez obtenir un certificat de serveur de site qui permette à Policy Director d'accepter les requêtes des navigateurs utilisant SSL et d'y répondre.

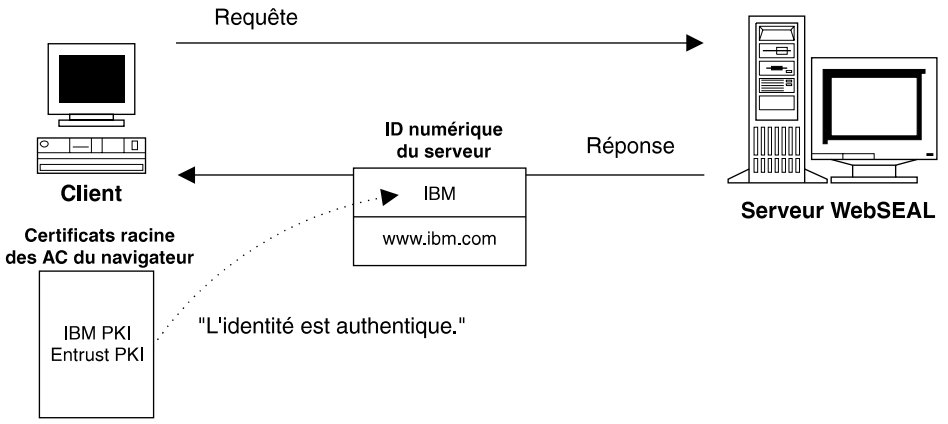


Mise en place de communications SSL sécurisées

Le serveur WebSEAL Policy Director gère l'authentification des clients utilisant HTTP en plus de SSL (HTTPS). WebSEAL doit disposer d'un certificat X.509 public de côté serveur pour répondre à ces clients. Le certificat X.509 prouve au client que la réponse du serveur WebSEAL provient bien d'un serveur autorisé.

Pour permettre les communications SSL sécurisées avec l'Internet, le navigateur doit authentifier le serveur. Pour cela, le navigateur vérifie le certificat de clé publique du serveur en le comparant avec un certificat d'AC racine correspondant. Ces certificats d'AC correspondants sont, soit contenus dans sa base de données, soit acquis par lui.

Un certificat de serveur autorisé (signé par une autorité de certification) empêche toute possibilité d'imposture.



WebSEAL est fourni avec un exemple de certificat de serveur signé par une autorité de certification IBM type. Ce modèle de certificat permet à WebSEAL de répondre à une requête de navigateur SSL. En revanche, le navigateur ne peut pas contrôler ce certificat dans la mesure où sa base de données ne contient pas de certificat d'AC racine IBM. Ce certificat ne permet donc pas d'établir des communications SSL totalement sécurisées.

Pour atteindre cet objectif, il est vital d'enregistrer le serveur afin d'obtenir un certificat de serveur de site de la part d'une autorité de certification sécurisée. Vous pouvez obtenir un certificat de serveur de site de la part d'une autorité de certification reconnue, ou créer votre propre certificat "maison" à partir d'un logiciel comme, par exemple, IBM SecureWay Trust Authority.

La configuration de Policy Director pour les communications SSL implique les tâches suivantes :

- «Création d'une clé publique et d'une clé privée».
- «Utilisation de l'utilitaire gencsr (facultatif)» à la page 165 (optionnel).
- «Enregistrement de la requête de signature de certificat par l'autorité de certification» à la page 167.
- «Installation du certificat du serveur» à la page 167.
- «Mise à jour du fichier de configuration du gestionnaire de sécurité» à la page 167 .
- «Test du nouveau certificat» à la page 168.

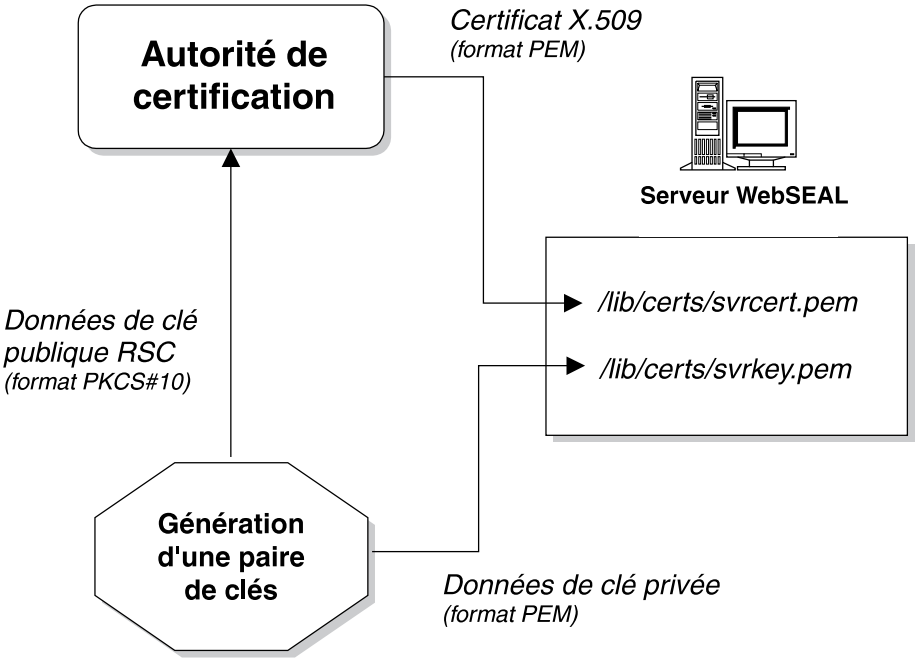
Création d'une clé publique et d'une clé privée

Pour obtenir un certificat de serveur de site de la part d'une autorité de certification, vous devez d'abord créer une paire de clés publique/privée pour votre serveur.

Définir la clé privée vous appartient.

La partie liée à la clé publique, qui contient les données d'identité de l'utilisateur, est aussi appelée la requête de signature de certificat (RSC). La RSC contient les informations que vous devez transmettre à l'autorité de certification (AC) lorsque vous enregistrez votre serveur pour obtenir un certificat de serveur de site. L'AC utilise ces informations pour créer votre certificat X.509 de côté serveur qui permet de répondre aux clients SSL.

Vous devez stocker votre clé privée et le certificat X.509 de côté serveur délivré par l'AC dans des emplacements spécifiquement définis à cette fin dans le fichier de configuration secmgrd.conf.



Pour créer une paire de clés publique/privée, utilisez les outils de création et les instructions fournis par l'autorité de certification. Policy Director comporte un utilitaire (**gencsr**) que vous pouvez utiliser à défaut d'en posséder d'autres. La section «Utilisation de l'utilitaire gencsr (facultatif)» décrit comment créer une paire de clés avec **gencsr**.

Utilisation de l'utilitaire gencsr (facultatif)

Policy Director comprend un utilitaire nommé **gencsr**, qui permet de créer une paire de clés publique et privée. Cet utilitaire peut être installé en même temps que Policy Director et réside dans le répertoire /bin :

UNIX : *chemin_installation*/bin/gencsr

Windows : *chemin_installation*\bin\gencsr

Format PKCS#10

L'utilitaire **gencsr** permet de créer la paire de clés. Les données de la clé privée sont enregistrées dans un fichier au format PEM. La clé publique est enregistrée dans un autre fichier qui contient également d'autres données de requête de signature de certificat (RSC). Les données de la clé publique sont enregistrées au format PKCS#10.

La syntaxe des requêtes de certification respecte le format PKCS (Public-Key Cryptography Standards). Une requête de certification se compose d'un DN (distinguished name), d'une clé publique et d'un ensemble d'attributs optionnels, collectivement signés par l'organisation demandant la certification. Une requête de signature de certificat est envoyée à une autorité de certification (AC). Cette AC génère ensuite un certificat de clé publique X.509 unique à l'intention de votre serveur.

Syntaxe des commandes de l'utilitaire gencsr

```
gencsr [-csrfile fichier_rsc] [-keyfile
fichier_clé] [-keylen longueur_clé] [-version]
```

Options	Description
-csrfile	Demande à créer la clé publique (RSC) dans un fichier (format PKCS#10). Le fichier désigné (fichier_rsc) contient la requête de signature de certificat en format ASCII. La valeur par défaut est la sortie standard.
-keyfile	Demande la création de la clé privée dans un fichier (format PEM). La valeur par défaut est la sortie standard.
-keylen	Indique la longueur des clés (en octets) de la paire de clés publique/privée. La valeur par défaut est 512.
-version	Affiche le numéro de version et les informations légales de l'utilitaire.
-help	Affiche les descriptions de la syntaxe des commandes et de leurs options.

Procédures de l'utilitaire gencsr

Pour utiliser l'utilitaire **gencsr** de Policy Director :

1. Exécutez l'utilitaire **gencsr** avec les arguments définissant le nom du fichier RSC, le nom du fichier de la clé privée et, éventuellement, la longueur des clés :

   UNIX : `$ gencsr -csrfile nom_fichier -keyfile nom_fichier -keylen 1024`

   Windows : `gencsr -csrfile nom_fichier -keyfile nom_fichier -keylen 1024`

   Vous pouvez utiliser n'importe quel nom de fichier pour la clé privée comme pour la clé publique ; vous pourrez renommer ces fichiers ultérieurement.

   Remarque : La longueur de clé par défaut est de 512 octets.
2. L'utilitaire demande des informations à l'utilisateur, notamment la phrase clé PEM.

   Vous ne devez surtout pas oublier cette phrase clé que vous consignerez ultérieurement dans le fichier de configuration secmgrd.conf. La phrase clé assure la protection de votre clé privée.
3. L'utilitaire génère un fichier RSC et un fichier contenant la clé privée. La section «Enregistrement de la requête de signature de certificat par l'autorité de certification» à la page 167 décrit comment envoyer ce fichier RSC à l'autorité de certification.
4. Faites une sauvegarde du modèle de fichier de clé privée fourni avec Policy Director :

   UNIX : `# cp svrkey.pem svrkey.pem.orig`

   Windows : `copy svrkey.pem svrkey.pem.orig`
5. Enregistrez le nouveau fichier de clé privée dans le même répertoire et nommez-le svrkey.pem :

   UNIX : `# cp newkey.txt svrkey.pem`

   Windows : `copy newkey.txt svrkey.pem`

Remarque : Vous devez protéger cette clé privée. Il ne doit exister qu'une seule instance de la clé privée ; ceci est vital pour le contrôle des communications entre client et serveur.

Enregistrement de la requête de signature de certificat par l'autorité de certification

Pour enregistrer la requête de signature de certificat auprès de l'autorité de certification :

1. L'autorité de certification propose généralement un formulaire d'enregistrement en ligne. Renseignez ce formulaire à l'aide d'un navigateur Web. Naturellement, le détail de la procédure varie selon l'autorité de certification choisie.
2. Le formulaire d'enregistrement vous demande de transmettre la requête de signature de certificat (RSC) créée dans la section «Création d'une clé publique et d'une clé privée» à la page 164 ou «Utilisation de l'utilitaire gencsr (facultatif)» à la page 165. Vous pouvez coller le contenu du fichier RSC dans le formulaire ou l'envoyer par courrier électronique.
3. L'autorité de certification vous transmet ensuite le certificat de clé publique X.509 de côté serveur que vous avez demandé, dans le format PEM. Ceci peut prendre plusieurs jours.

WebSEAL demande un certificat au format PEM. L'encodage PEM est une méthode de chiffrement en base 64 appliquée à un certificat binaire. Un fichier au format PEM est un fichier ASCII dont les lignes sont limitées à 64 caractères. Le fichier ASCII commence par :

```
-----BEGIN CERTIFICATE----
```

et se termine par :

```
-----END CERTIFICATE----
```

Installation du certificat du serveur

Pour installer le certificat du serveur :

1. Faites une sauvegarde du modèle de fichier de certificat fourni avec Policy Director :

   Pour le format PEM :

   UNIX : `# cp svrcert.pem svrcert.pem.orig`

   Windows : `copy svrcert.pem svrcert.pem.orig`
2. Enregistrez le fichier du certificat délivré par l'autorité de certification dans le même répertoire et nommez-le svrkey.pem (changez l'ancien nom) :

   UNIX : `# cp newcert.txt svrcert.pem`

   Windows : `copy newcert.txt svrcert.pem`

Mise à jour du fichier de configuration du gestionnaire de sécurité

Vérifiez et réactualisez, si nécessaire, les entrées suivantes du fichier de configuration secmgrd.conf :

`certificate-file =`	Nom de chemin du fichier contenant le certificat au format PEM délivré par l'autorité de certification. Valeur par défaut : lib/certs/svrcert.pem
`key-file =`	Nom de chemin du fichier de la clé privée créée localement. Valeur par défaut : lib/certs/svrkey.pem
`pass-key =`	Phrase clé PEM utilisée pour protéger la clé privée.

Ne modifiez les entrées `certificate-file` et `key-file` que si vous utilisez des noms de fichier différents des valeurs par défaut indiquées.

Test du nouveau certificat

Pour tester le nouveau certificat :

1. Arrêtez, puis relancez Policy Director pour commencer à utiliser le nouveau certificat :

   UNIX :

   ```
   # /etc/init.d/iv stop
   # /etc/init.d/iv start
   # /etc/init.d/iv status
   ```

   Windows : Utilisez le panneau de configuration.

2. Vérifiez que le gestionnaire de sécurité (secmgrd) s'est initialisé correctement.

   Si secmgrd ne démarre pas, consultez le fichier journal suivant pour en connaître la cause :

   UNIX : *chemin_installation*/secmgr/log/secmgrd.log

   Windows : *chemin_installation*\secmgr\log\secmgrd.log

   Si aucun message d'erreur n'apporte de réponse, démarrez secmgrd manuellement en mode débogage. Reportez-vous à la section «Mode de débogage pour l'acheminement des messages vers la sortie standard» à la page 148. Le cas échéant, consultez les dernières informations disponibles sur la résolution d'incidents, sur le site WEB d'IBM SecureWay Policy Director à l'adresse :

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

3. A partir d'un navigateur, connectez-vous au serveur HTTPS et vérifiez si le navigateur accepte le certificat du serveur.

   Par exemple, la base de données du navigateur doit déjà contenir par défaut le certificat de racine largement reconnu VeriSign. Vous ne devriez donc voir s'afficher ni messages d'avertissement, ni boîtes de dialogue avant l'invite de connexion de Policy Director.

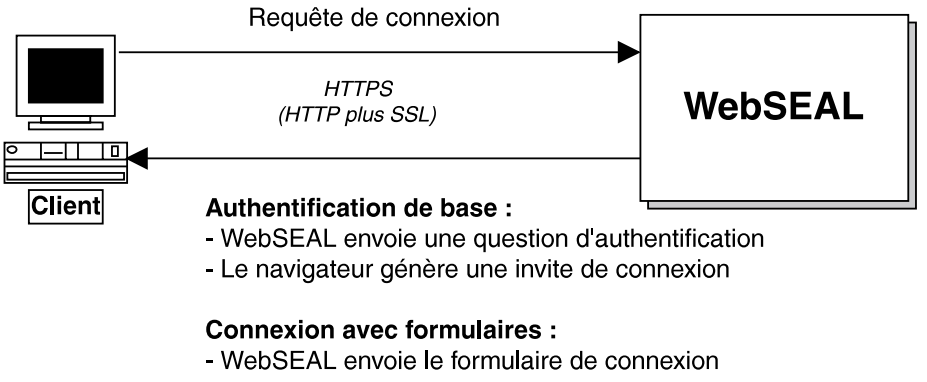
   En revanche, des messages d'avertissement apparaîtront si vous utilisez le modèle de certificat fourni avec Policy Director puisque la base de données du navigateur ne contient pas de certificat de racine IBM pouvant authentifier ce modèle de certificat de serveur. Ces messages vous demandent d'accepter ou de rejeter le certificat de serveur. En l'absence de certificat de racine correspondant, le navigateur est incapable de vérifier l'authenticité du certificat de serveur. C'est pour cette raison qu'il vous confie la responsabilité d'accepter ou de refuser ce certificat.

   Vous possédez à présent un certificat de serveur de site validé par une autorité de certification sécurisée. Désormais, les clients SSL peuvent sans danger authentifier votre serveur WebSEAL.

Méthodes d'authentification par nom d'utilisateur et mot de passe

Les méthodes d'authentification par clé secrète Kerberos et LDAP demandent de fournir des données d'identité sous la forme d'un nom d'utilisateur et d'un mot de passe. WebSEAL permet de soumettre ces informations de deux manières différentes :

- «Méthode d'authentification de base» à la page 169.
- «Méthode de connexion par formulaires» à la page 170.



Méthode d'authentification de base

WebSEAL prend en charge le protocole SSL, utilisé par Netscape Communicator/Navigator et Microsoft Internet Explorer (IE), pour obtenir des données d'identité telles que les noms d'utilisateur et les mots de passe. Par convention, les URL utilisant une connexion SSL sécurisée commencent par **https:** au lieu de **http:**.

Pour que la connexion aboutisse, Policy Director demande aux clients d'utiliser leur identité Policy Director telle qu'elle est enregistré dans le registre de sécurité. L'authentification de base est une méthode standard qui permet de soumettre un nom d'utilisateur et un mot de passe à un système d'authentification.

Dans la première phase, le serveur s'authentifie auprès du client à l'aide de son certificat de côté serveur. Si le client accepte ce certificat, le serveur demande au client de s'authentifier à son tour. Le navigateur affiche une invite de connexion demandant un nom d'utilisateur et un mot de passe.

Remarque : Le navigateur place ensuite ces informations en antémémoire. L'authentification de base standard a besoin des données du nom d'utilisateur et du mot de passe pour toutes les requêtes suivantes. Les données mises en antémémoire sont transmises à l'utilisateur de manière transparente.

Les aspects importants de l'authentification de base sont les suivants :

- Policy Director utilise le protocole SSL comme canal de communication sécurisé.
- Policy Director transmet les noms d'utilisateur et les mots de passe via ce canal SSL sécurisé.

A l'occasion d'une étape de la procédure d'authentification de base, vous verrez peut-être s'afficher une invite de connexion semblable à celle-ci :

```
Entrez votre nom d'utilisateur pour Policy Director [/.../www.ibm.com] at www.ibm.com

nom d'utilisateur :
Mot de passe :
```

Entrez les informations demandées dans les champs **nom d'utilisateur** et **Mot de passe**.

Modèle d'authentification de base

La procédure d'authentification de base type comprend les étapes suivantes :

1. Un navigateur contacte le serveur en utilisant SSL.

2. Le serveur envoie le certificat de serveur qu'il a obtenu d'une autorité de certification.
3. Le navigateur effectue l'une des actions suivantes :
   - Recherche et trouve un certificat d'AC racine correspondant dans sa base de données et accepte le certificat du serveur.
   - Recherche mais ne trouve aucun certificat d'AC racine correspondant dans sa base de données et adresse un message d'avertissement à l'utilisateur pour qu'il choisisse lui-même d'accepter ou de refuser le certificat reçu.
4. S'il est accepté, le serveur envoie une question d'authentification au navigateur.
5. Le navigateur y répond en affichant une invite de connexion demandant un nom d'utilisateur et un mot de passe.
6. L'utilisateur entre ces informations, puis le navigateur les transmet au serveur Policy Director.
7. Policy Director génère un droit d'accès si le nom d'utilisateur et le mot de passe existent aussi dans son registre des utilisateurs. Policy Director prend les décisions d'autorisation sur la base de ce droit d'accès. WebSEAL met ce droit d'accès en antémémoire pour toute la durée de la session SSL.
8. Le navigateur place également les données du nom d'utilisateur et du mot de passe en antémémoire.

   L'authentification de base standard a besoin de ces données d'identité pour toutes les requêtes ou sessions suivantes du navigateur. Cette exigence est satisfaite de manière transparente par l'utilisation des données d'authentification placées en antémémoire.

   Remarque : Dans la mesure où, dans le contexte de l'authentification de base, le navigateur met en antémémoire les données d'identité, la commande **pkmslogout** ne fonctionne pas correctement. Pour se déconnecter totalement, vous devez fermer la session du navigateur. Pour utiliser la commande **pkmslogout**, utilisez plutôt la méthode de connexion par formulaires.

Tâches d'administration

L'administrateur doit conduire les tâches suivantes pour préparer le serveur WebSEAL à l'accès SSL dans le mode authentification de base.

- Installation du certificat X.509 de côté serveur sur le serveur WebSEAL
- Création d'un compte Policy Director pour chaque utilisateur membre du domaine sécurisé

Méthode de connexion par formulaires

Outre l'authentification de base, Policy Director propose une autre méthode d'authentification : la connexion par formulaires. Cette méthode utilise un formulaire de connexion HTML au lieu de l'invite de connexion standard utilisée dans le cadre de l'authentification de base.

Lorsque vous utilisez la connexion par formulaires, le navigateur ne met pas en antémémoire les données d'identité (nom d'utilisateur et mot de passe) comme dans le cas de l'authentification de base. Cet aspect permet d'utiliser la commande de fin de session SSL **pkmslogout**. Dans la mesure où Policy Director ne demande les données de droit d'accès qu'une seule fois (et les met en antémémoire), il n'est pas nécessaire de répéter les requêtes de connexion avec chaque requête du navigateur.

La connexion par formulaires nécessite de définir le paramètre **https-forms-auth** dans la strophe [wand] du fichier de configuration iv.conf. Ce paramètre peut prendre la valeur yes ou no. La valeur par défaut est no.

```
[wand]
https-forms-auth = no
```

Policy Director est fourni avec sept formulaires HTML types. Vous pouvez personnaliser ces formulaires en y intégrant des messages ou des actions adaptés à votre site.

La strophe [wand] du fichier de configuration iv.conf définit les emplacements de ces formulaires dans la section Emplacements des pages HTML SSL.

L'emplacement du répertoire par défaut est :

UNIX : *chemin_installation*/www/lib/html/

Windows : *chemin_installation*\www\lib\html\

Formulaire	Description
login.html	Requête de nom d'utilisateur et de mot de passe.
login_rep.html	Message d'erreur de connexion.
logout.html	Message indiquant la fin normale de la session SSL.
passwd.html	Formulaire de modification du mot de passe.
passwd_exp.html	Message signalant l'arrivée à expiration du mot de passe.
passwd_rep.html	Message signalant une erreur lors de la modification du mot de passe.
help.html	Références des commandes.

Deux macro-commandes sont également à votre disposition pour ces pages. Vous pouvez placer ces chaînes de macro dans les fichiers types. Le sous-programme remplace automatiquement les valeurs appropriées.

Macro	Description
%USERNAME%	Nom de l'utilisateur connecté.
%ERROR%	Message d'erreur codé dans le programme renvoyé par Policy Director.

Modèle d'authentification par formulaires

La procédure type d'authentification par formulaires comprend les étapes suivantes :

1. Un navigateur contacte le serveur en utilisant SSL.
2. Le serveur envoie le certificat de serveur qu'il a obtenu d'une autorité de certification.
3. Le navigateur effectue l'une des actions suivantes :
   - Recherche et trouve un certificat d'AC correspondant dans sa base de données et accepte le certificat du serveur.
   - Recherche mais ne trouve aucun certificat d'AC correspondant dans sa base de données et adresse un message d'avertissement à l'utilisateur pour qu'il choisisse lui-même d'accepter ou de refuser le certificat reçu.
4. S'il est accepté, le serveur WebSEAL demande au client de fournir un nom d'utilisateur et un mot de passe à l'aide d'un formulaire HTML personnalisé.

Policy Director utilise ce formulaire pour retourner ces données d'identité au serveur WebSEAL.

5. Policy Director génère un droit d'accès si le nom d'utilisateur et le mot de passe existent aussi dans son registre des utilisateurs. Policy Director prend les décisions d'autorisation sur la base de ce droit d'accès. WebSEAL met ce droit d'accès en antémémoire pour toute la durée de la session SSL.

   A la différence de l'authentification de base, ici le navigateur ne met pas en antémémoire les données du nom d'utilisateur et du mot de passe. La commande **pkmslogout** peut fonctionner sans incident.

Tâches d'administration

L'administrateur doit conduire les tâches suivantes pour préparer le serveur WebSEAL à l'accès SSL dans le mode connexion par formulaires :

1. Installation du certificat d'AC X.509 de côté serveur sur le serveur WebSEAL
2. Création d'un compte Policy Director pour chaque utilisateur membre du domaine sécurisé
3. Personnalisation des formulaires de Policy Director et définition de leur emplacement dans le fichier de configuration iv.conf

Commandes des méthodes d'authentification par nom d'utilisateur et mot de passe

Les commandes Policy Director suivantes permettent d'administrer les clients SSL utilisant l'authentification par nom d'utilisateur et mot de passe :

- pkmslogout
- pkmspasswd

pkmslogout

La commande pkmslogout permet de se déconnecter de la session SSL en cours. Cette commande peut être utilisée avec la méthode de connexion par formulaires.

```
https: //chemin_installation_URL/pkmslogout
```

Par exemple :

```
https: /www.ibm.com/pkmslogout
```

Le fichier qui s'affiche en réponse à cette commande de déconnexion se définit dans le fichier de configuration iv.conf.

```
# emplacements des pages HTML SSL
pkms-logout-page = lib/html/logout.html
```

Vous pouvez adapter le fichier logout.html à vos besoins spécifiques.

L'utilitaire **pkmslogout** peut gérer plusieurs types de page de réponse à une requête de déconnexion lorsque l'architecture du réseau nécessite différents écrans de sortie pour les divers systèmes finaux utilisés.

L'expression suivante désigne un fichier de réponse déterminé :

```
https://pkmslogout?filename=fichier_déconnexion_personnalisé
```

Où fichier_déconnexion_personnalisé désigne le nom de fichier de la réponse de déconnexion. Ce fichier doit résider dans le même répertoire /lib/html/ que celui défini pour le fichier logout.html par défaut.

pkmspasswd

Cette commande permet de modifier le mot de passe :

`https://chemin_installation_URL/pkmspasswd`

Par exemple :

`https://www.ibm.com/pkmspasswd`

Méthode d'authentification par certificat X.509

WebSEAL gère l'authentification en utilisant un certificat X.509 de côté serveur en plus de SSL. Le certificat X.509 fournit les données d'identité du client au serveur au lieu de nécessiter la saisie d'un nom d'utilisateur et d'un mot de passe.

Tâches de configuration pour la prise en charge des certificats X.509 de côté client

Exécutez les tâches suivantes pour permettre au serveur WebSEAL d'accepter les certificats numériques X.509 de côté client.

Tâches du client

Pour exécuter les tâches du client :

1. Demandez un certificat numérique X.509 de côté client (clé publique signée) à une autorité de certification.
2. Installez le certificat obtenu sur le système du client.

Tâches du serveur WebSEAL

Pour exécuter les tâches du serveur WebSEAL :

1. Demandez le certificat d'AC racine à la même autorité de certification.

   Ce certificat peut être au format PEM ou PKCS#12.
2. Copiez le certificat d'AC racine à l'emplacement approprié du système et indiquez cet emplacement dans le fichier de configuration secmgrd.conf :

   Format PEM :

   Ajoutez les certificats de racine au fichier suivant :

   UNIX : `ca-cert-file = lib/certs/cacert.pem`

   Windows : `ca-cert-file = lib\certs\cacert.pem`

   Format PKCS#12 :

   Ajoutez chaque certificat de racine dans un fichier séparé dans le répertoire suivant :

   UNIX : `ca-cert-p12-dir = lib/certs/ca_p12`

   Windows : `ca-cert-p12-dir = lib\certs\ca_p12`

   Remarque : Ces certificats PEM et PKCS#12 sont délivrés par les autorités de certification sécurisées par Policy Director.
3. Pour choisir comment WebSEAL doit gérer ces certificats, vous devez définir la valeur du paramètre **verify-clients**. Pour cela, entrez l'une des valeurs suivantes dans la strophe `[wand]` du fichier de configuration iv.conf : never, optional, ou required.

   Reportez-vous à la section «Configuration de la gestion des certificats» à la page 162 pour les descriptions de ces valeurs.
4. Pour configurer WebSEAL de manière à utiliser un serveur SAD, ouvrez le fichier iv.conf et changez la valeur du paramètre **cert-cdas** dans la strophe [authentication-mechanisms] en fonction de votre plate-forme :

```
[authentication-mechanisms]
cert-cdas =
&entry=/.:/subsys/intraverse/cdas/servers/nom_hôte
```

Les modules SAD disponibles sont cdasauthn.dll pour Windows NT, libcdasauthn.a pour AIX et libcdasauthn.so pour Solaris.

Reportez-vous à la section «Configuration de base du service d'acquisition de droits d'accès de Policy Director» à la page 176 pour plus d'informations sur le paramètre **cert-cdas**.

5. Pour définir l'identité du serveur, renseignez les paramètres **certificate-file** et **key-file** dans le fichier de configuration secmgrd.conf. Notez que la clé privée du serveur est au format PEM. Ces paramètres varient selon la plate-forme utilisée.

   Pour le paramètre certificate-file avec format PEM :

   UNIX : `certificate-file = /opt/intraverse/lib/certs/svrcert.pem`

   Windows : `certificate-file = C:\Program Files\ibm\Policy Director\lib\certs\svrcert.pem`

   Pour le paramètre key-file avec format PEM :

   UNIX : `key-file = /opt/intraverse/lib/certs/srvkey.pem`

   Windows : `key-file = C:\Program Files\ibm\Policy Director\lib\certs\srvkey.pem`

   Reportez-vous à la section «Stockage des certificats» à la page 161 pour plus d'informations sur les paramètres de stockage des certificats du fichier secmgrd.conf.

6. Pour définir l'identité du serveur, renseignez le paramètre certificate-file dans le fichier de configuration secmgrd.conf. Notez que le certificat de serveur est au format PKCS#12 :

   Pour le paramètre certificate-file avec format PKCS#12 :

   Pour UNIX: `certificate-file = /opt/intraverse/lib/certs/svrcert.p12`

   Pour Windows : `certificate-file = C:\Program Files\ibm\Policy Director\lib\certs\svrcert.p12`

7. Utilisez le service d'acquisition de droits d'accès (SAD) de Policy Director pour procéder à l'acquisition et au mappage des droits d'accès.

   Vous pouvez, si vous le souhaitez, créer et installer votre propre programme de service d'acquisition et de mappage de droits d'accès sur le système du serveur. Reportez-vous au manuel Policy Director - Guide de programmation et de référence et à la section «Configuration du service d'acquisition de droits d'accès de Policy Director» pour plus d'informations.

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

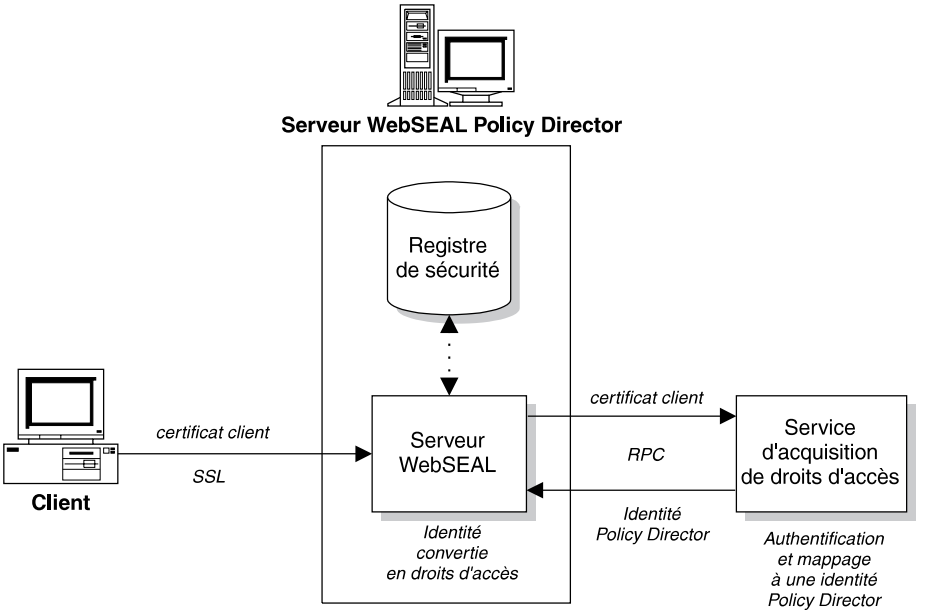
Le service d'acquisition de droits d'accès (SAD) de Policy Director est un composant adaptable qui permet d'étendre les méthodes d'authentification prises en charge par WebSEAL. Le SAD par défaut de Policy Director utilise le fichier cdas_server(.exe). Reportez-vous à la section «Configuration de WebSEAL pour utiliser le service d'acquisition de droits d'accès de Policy Director» à la page 175.

Vous pouvez, si vous le souhaitez, créer et installer votre propre programme de service d'acquisition et de mappage de droits d'accès sur le système du serveur.

Reportez-vous au manuel Policy Director - Guide de programmation et de référence pour plus d'informations sur la création et l'installation d'un service d'acquisition de droits d'accès.

Présentation du SAD de Policy Director

Le service d'acquisition de droits d'accès (SAD) de Policy Director permet l'authentification des données d'identité d'un utilisateur (par exemple, un certificat X.509) et leur association, ou mappage, à une identité d'utilisateur Policy Director. Le gestionnaire de sécurité renvoie des droits d'accès pour cette identité sur la base des données de son registre des utilisateurs.



Reportez-vous aux sections «SAD de Policy Director» à la page 31 et «Configuration de WebSEAL pour utiliser le service d'acquisition de droits d'accès de Policy Director» pour plus d'informations sur le service d'acquisition de droits d'accès de Policy Director.

Configuration de WebSEAL pour utiliser le service d'acquisition de droits d'accès de Policy Director

Vous pouvez configurer toutes les méthodes d'authentification prises en charge par WebSEAL dans la strophe `authentication-mechanisms` du fichier de configuration iv.conf. Ces méthodes concernent aussi bien les processus locaux que les processus distants personnalisés mis en oeuvre par les serveurs SAD.

Modules plug-in locaux

Vous devez associer chaque méthode d'authentification à un module plug-in local dans le fichier de configuration. Sur les plates-formes UNIX, ces modules sont des bibliothèques partagées. Sur Windows NT, il s'agit de bibliothèques DLL (Dynamic Link Libraries). Ces modules sont fournis avec Policy Director et ne peuvent pas être personnalisés.

Policy Director comprend un module plug-in standard qui permet l'interface avec n'importe quel serveur SAD tiers.

Plate-forme	Nom du module SAD
Solaris	libcdasauthn.so
AIX	libcdasauthn.a
Windows NT	cdasauthn.dll

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

Vous pouvez configurer un service d'acquisition de droits d'accès Policy Director capable de traiter les certificats X.509, qui permettent l'authentification du côté client de l'interface du SAD WebSEAL. La configuration du SAD de Policy Director requiert un argument supplémentaire qui indique l'emplacement de l'espace des noms du SRC du DCE où résident les données de liaisons du serveur SAD.

Pour configurer WebSEAL de manière à utiliser un serveur SAD, ouvrez le fichier iv.conf et changez la valeur du paramètre cert-cdas dans la strophe [authentication-mechanisms] en fonction de votre plate-forme :

Par exemple, la formule suivante (pour Windows NT) n'identifie qu'un seul serveur SAD pour gérer l'authentification par certificat X.509 :

```
[authentication-mechanisms]
cert-cdas = cdasauthn.dll&entry=/.:/subsys/intraverse/cdas/servers/nom_hôte
```

Dans cette expression, `cdasauthn.dll` indique le module SAD adapté à la plate-forme, nom_hôte le nom du système hôte, et `&entry=/.:/subsys/intraverse/cdas/servers/`*nom_hôte* l'emplacement de l'espace des noms du SRC du DCE où résident les données de liaison du serveur SAD.

Syntaxe des entrées de configuration

Une entrée de configuration d'authentification respecte le format suivant :

authn-mechanism = *module*[&*arg1*[
arg2]...[*argN*]]

Configuration de plusieurs serveurs SAD Policy Director

Un même service d'acquisition de droits d'accès peut prendre en charge plusieurs méthodes d'authentification. Dans ce cas, chaque système d'authentification dispose de données de configuration dupliquées.

Mappage des DN

Le service d'acquisition de droits d'accès de Policy Director mappe les certificats numériques de client transmis par le navigateur SSL à une identité Policy Director. 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 Policy Director tente alors de mapper ce certificat à une identité d'utilisateur reconnue par Policy Director.

Dans le fichier de configuration du SAD de Policy Director (cdas.conf), l'administrateur peut créer une table associant le DN d'un certificat à celui d'un utilisateur Policy Director. Lorsque WebSEAL soumet un certificat au SAD de Policy Director, celui-ci extrait d'abord son DN puis recherche son occurrence dans la table. S'il en trouve une, le SAD Policy Director renvoie à WebSEAL le DN d'utilisateur Policy Director associé. Cette procédure est appelé le mappage des DN.

WebSEAL utilise ensuite ce DN pour identifier l'utilisateur Policy Director. En l'absence d'occurrence, le SAD renvoie à WebSEAL le DN issu 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.

Le fichier de configuration cdas.conf, utilisé pour le mappage des noms distinctifs (DN), se trouve dans le répertoire suivant :

UNIX : `/opt/intraverse/cdas_server/lib/cdas.conf`

Windows : `C:\Program Files\IBM\Policy Director\cdas_server\lib\cdas.conf`

Le fichier de configuration cdas.conf contient les informations suivantes :

```
# Mappage des DN

# Si le DN du certificat est dans ce tableau, utiliser le DN LDAP
# correspondant. Sinon, utiliser le DN du certificat lui-même.
# Chaque entrée doit occuper une ligne et respecter ce format :
# [DN du certificat]DN LDAP correspondant
# Par exemple :
# [/C=US/O=IBM/CN=Policy Director User] cn=Policy Director User,o=IBM,c=FR
# [/C=US/O=IBM/CN=User1] cn=IBM Policy Director User,o=IBM,c=FR
```

Le DN du certificat se trouve toujours de côté gauche de la table et est obligatoirement entre crochets : `[/C=US/O=IBM/CN=Policy Director User]`. Le DN de l'utilisateur Policy Director (identique à celui contenu dans le registre LDAP) se trouve toujours de côté droit de la table : `cn=Policy Director User,o=IBM,c=FR`. Il suit toujours le crochet fermé du DN du certificat ( ]) après un espace obligatoire. Les deux côtés de l'entrée de table de mappage doivent être définis comme il convient pour que la configuration fonctionne.

Les navigateurs SSL, tels que Netscape Navigator/Communicator et Microsoft Internet Explorer, permettent d'afficher les DN des certificats. Le DN peut apparaître de différentes façons selon le navigateur utilisé mais tous ses éléments doivent être présents dans tous les cas.

Chapitre 14. WebSEAL - Tâches d'administration générale

Ce chapitre détaille les tâches de configuration et d'administration générale que vous devez exécuter pour adapter WebSEAL aux besoins de votre réseau.

Ce chapitre comprend les sections suivantes :

Activation et désactivation de la sécurité de WebSEAL

L'utilitaire **ivadmin** permet d'activer et de désactiver WebSEAL.

Pour activer WebSEAL sur un serveur Policy Director :

```
ivadmin> server enable /WebSEAL/nom_hôte
```

Où nom_hôte est le nom du serveur, sans le nom de domaine.

Lorsque le service est déjà activé ou que la spécification de service est incorrecte, Policy Director renvoie un message d'erreur.

Par défaut, Policy Director active WebSEAL.

Pour désactiver WebSEAL sur un serveur Policy Director, utilisez la commande **ivadmin server disable** :

```
ivadmin> server disable /WebSEAL/
```

Pour connaître l'état du serveur WebSEAL, utilisez la commande **ivadmin server status** :

```
ivadmin> server status nom_hôte
```

Le rapport d'état indique :

- si le serveur WebSEAL est activé ou désactivé ;
- si le serveur WebSEAL peut être contacté par un appel ping ;
- l'état de la base de données de configuration de WebSEAL.

Gestion de l'espace Web

Cette section décrit les tâches liées à l'administration de l'espace des noms de WebSEAL :

Spécification des emplacements des documents Web dans l'arborescence

L'emplacement des documents Web utilisés par le serveur s'exprime sous la forme d'un chemin d'accès absolu défini à partir de la racine de l'arborescence contenant ces documents. L'emplacement par défaut de chaque document est établi dès l'installation du gestionnaire de sécurité.

UNIX : *chemin_installation*/www/docs

Windows : *chemin_installation*\www\docs

Vous pouvez modifier cet emplacement à l'aide du script d'installation. Une fois l'installation faite, utilisez l'utilitaire **junctioncp** pour exécuter cette opération. Reportez-vous à la section «Gestion des jonctions intelligentes avec l'utilitaire junctioncp» à la page 195 pour une description complète de cette commande.

L'exemple suivant montre comment modifier l'emplacement des documents Web à l'aide de l'utilitaire **junctioncp**, pour une plate-forme UNIX :

1. Exécutez la commande **junctioncp** :

```
# junctioncp -e hostA
Tentative de liaison à hostA sur
/.:/subsys/intraverse/secmgr/server/hostA
junctioncp>
```

2. Utilisez la commande **list** pour afficher tous les points de jonction courants :

```
junctioncp> list
/
```

3. Utilisez la commande **show** pour afficher les propriétés d'une jonction :

```
junctioncp> show /

Point de jonction : /
Type : racine locale
Répertoire : /opt/intraverse/www/docs
```

4. Créez une jonction locale pour remplacer le point de jonction courant :

```
junctioncp> create -t local -d /tmp/docs /
Avertissement : Il existe déjà une jonction sur /
Voulez-vous la remplacer ? [no]? yes
Jonction créée sur /
```

5. Affichez le nouveau point de jonction :

```
junctioncp> list
/
```

6. Affichez les propriétés de cette jonction :

```
junctioncp> show /

Point de jonction : /
Type : racine locale
Répertoire : /tmp/docs
```

Configuration de l'indexation des répertoires

Vous pouvez définir le nom du fichier par défaut retourné par le serveur. Ce nom doit être indiqué lorsque vous spécifiez un nom de répertoire comme URL. Policy Director retourne ce fichier par défaut au client s'il existe. Dans le cas contraire, Policy Director génère dynamiquement un index des répertoires et l'envoie à ce client.

Remarque : Policy Director n'enregistre pas l'index généré sur le disque dur de la machine. Au lieu de cela, l'index est extrait du cache wand ou dirindex du serveur ou est régénéré chaque fois qu'un accès au répertoire intervient.

La strophe [wand-indexing] du fichier de configuration iv.conf contient des paramètres qui déterminent la configuration de l'indexation des répertoires.

La valeur du fichier par défaut est :

```
[wand-indexing]
dirindex = index.html
```

Si votre site applique une autre convention, vous devrez modifier ce nom de fichier :

```
[wand-indexing]
dirindex = default.html
```

Chaque paramètre utilisé pour l'indexation des répertoires est associé à une icône par défaut (fichier .gif) qui s'affiche pour chaque type de document et chaque type MIME détecté :

```
[wand-indexing]
image/*= /icons/image2.gif
video/* = /icons/movie.gif
audio/* = /icons/sound2.gif
text/html = /icons/html.gif
text/* = /icons/text.gif
application/* = /icons/binary.gif
```

Vous pouvez spécifier d'autres icônes pour chaque paramètre, localiser ces icônes à distance et utiliser des URL comme valeurs des paramètres. Par exemple :

```
application/* = http://www.acme.com/icons/binary.gif
```

Spécification des types d'extension de fichier pour les programmes CGI

Les paramètres contenus dans la strophe [wand-cgi-types] du fichier de configuration iv.conf permettent de définir les types d'extension des fichiers Windows. Policy Director reconnaît les types d'extension Windows des fichiers exécutables des programmes CGI.

Le système d'exploitation UNIX n'a aucune exigence en matière d'extension de nom de fichier. En revanche, vous devez définir ces types d'extension pour Windows NT. La strophe [wand-cgi-types] répertorie tous les types d'extension acceptés et associe chacun d'eux (le cas échéant) à un programme CGI approprié.

Par défaut, Policy Director n'exécute que les fichiers dont l'extension figure dans la liste de la strophe et uniquement si elle est associée à un programme CGI. Ceci ne concerne pas les fichiers .exe qui sont exécutés comme des programmes par défaut et ne demandent pas de mappage. Pour les fichiers dont l'extension indique des scripts interprétés, vous devez spécifier les interpréteurs appropriés. Les différents types d'extension comprennent .sh et .ksh (scripts shell), .pl (scripts Perl) et .tcl (scripts Tcl).

L'exemple suivant illustre une configuration type de la strophe [wand-cgi-types] :

```
#
# Mappages extensions de fichier CGI / commandes (Windows NT uniquement)
#
```

```
# Pour les serveurs WIN32, nous indiquons les extensions de fichier
# CGI et le programme
# utilisé pour les exécuter. Si l'extension d'un fichier CGI n'est
# pas dans cette liste, le fichier n'est pas exécuté.
#
[wand-cgi-types]
.exe =
.bat =
.cmd =
.pl = perl
.sh = sh
.tcl = tclsh76
```

Remarque : L'utilisation des fichiers .bat pose de sérieuses questions s'agissant de la sécurité du réseau. Pour plus de sûreté, n'utilisez pas ce type de fichier.

Configuration des unités d'exécution d'agent HTTP et HTTPS

Le nombre d'unités d'exécution d'agent configurées détermine le nombre de requêtes entrantes que le serveur peut satisfaire simultanément. Lorsque tous les agents sont occupés, Policy Director met en mémoire tampon les nouvelles demandes de connexion jusqu'à ce qu'une unité d'exécution d'agent se libère.

Vous pouvez définir le nombre d'unités d'exécution disponibles pour servir les connexions entrantes. Définissez ce nombre avec soin en raison des effets possibles sur les performances.

Ce paramètre de configuration n'impose pas de limite supérieure au nombre de connexions simultanées. Il ne fait que spécifier le nombre d'unités d'exécution mises à disposition pour traiter une file d'attente de travaux potentiellement illimitée.

Le nombre idéal d'unités d'exécution d'agent dépend de la quantité et du type de transactions intervenant dans votre réseau.

En général, plus ce nombre augmente, plus le temps moyen de traitement des requêtes est supposé diminuer. D'un autre côté, augmenter le nombre d'unités d'exécution affecte d'autres facteurs susceptibles de faire baisser les performances du serveur.

Configuration du pool d'unités d'exécution d'agent pour WebSEAL

WebSEAL administre une unique liste d'agents génériques ainsi qu'un pool d'unités d'exécution d'agent pour gérer les requêtes des clients utilisant la transmission par tunnel TCP, SSL, ou GSS. Ce mécanisme avancé permet à WebSEAL d'assurer un travail plus important tout en sollicitant moins les ressources du système.

La taille du pool d'unités d'exécution d'agent se définit par le biais du paramètre `worker-threads`, dans la strophe `[wand]` du fichier de configuration iv.conf.

```
worker-threads = 50
```

Configuration de WebSEAL pour les requêtes HTTP

Ordinairement, WebSEAL administre un grand nombre de requêtes HTTP provenant d'utilisateurs non authentifiés. Il peut être souhaitable cependant d'autoriser des utilisateurs inconnus (et donc non authentifiés) à accéder en lecture seule à une sélection de ressources sur un site Web public.

La strophe [wand] du fichier de configuration iv.conf contient des paramètres qui déterminent comment gérer les requêtes HTTP utilisant le protocole TCP.

Activation et désactivation de l'écoute des requêtes HTTP

Par défaut, Policy Director active (autorise) l'écoute des requêtes HTTP utilisant le protocole TCP :

```
allow-tcp-http = yes
```

Associez la valeur no à ce paramètre pour désactiver l'écoute HTTP.

Définition du numéro de port

Le numéro du port dédié par défaut à l'écoute des requêtes HTTP utilisant TCP est 80 :

```
http-tcp-port = 80
```

Pour le remplacer par le port 8080, entrez :

```
http-tcp-port = 8080
```

Configuration de WebSEAL pour les requêtes HTTPS

La strophe [wand] du fichier de configuration iv.conf contient des paramètres qui déterminent comment gérer les requêtes HTTPS (HTTP et SSL).

Activation et désactivation de l'écoute des requêtes HTTPS

Par défaut, Policy Director active (autorise) l'écoute des requêtes HTTPS :

```
allow-ssl-http = yes
```

Associez la valeur no à ce paramètre pour désactiver l'écoute HTTPS.

Définition du numéro de port

Le numéro du port dédié par défaut à l'écoute des requêtes HTTPS est 443 :

```
ssl-port = 443
```

Pour le remplacer par le port 4343, entrez :

```
ssl-port = 4343
```

Définition des paramètres de délai d'expiration

Vous pouvez définir les paramètres de délai d'expiration de Policy Director suivants :

- Paramètres de délai d'expiration des communications HTTP
- Paramètres de délai d'expiration du serveur WebSEAL (strophe [wand] du fichier de configuration iv.conf)

Paramètres de délai d'expiration des communications HTTP

WebSEAL gère les paramètres de délai d'expiration suivants pour les communications HTTPS :

ssl-init-connect-timeout (HTTPS uniquement)

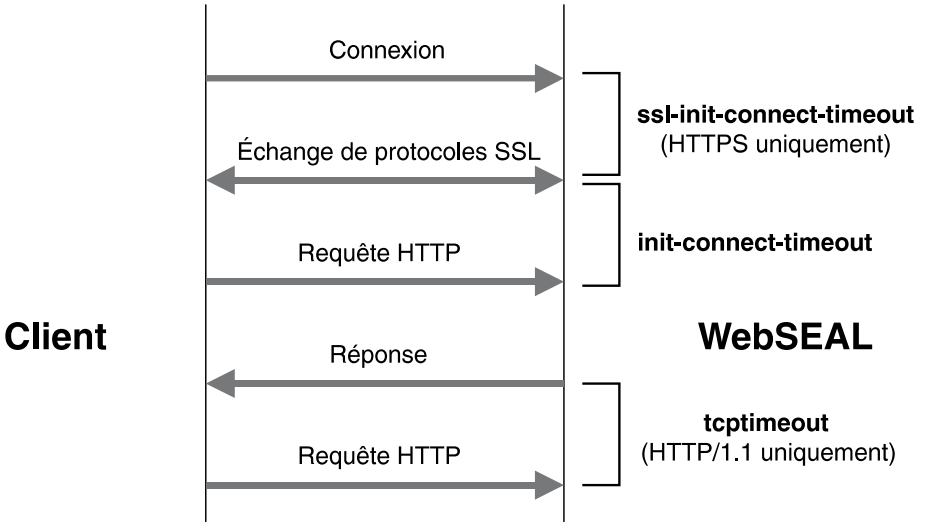
Lorsque WebSEAL accepte une demande de connexion SSL adressée par un navigateur, un échange de protocoles SSL doit avoir lieu. Le processus d'échange de protocoles consiste à échanger des signaux pour établir les communications entre deux modems. Le paramètre de délai d'expiration détermine le délai pendant lequel le gestionnaire de sécurité attend qu'un navigateur SSL initialise un échange de protocoles SSL. Cette initialisation intervient au début de la connexion SSL.

init-connect-timeout

Ce paramètre détermine le délai pendant lequel WebSEAL attend la première requête HTTP une fois l'échange de protocoles SSL terminé. Il peut s'agir d'une connexion HTTP, HTTPS, ou NetSEAT (HTTP et GSS).

tcptimeout

Ce paramètre concerne exclusivement les connexions HTTP/1.1 (pas HTTP/1.0). Il détermine le délai maximal (en secondes) pendant lequel le serveur maintient ouverte la connexion HTTP/1.1 une fois passées la première requête HTTP/1.1 et la première réponse du serveur. La connexion est fermée une fois ce délai atteint.



Paramètre	Fichier de configuration	Valeur par défaut (en secondes)
ssl-init-connect-timeout	strophe [ssl] de secmgrd.conf	120
init-connect-timeout	strophe [wand] de iv.conf	120
tcptimeout	strophe [wand] de iv.conf	5

Autres paramètres de délai d'expiration du serveur WebSEAL

La strophe [wand] du fichier de configuration iv.conf contient d'autres paramètres de délai d'expiration :

Paramètre	Description	Valeur par défaut (en secondes)
tcp-junction-timeout	Délai d'attente maximal pour envoyer et recevoir les requêtes et les réponses d'un serveur d'arrière-plan dans le cadre d'une jonction TCP.	120
ssl-junction-timeout	Délai d'attente maximal pour envoyer et recevoir les requêtes et les réponses d'un serveur d'arrière-plan dans le cadre d'une jonction SSL.	120
cgi-timeout	Délai d'attente maximal pour envoyer et recevoir les requêtes et les réponses d'un processus CGI local.	120

junction-ping-time	WebSEAL envoie périodiquement un appel ping en arrière-plan à chaque serveur relié au réseau par une jonction pour vérifier son état. Cet appel n'intervient pas plus d'une fois au cours de la période définie (300 secondes par défaut).	300

Configuration des messages d'erreur HTTP

Il arrive que le serveur WebSEAL tente de répondre à une requête et n'y parvienne pas. Cet échec peut avoir différentes causes. Par exemple :

- Un fichier nécessaire n'existe pas.
- Les autorisations définies interdisent l'accès.
- Les droits des fichiers UNIX, ou quelque chose de semblable, interdisent l'exécution des programmes CGI.

En cas d'impossibilité de répondre à une requête, le serveur retourne un message d'erreur au navigateur (par exemple `403 Interdit`) sous la forme d'une page HTML. Il existe de nombreux messages d'erreur, chacun d'eux étant contenu dans une page HTML.

Ces fichiers résident dans le répertoire suivant :

UNIX :

chemin_installation`/www/lib/errors/`*répertoire environnement local*

Windows :

chemin_installation`\www\lib\errors\`*répertoire environnement local*

Le répertoire `errors` contient plusieurs sous-répertoires d'environnement local. Ces sous-répertoires contiennent les fichiers des messages d'erreur traduits dans différentes langues.

Les messages de chaque répertoire sont au format HTML et peuvent s'afficher dans n'importe quel navigateur. Vous pouvez éditer ces fichiers pour personnaliser leur contenu. Les noms des fichiers reflètent les valeurs hexadécimales des codes d'erreur interne retournés en cas d'échec. Ne modifiez pas ces noms de fichier.

Le tableau suivant présente les noms et les contenus des fichiers des messages d'erreur les plus fréquemment utilisés :

Nom de fichier	Titre	Description	Code d'erreur HTTP
1354a2fa.html	Répertoire non vide	L'opération demandée nécessite la suppression d'un répertoire non vide. Cette opération est interdite.	
1898d25a.html	Impossible d'établir la connexion utilisateur.	La ressource demandée nécessite que le serveur Policy Director WebSEAL connecte l'utilisateur à un autre serveur Web. En outre, un incident s'est produit pendant que WebSEAL tentait de récupérer des informations.	

1898d25b.html	Il n'existe aucune données SSO pour cet utilisateur.	WebSEAL ne parvient à localiser l'utilisateur GSO pour la ressource demandée.	
1898d25c.html	Aucune destination SSO définie pour cet utilisateur.	WebSEAL ne parvient à localiser la destination GSO pour la ressource demandée.	
1898d25d.html	Plusieurs destinations de connexion sont définies pour l'utilisateur.	Plusieurs destinations GSO sont définies pour l'utilisateur demandé. Les destinations GSO sont mal configurées.	
1898d25e.html	Connexion obligatoire	La ressource demandée est protégée par un serveur Web d'arrière-plan relié au réseau via une jonction et WebSEAL doit connecter l'utilisateur à ce serveur Web. Pour y parvenir, l'utilisateur doit se connecter préalablement au serveur WebSEAL.	
1898d25f.html	Impossible d'établir la connexion utilisateur.	La ressource demandée nécessite que WebSEAL connecte l'utilisateur à un autre serveur Web. Cependant, les données de connexion de ce compte utilisateur sont incorrectes.	
1898d260.html	Question d'authentification inattendue	WebSEAL a reçu une question d'authentification inattendue d'un serveur Web d'arrière-plan relié par une jonction.	
1898d421.html	Déplacé provisoirement	La ressource demandée a été provisoirement déplacée. Ceci résulte sans doute d'une erreur de réorientation.	302
1898d424.html	Requête incorrecte	WebSEAL a réceptionné une requête HTTP incorrecte.	400
1898d425.html	Connexion obligatoire	La ressource demandée est protégée par WebSEAL et, pour y accéder, vous devez vous connecter préalablement.	
1898d427.html	Interdit	L'utilisateur n'a pas l'autorisation requise pour accéder à la ressource demandée.	403
1898d428.html	Non trouvé	La ressource demandée n'a pas été localisée.	404
1898d432.html	Service non disponible	Un service nécessaire à WebSEAL pour traiter une requête est actuellement indisponible.	503
1898d437.html	Le serveur est provisoirement indisponible.	Le serveur WebSEAL a été provisoirement suspendu par l'administrateur système. Aucune requête ne pourra être traitée tant que l'administrateur ne l'aura pas remis en service.	

1898d439.html	Les données de la session ont été perdues.	La dernière transaction entre le navigateur et le serveur a occasionné une session avec conservation de l'état avec un serveur d'arrière-plan relié au réseau par jonction. Ce serveur ne répond plus. WebSEAL a besoin d'un service installé sur ce serveur pour terminer le traitement de votre requête. Reportez-vous à la section «Gestion d'un état (option -s)» à la page 201.	
1898d7af.html	Le programme CGI a échoué.	L'exécution d'un programme CGI n'a pas abouti.	
default.html	Erreur du serveur	WebSEAL n'a pas pu traiter votre requête suite à une erreur.	500

Gestion des macro-commandes

Les macro-commandes suivantes peuvent être utilisées dans une page HTML de message d'erreur personnalisée. Ces macros modifient dynamiquement les informations existantes.

Macro	Description
ERROR_CODE	Valeur numérique du code d'erreur.
ERROR_TEXT	Texte associé au code d'erreur dans le catalogue de messages.
METHOD	Méthode HTTP demandée par le client.
URL	Adresse URL demandée par le client.
HOSTNAME	Nom complet du système hôte.
HTTP_BASE	Adresse URL HTTP de base du serveur : `http://`*`hôte`*`:`*`port_tcp`*`/`
HTTPS_BASE	Adresse URL HTTPS de base du serveur : `https://`*`hôte`*`:`*`port_ssl`*`/`
REFERER	Valeur de l'en-tête de référent de la requête, ou `Unknown` (inconnu) si aucun en-tête n'est défini.
BACK_URL	Valeur de l'en-tête de référent de la requête, ou / (si aucun en-tête).
BACK_NAME	Valeur `BACK`, si la requête contient un en-tête de référent, ou `HOME` si elle n'en contient pas.

Chapitre 15. WebSEAL - Administration des jonctions intelligentes

Le serveur WebSEAL peut fonctionner comme un serveur Web autonome ou comme un serveur de jonction capable de gérer des services d'autorisation et d'authentification pour le compte de serveurs d'applications d'arrière-plan. L'atout majeur de WebSEAL est sa capacité à intégrer et protéger des ressources Web supplémentaires résidant sur des serveurs d'applications d'arrière-plan. Pour servir cet objectif, le serveur WebSEAL fait appel à la technologie Smart Junction (jonction intelligente).

Ce chapitre comprend les sections suivantes :

Utilisation de WebSEAL comme serveur de jonction intelligente

Policy Director apporte à votre réseau des services d'authentification, d'autorisation et de gestion. Dans le contexte d'un réseau ouvert sur le Web, ces services sont mieux gérés par un serveur WebSEAL frontal. Le serveur WebSEAL frontal protège les ressources Web installées sur les serveurs d'applications d'arrière-plan.

La connexion reliant un serveur WebSEAL à un serveur d'arrière-plan est appelée une jonction intelligente, ou plus simplement une jonction. La jonction permet de fusionner les espaces Web physiques du serveur WebSEAL et des serveurs d'arrière-plan en une unique représentation logique d'un espace Web global.

Le client n'a jamais besoin de connaître l'emplacement physique d'une ressource Web. WebSEAL convertit les adresses URL logiques en adresses physiques utilisables par un serveur d'arrière-plan. Vous pouvez déplacer les objets Web d'un serveur à un autre sans aucunement modifier la manière dont le client accède à ces objets.

En tant que serveur de jonction, WebSEAL peut exécuter des contrôles d'autorisation et d'authentification sur toutes les requêtes avant de les transmettre à un serveur d'arrière-plan. Les jonctions permettent de mettre en place un environnement sécurisé évolutif qui offre un bon équilibrage de charge, une accessibilité avancée et des possibilités de gestion d'état, tout ceci de manière transparente du point de vue des clients. De plus, la gestion centralisée de l'espace des noms facilite le travail des administrateurs.

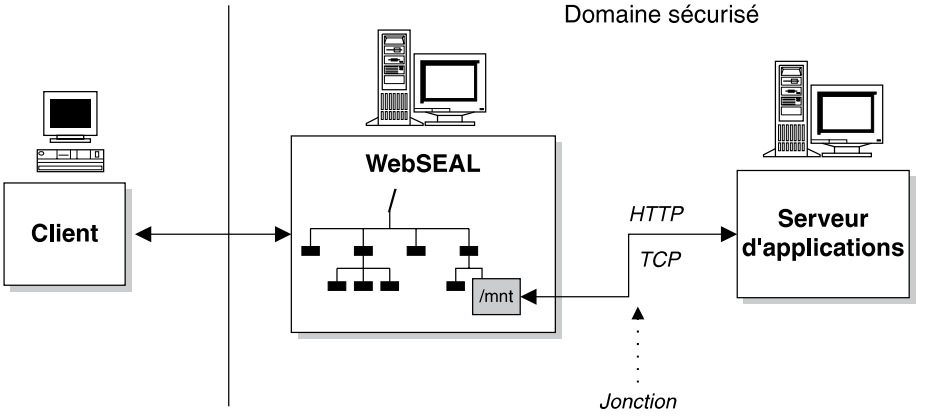
La plupart des serveurs Web à vocation commerciale n'ont pas la possibilité de définir un espace des noms Web logique. Leur contrôle d'accès est lié à la structure des fichiers physiques et des répertoires. Les jonctions intelligentes

permettent de définir de manière transparente un espace des noms reflétant la structure d'une organisation plutôt que celle de la machine et de ses répertoires, comme on le rencontre souvent avec les serveurs Web standard.

Les jonctions intelligentes permettent également de créer des solutions de connexion unique (SSO). Une configuration SSO permet à un utilisateur d'accéder à une ressource, quelque soit l'emplacement de celle-ci, à partir de sa seule connexion initiale. Toutes les autres connexions nécessaires à l'opération sont traitées de manière transparente du point de vue de l'utilisateur.

Principes des jonctions intelligentes

Une jonction intelligente est une connexion TCP/IP physique entre un serveur WebSEAL frontal et un serveur d'applications d'arrière-plan. Le serveur d'arrière-plan peut être un autre serveur WebSEAL ou un serveur d'applications tiers. L'espace Web du serveur d'applications d'arrière-plan se connecte au serveur WebSEAL en un point de jonction (point de montage) précisément défini dans l'espace Web du serveur WebSEAL.

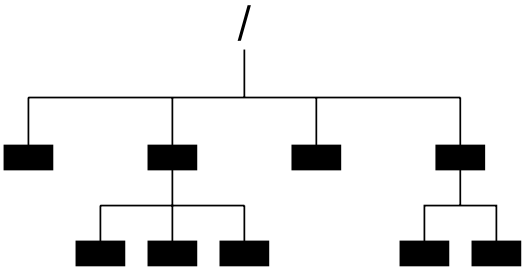


Une jonction intelligente permet à WebSEAL d'offrir des services de protection au serveur d'applications d'arrière-plan. Le serveur d'arrière-plan requiert un contrôle d'accès renforcé pour ses objets. Lorsque ce contrôle est effectivement demandé, vous devez configurer le service de sécurité de Policy Director pour y définir l'espace Web du serveur tiers.

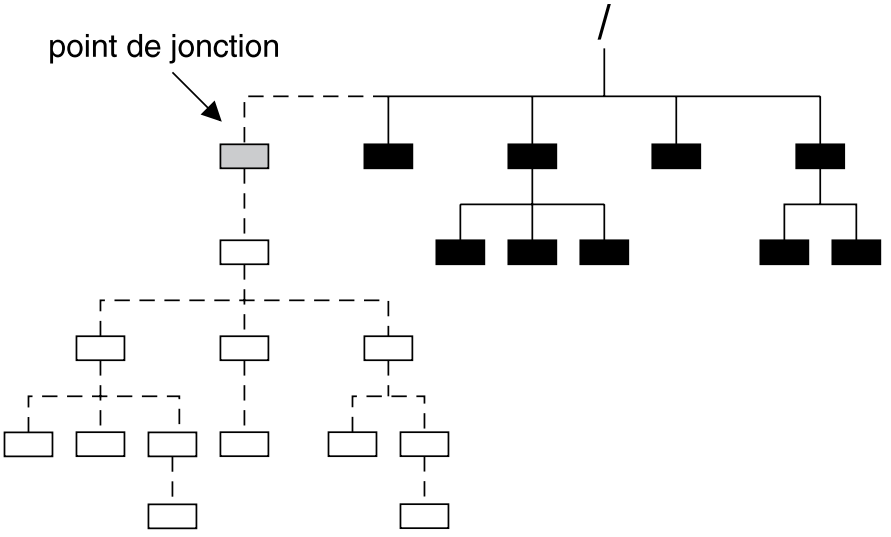
Une fois configuré, WebSEAL protège alors ses propres ressources ainsi que celles du serveur relié par jonction, par le biais de ses services de sécurité (authentification, autorisation et audit).

Les jonctions intelligentes permettent la fusion logique de l'espace Web du serveur WebSEAL et de l'espace Web du serveur d'arrière-plan. De la coopération ainsi instaurée entre ces serveurs naît un unique espace Web partagé dont la complexité est imperceptible pour les utilisateurs.

Un espace Web unifié simplifie aussi la gestion des ressources pour l'administrateur système. Les autres avantages acquis, en termes d'administration, sont la modularité, l'équilibrage de charge et l'accessibilité avancée.



Espace Web du serveur WebSEAL



Espace Web combiné :
WebSEAL et serveur relié au réseau par jonction

Les jonctions intelligentes rendent un site WEB plus évolutif. Elles permettent notamment de répondre à l'augmentation des demandes d'accès en reliant ce site à d'autres serveurs.

Jonctions intelligentes et modularité des sites WEB

Les jonctions intelligentes rendent les sites WEB plus évolutifs. A mesure qu'augmente le nombre des demandes d'accès à votre site WEB, vous pouvez facilement lui adjoindre de nouveaux serveurs pour accroître ses capacités. L'ajout de nouveaux serveurs par le biais de jonctions peut avoir les raisons suivantes :

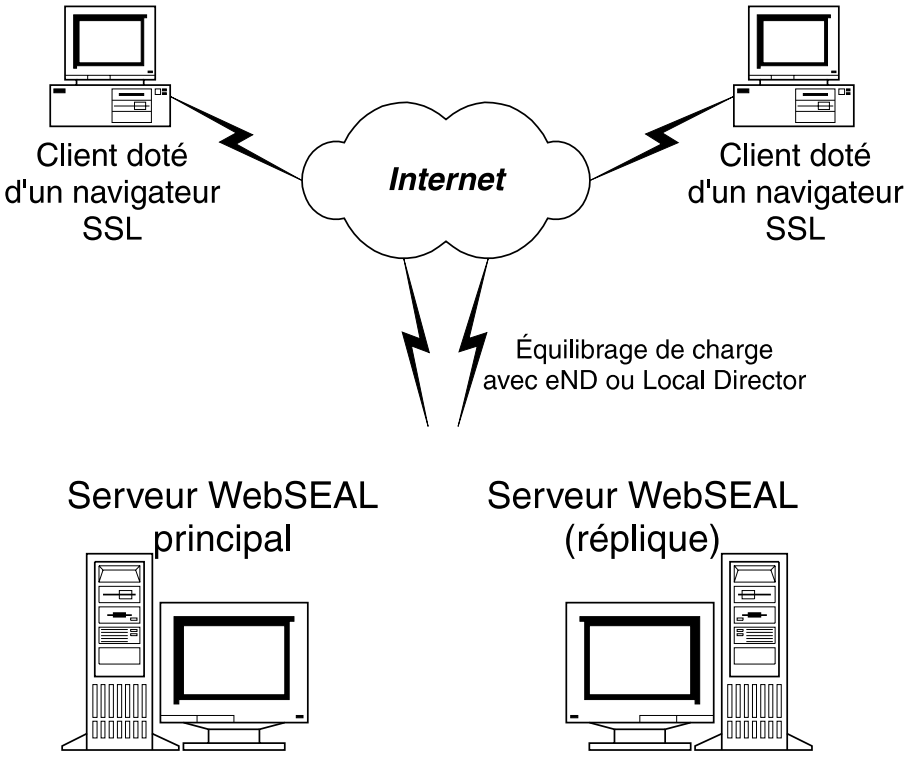
- Pour agrandir le site en augmentant son contenu.
- Pour dupliquer le contenu existant pour des motifs d'équilibrage de charge, d'accessibilité avancée ou simplement comme recours en cas de panne.

Duplication des serveurs WebSEAL frontaux

L'établissement de jonctions avec des serveurs d'arrière-plan nécessite au moins un serveur WebSEAL frontal. La duplication des serveurs WebSEAL frontaux

permet l'équilibrage de la charge du site sur les périodes de forte demande. Une application (par exemple Policy Director eND ou Cisco Local Director) gère le mécanisme d'équilibrage de charge.

Cette duplication permet aussi au site de proposer une solution de repli en cas de panne. Si un serveur tombe en panne pour une raison quelconque, les autres serveurs continueront d'assurer l'accès au site. L'équilibrage de charge et la capacité de recours procurent conjointement une accessibilité avancée aux utilisateur du site.



La duplication des serveurs WebSEAL frontaux implique deux aspects fondamentaux :

- Chaque serveur doit posséder une copie exacte de l'espace Web.
- Vous devez aussi dupliquer la base de données des comptes des utilisateurs pour que l'authentification soit cohérente.

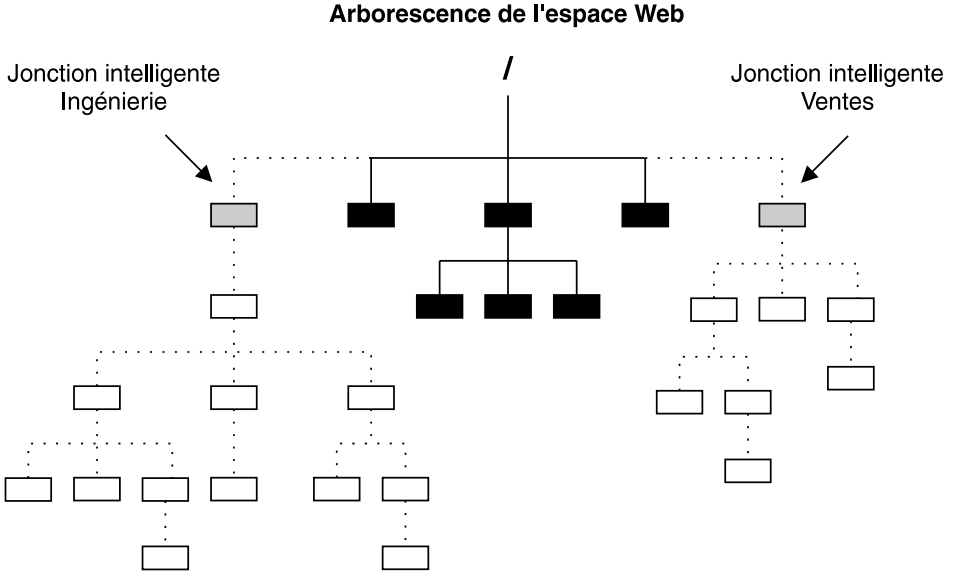
Le service d'autorisation de Policy Director duplique automatiquement la base de données des autorisations aux emplacements requis.

Prise en charge des serveurs d'arrière-plan

Le serveur WebSEAL lui-même, un ou des serveurs d'arrière-plan, ou une combinaison des deux, peuvent répondre aux besoins d'un site WEB. L'utilisation de jonctions intelligentes avec les serveurs d'arrière-plan permet de faire évoluer le site WEB par l'ajout de contenus et de ressources supplémentaires.

Chaque serveur d'arrière-plan doit être relié au réseau sur un point de jonction (point de montage) distinct. A mesure que la demande de contenu et de ressources augmente, vous pouvez ajouter d'autres serveurs à l'aide de jonctions intelligentes. Cette approche constitue une solution pour les réseaux ayant largement investi dans des serveurs Web tiers.

Le schéma suivant illustre comment les jonctions intelligentes permettent de créer un espace Web logique unifié. Cet espace Web est transparent du point de vue de l'utilisateur et peut être géré de manière centralisée.



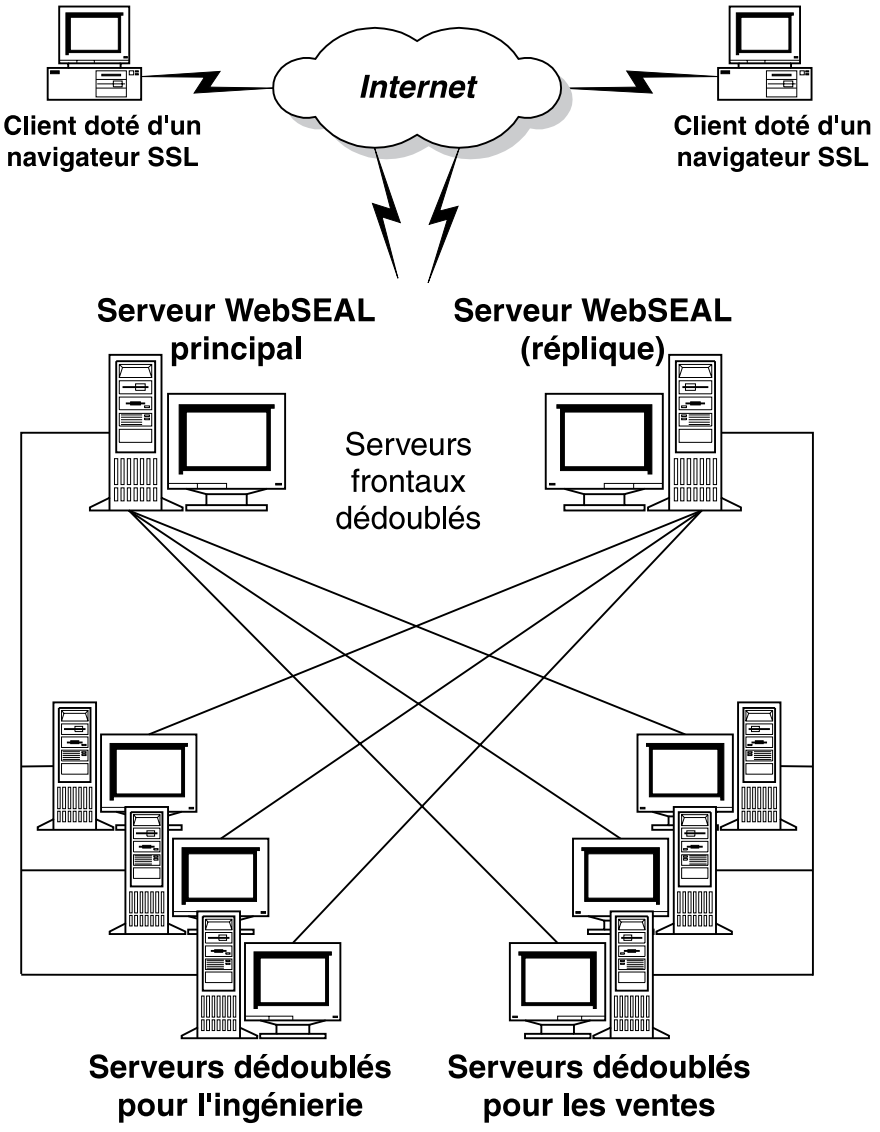
Les serveurs d'arrière-plan dupliqués sont reliés au réseau sur le même point de jonction comme décrit dans la section «Duplication des serveurs d'arrière-plan».

Duplication des serveurs d'arrière-plan

Pour étendre encore davantage la modularité du réseau, pour pouvez également dupliquer des serveurs d'arrière-plan. Comme pour la duplication des serveurs frontaux, les serveurs d'arrière-plan dupliqués doivent contenir la copie des espaces Web de leurs homologues.

WebSEAL équilibre la charge entre les serveurs dupliqués à l'aide d'un algorithme de répartition fonctionnant sur le principe du "moins occupé". WebSEAL se replie sur le serveur de secours lorsqu'un serveur tombe en panne et relance ce dernier lorsqu'il redevient opérationnel.

Si l'application d'arrière-plan demande à garder cet état pour plusieurs pages, vous pouvez utiliser des jonctions avec conservation de l'état. Ces jonctions avec conservation de l'état font revenir chaque session au même serveur d'arrière-plan. Reportez-vous à la section «Gestion d'un état (option -s)» à la page 201.



Synthèse des tâches à conduire pour la création de jonctions

Vous pouvez créer les types de jonction suivants :

- Policy Director / serveur tiers : connexion TCP
- Policy Director / serveur tiers : connexion SSL
- Policy Director / système de fichiers local

Les tâches à exécuter pour établir une jonction entre l'espace Web d'une application d'arrière-plan et celui de WebSEAL sont les suivantes :

1. Choisissez dans l'espace Web de WebSEAL l'emplacement où monter la jonction avec les nouveaux serveurs.
2. Déterminez les conditions de sécurité à appliquer pour garantir l'intégrité de votre réseau.

Contrôle d'accès allégé

Pour établir un contrôle d'accès allégé :

1. Montez une jonction intelligente entre le serveur d'application tiers d'arrière-plan et le serveur WebSEAL à l'aide de l'utilitaire de Policy Director **junctioncp**.

2. Placez un modèle de règle (LCA) adapté sur le point de jonction pour établir un contrôle d'accès allégé sur le serveur d'arrière-plan.

Contrôle d'accès renforcé

Pour établir un contrôle d'accès renforcé :

1. Montez une jonction intelligente entre le serveur d'application tiers d'arrière-plan et le serveur WebSEAL à l'aide de l'utilitaire **junctioncp**.

   WebSEAL ne peut pas voir ou comprendre un système de fichiers tiers de manière automatique. Vous devez lui faire connaître le contenu de cet espace des noms tiers à l'aide du programme **query_contents**. Cette application dresse l'inventaire de l'espace Web tiers et rapporte sa structure à WebSEAL.
2. Copiez le programme **query_contents** sur le serveur tiers.
3. Utilisez la console de gestion pour appliquer les modèles de règle (LCA) aux objets nécessitant une protection dans l'espace Web unifié.

Recommandations pour la création des jonctions intelligentes

Les recommandations suivantes illustrent les règles appliquées aux jonctions intelligentes :

- Vous pouvez monter une jonction intelligente n'importe où dans l'espace des noms primaire de WebSEAL.
- Plusieurs instances d'un même serveur peuvent être reliées au réseau via le même point de montage (point de jonction).
- Ces répliques doivent obligatoirement être du même type (TCP ou SSL).
- Les serveurs tiers ne peuvent pas être montés en chaîne (par exemple, Policy Director — tiers — tiers).

Contrôle d'accès et privilèges d'administrateur

Par défaut, le compte de l'administrateur de la cellule détient tous les droits sur l'ensemble de l'espace Web, ceci comprenant celui des serveurs reliés par des jonctions. L'administrateur d'un serveur relié par jonction n'est responsable que de l'espace Web associé à son serveur. En revanche, si cela s'avère nécessaire, il peut retirer des privilèges à l'administrateur de la cellule pour ce qui concerne son serveur.

Par le jeu de l'héritage, les listes de contrôle d'accès se transmettent aux serveurs tiers via les jonctions intelligentes.

Gestion des jonctions intelligentes avec l'utilitaire junctioncp

L'utilitaire **junctioncp** permet de réaliser toutes les tâches de gestion des jonctions :

- Création d'un nouveau point de jonction
- Ajout d'un serveur sur un point de jonction
- Suppression d'un serveur monté sur un point de jonction
- Suppression d'un point de jonction
- Affichage de la liste des points de jonction
- Affichage des propriétés d'une jonction

L'utilitaire **junctioncp** comporte une invite de commande interactive qui permet de taper les commandes de gestion des jonctions.

Avant d'exécuter **junctioncp**, vous devez vous connecter au domaine sécurisé en qualité d'utilisateur administratif. Vous pouvez utiliser dce_login dans un environnement UNIX ou Windows, ou netseat_login dans un environnement Windows.

Démarrez l'utilitaire **junctioncp** avec l'option **-e** pour indiquer le serveur (nom d'hôte) concerné par les tâches de gestion des jonctions. L'invite de commande de **junctioncp** apparaît.

Par exemple :

UNIX :

```
#
# junctioncp -e nom_serveur

junctioncp>
```

Windows :

```
junctioncp -e <nom_serveur>

junctioncp>
```

Utilisation des commandes de junctioncp

L'utilitaire **junctioncp** dispose des commandes suivantes :

Commande	Description
create	Crée une jonction pour un premier serveur.
add	Ajoute de nouveaux serveurs sur un point de jonction existant.
remove	Supprime un serveur monté sur un point de jonction.
delete	Supprime un point de jonction.
list	Affiche la liste des points de jonction montés dans l'espace des noms du serveur.
show	Affiche les propriétés d'une jonction.
help	Affiche la liste des commandes de **junctioncp**.
help commande	Affiche une rubrique d'aide sur une commande de l'utilitaire **junctioncp**.
exit	Quitte l'utilitaire **junctioncp**.

Pour plus d'informations sur ces commandes et sur leurs options, reportez-vous à la section «Création d'une jonction pour un premier serveur».

Création d'une jonction pour un premier serveur

Opération : Monte un point de jonction et y établit une jonction avec un premier serveur.

Syntaxe : `create -t type -h nom_hôte options point_jonction`

type

Au choix : • **tcp** • **ssl** • **local**		Argument obligatoire Définit le type de la jonction. Choisissez **tcp** pour les serveurs d'arrière-plan tiers. Si vous sélectionnez **ssl**, le port TCP par défaut (80) devient 443. Reportez-vous à la section «Création de jonctions intelligentes SSL sécurisées» à la page 202.
options		
	Options de jonction TCP et SSL (s'emploient avec **-t tcp** ou **-t ssl**)	
	-2	Etablit des communications avec le serveur d'arrière-plan exclusivement avec le protocole SSL version 2. Reportez-vous à la section «Création de jonctions intelligentes SSL sécurisées» à la page 202.
	-b valeur Au choix : • **filter** (par défaut) • **ignore** • **supply** • **gso**	Détermine comment le serveur WebSEAL communique les données d'authentification aux serveurs d'arrière-plan. Reportez-vous à la section «Communication de données d'authentification aux serveurs reliés par jonction» à la page 207.
	-c	Insère l'identité du client Policy Director dans les en-têtes HTTP. Reportez-vous à la section «Insertion des données d'identité du client (option -c)» à la page 201.
	-i	Demande au serveur WebSEAL de ne pas tenir compte des différences de format de caractères dans les URL. Reportez-vous à la section «Gestion des URL sans différenciation du format des caractères (option -i)» à la page 199.
	-h nom_hôte	Argument obligatoire Nom d'hôte (DNS) du serveur d'arrière-plan de destination. A défaut, vous pouvez indiquer son adresse IP.
	-p port	Port TCP du serveur d'arrière-plan tiers. La valeur par défaut est de 80 pour les jonctions TCP et de 443 pour les jonctions SSL.
	-q url	URL du script de **query_contents**. Policy Director recherche le programme **query_contents** dans /cgi_bin/. Si ce répertoire est différent ou que le fichier de **query_contents** a été renommé, utilisez cette option pour indiquer à WebSEAL sa nouvelle URL. Utilisez cette option **-q** lorsque vous créez une jonction intelligente pour relier le serveur Win32 tiers au réseau. Reportez-vous à la section «Configuration d'une jonction intelligente pour utiliser query_contents» à la page 216.
	-s	Indique que la jonction doit supporter les applications avec conservation de l'état. Par défaut, les jonctions ne sont pas avec conservation de l'état. Reportez-vous à la section «Gestion d'un état (option -s)» à la page 201.

	-T ressource	Nom de l'application associée aux droits d'accès des ressources GSO. Obligatoire et exclusivement utilisé pour l'option **-b gso**. Reportez-vous à la section «Intégration du serveur GSO et de la solution SSO de WebSEAL» à la page 210.
	-v nom_hôte	Nom d'hôte virtuel du serveur.
	-w	Spécifie le support du système de fichiers Win32. Reportez-vous à la section «Interdiction des noms de fichier courts (option -w)» à la page 200.
	Options des jonctions locales et DFS (s'emploient avec **-t dfs** ou **local**)	
	-d répertoire	Système de fichiers distribué (DFS) ou répertoire local cible de la jonction. Argument obligatoire
point_jonction		
	Emplacement de l'espace des noms de WebSEAL où la jonction doit être montée.	

Ajout d'un nouveau serveur sur une jonction existante

Opération : Ajoute un serveur supplémentaire sur un point de jonction existant.

Syntaxe : `add -h` *`nom_hôte options point_jonction`*

options		
	Options de jonction TCP et SSL	
	-i	Demande au serveur WebSEAL de ne pas tenir compte des différences de format de caractères dans les URL. Reportez-vous à la section «Gestion des URL sans différenciation du format des caractères (option -i)» à la page 199.
	-h nom_hôte	Argument obligatoire Nom d'hôte (DNS) du serveur d'arrière-plan de destination. A défaut, vous pouvez indiquer son adresse IP.
	-p port	Port TCP du serveur d'arrière-plan tiers. La valeur par défaut est de 80 pour les jonctions TCP et de 443 pour les jonctions SSL.
	-q url	URL du script de **query_contents**. Policy Director recherche le programme **query_contents** dans /cgi_bin/. Si ce répertoire est différent ou que le fichier de **query_contents** a été renommé, utilisez cette option pour indiquer à WebSEAL sa nouvelle URL.
	-v nom_hôte	Nom d'hôte virtuel du serveur.
	-w	Spécifie le support du système de fichiers Win32. Reportez-vous à la section «Interdiction des noms de fichier courts (option -w)» à la page 200.
point_jonction		
	Ajoute un serveur sur ce point de jonction.	

Utilisation des autres commandes de junctioncp

Les sections «Création d'une jonction pour un premier serveur» à la page 196 et «Ajout d'un nouveau serveur sur une jonction existante» à la page 198 détaillent les commandes **junctioncp create** et **junctioncp add**. Le tableau suivant répertorie les autres commandes de l'utilitaire **junctioncp** :

Commande	Description
remove	**Opération :** Supprime un serveur monté sur un point de jonction. **Syntaxe :** `remove -i id_serveur point_jonction` **Options : -i** id_serveur ID du serveur à supprimer de la jonction. Utilisez la commande show pour déterminer l'ID d'un serveur donné.
delete	**Opération :** Supprime un point de jonction. **Syntaxe :** `delete point_jonction`
show	**Opération :** Affiche les propriétés d'une jonction. **Syntaxe :** `show point_jonction`
list	**Opération :** Affiche la liste des jonctions existantes. **Syntaxe :** `list`
help	**Opération :** Affiche la liste des commandes de l'utilitaire **junctioncp**. **Syntaxe :** `help`
help commande	**Opération :** Affiche une rubrique d'aide sur une commande de **junctioncp** et sur ses options. **Syntaxe :** `help commande`
exit	**Opération :** Quitte l'utilitaire **junctioncp** et revient à l'invite du système d'exploitation. **Syntaxe :** `exit`

Gestion des URL sans différenciation du format des caractères (option -i)

L'option **-i**, utilisée lors de jonctions avec des serveurs tiers, demande à WebSEAL de traiter les URL sans différencier les majuscules des minuscules. Le serveur ne distinguera pas ces deux formats de caractère lors de l'analyse syntaxique des URL. Notez que, par défaut, les serveurs font cette distinction.

Bien que la plupart des serveurs HTTP gèrent la spécification d'URL HTTP, avec distinction des majuscules et minuscules, certains de ces serveurs traitent les URL sans faire cette distinction.

Par exemple, sur les serveurs ne la faisant pas, les deux URL suivantes apparaîtront de la même manière :

```
http://server/ventes/index.htm

http://server/VENTES/index.HTM
```

Ce mode opératoire implique que Policy Director place les mêmes listes de contrôle d'accès sur les deux URL. Par défaut, Policy Director traite les URL en distinguant

les majuscules des minuscules lors de l'application des modèles de règle. Lors d'une jonction avec un serveur tiers, si vous spécifiez l'option **-i**, WebSEAL traitera les URL désignant ce serveur sans distinguer ces deux formats de caractère.

Interdiction des noms de fichier courts (option -w)

L'objectif de cette mesure est de limiter le contrôle d'accès à une seule représentation d'un objet. Ne laissez pas de brèches permettant de contourner le système de sécurité.

WebSEAL effectue des contrôles de sécurité sur les requêtes adressées par les clients aux serveurs d'arrière-plan liés au réseau par jonction, sur la base des chemins de fichier spécifiés dans les URL. Ce contrôle de sécurité peut être imparfait dans la mesure où les systèmes de fichiers Win32 disposent de deux méthodes pour accéder aux noms de fichier longs.

La première reconnaît l'intégralité du nom de fichier (`abcdefghijkl.txt`). La deuxième utilise l'ancien format de nom de fichier du DOS 8.3 pour la compatibilité amont (`abcdef~1.txt`).

L'option **-w** ajoutée à la commande **junctioncp** interdit l'usage du format de nom de fichier DOS 8.3. Un utilisateur ne peut donc pas éviter une liste de contrôle d'accès explicitement attachée à un nom de fichier long en utilisant la forme courte (DOS 8.3) de ce nom de fichier. Le serveur renvoie un message d'erreur `403 Interdit` devant tout nom de fichier court entré.

Windows traite de la même manière le nom de fichier "foo." et le nom de fichier "foo", qui n'est pas suivi d'un point. L'option **-w** supprime les points de fin des noms de fichier entrés dans une URL avant d'envoyer la requête au serveur d'arrière-plan. Policy Director définit les contrôles par LCA d'après les noms de fichier ; sans point de fin.

Remarque : L'option **-i** résout le problème que pose la non-distinction par Win32 des majuscules et des minuscules (`abced.txt` = `AbCdE.txt`).

Exemple :

Sur Windows NT 4.0, vous pouvez accéder au fichier \Program Files\ibm corp\readme.txt par des chemins exprimés différemment :

1. \program files\ibm corp.\readme.txt
2. \program files\ibm corp\readme.txt
3. \progra~1\ibm~2\readm~3.txt

Le premier exemple ci-dessus illustre l'effet de la non-distinction des majuscules et des minuscules. L'option **-i** (et non pas l'option **-w**) résout ce problème.

L'exemple 2 illustre comment Windows NT ignore le point d'extension de fin.

L'exemple 3 illustre comment Windows NT génère un alias pour assurer la compatibilité avec le DOS. Cet alias ne doit contenir aucun espace pour respecter le format du DOS 8.3.

L'option **-w** comble les brèches du système de sécurité (voir les exemples 2 et 3). Elle demande à Policy Director d'ignorer les points de fin et de rejeter les requêtes adressées au serveur relié par jonction et contenant une URL intégrant un nom de fichier court avec un caractère "~".

Gestion d'un état (option -s)

La plupart des applications Web gèrent un état tout au long des requêtes HTTP d'une session de client. Par exemple, gérer cet état permet de :

- suivre la progression d'un utilisateur à travers les zones de saisie d'un formulaire de données généré par un programme CGI ;
- gérer le contexte d'un utilisateur au cours d'une série de requêtes de base de données ;
- gérer une liste d'articles dans une application de magasin virtuel où un utilisateur navigue au hasard dans les pages et sélectionne les articles qu'il désire acheter.

Comme n'importe quel serveur, vous pouvez dupliquer les serveurs exécutant des applications Web pour en améliorer les performances par l'équilibrage de charge. Le serveur Policy Director peut établir une jonction intelligente pour ces instances de serveur. Dans ce contexte, Policy Director doit s'assurer que toutes les requêtes formulées au cours d'une session de client sont bien acheminées au serveur qui convient. Il doit aussi contrôler que les requêtes ne sont pas réparties entre les instances du serveur en vertu des règles d'équilibrage de charge.

Par défaut, Policy Director équilibre la charge du serveur en répartissant les requêtes entre toutes les instances disponibles. Policy Director applique un algorithme déterminant le serveur le "moins occupé".

Pour contourner l'effet de l'équilibrage de charge et créer une jonction avec conservation de l'état, utilisez la commande **junctioncp** avec l'option **-s**. La jonction avec conservation de l'état permet aux requêtes d'un client d'être systématiquement acheminées au même serveur pendant toute la session.

Insertion des données d'identité du client (option -c)

L'option **-c** permet d'insérer les données de l'identité Policy Director des clients et leur appartenance de groupe dans les en-têtes des requêtes HTTP. Dans le cas présent, les requêtes HTTP sont destinées aux serveurs tiers reliés au réseau par une jonction. Les en-têtes HTTP définis par Policy Director permettent aux applications installées sur les serveurs tiers reliés par jonction d'exécuter des actions sur les utilisateurs. Ces actions reposent sur l'identité Policy Director du client.

Pour que les données des en-têtes HTTP puissent être utilisées par un service installé sur le serveur d'arrière-plan, vous devez les convertir en variables d'environnement. Pour cela, remplacez tous les tirets (-) par des signes soulignés (_) et ajoutez "HTTP" au début de la chaîne. La valeur de l'en-tête HTTP devient celle de la nouvelle variable d'environnement.

Les en-têtes HTTP définis par Policy Director comprennent :

En-tête HTTP défini par Policy Director	Variable d'environnement CGI	Description
iv-user	HTTP_IV_USER	Nom du client. Devient par défaut **unauthenticated** lorsque le client n'est pas authentifié (est inconnu).
iv-groups	HTTP_IV_GROUPS	Liste des groupes auxquels le client appartient. Se compose d'entrées séparées par des espaces.

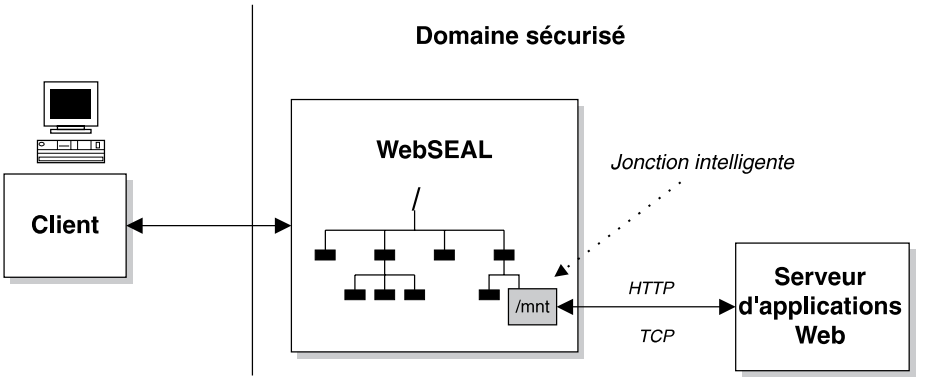
iv-creds	HTTP_IV_CREDS	Structure de données codée représentant un droit d'accès de ressource Policy Director. S'utilise conjointement avec l'API d'autorisation de Policy Director. Pour plus d'informations, reportez-vous au manuel Policy Director - Guide de programmation et de référence.

Les en-têtes HTTP sont communiqués aux programmes CGI sous la forme des variables d'environnement HTTP_IV_USER, HTTP_IV_GROUP et HTTP_IV_CREDS. Pour savoir comment extraire les en-têtes des requêtes HTTP avec d'autres applications, reportez-vous à la documentation des produits concernés.

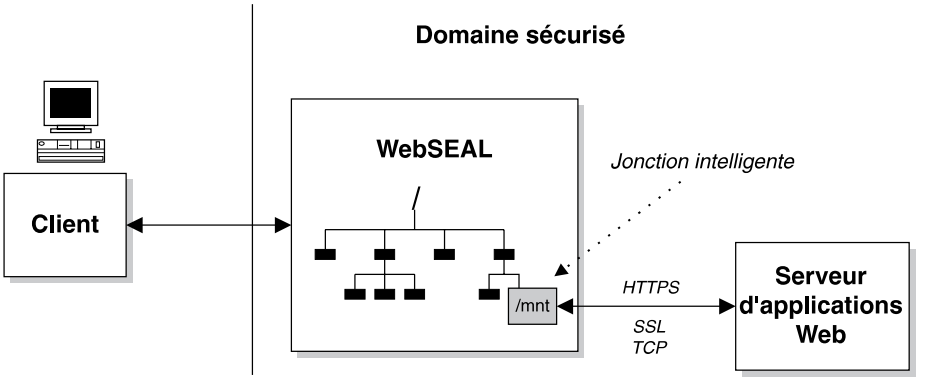
Création de jonctions intelligentes SSL sécurisées

WebSEAL permet de créer des jonctions TCP (HTTP) standard et des jonctions SSL (HTTPS) sécurisées entre lui-même et les serveurs d'arrière-plan. Les jonctions SSL fonctionnent de la même manière que les jonctions TCP mais permettent en plus de coder les communications entre WebSEAL et le serveur d'arrière-plan.

L'illustration suivante présente une jonction TCP (HTTP) non sécurisée.



L'illustration suivante présente une jonction SSL (HTTPS) sécurisée.



La jonction entre WebSEAL et le serveur d'arrière-plan est indépendante du type (et du niveau de sécurité) de la connexion établie entre le client et le serveur WebSEAL.

Les jonctions SSL permettent des transactions sécurisées entre les deux extrémités de la connexion : le navigateur et l'application. Utilisez une jonction SSL pour sécuriser les communications entre le client et WebSEAL comme entre WebSEAL et les serveurs d'arrière-plan.

Configuration d'une jonction SSL sécurisée

Les jonctions intelligentes SSL nécessitent que le serveur Web d'arrière-plan puisse utiliser le protocole HTTPS.

L'utilitaire **junctioncp** permet de créer une jonction intelligente. Reportez-vous à la section «Gestion des jonctions intelligentes avec l'utilitaire junctioncp» à la page 195 pour plus d'informations sur l'utilitaire **junctioncp**.

Pour créer une jonction SSL sécurisée et y ajouter un premier serveur, utilisez la commande **junctioncp create**. L'exemple suivant illustre la syntaxe de la commande create qui permet de créer une jonction SSL sécurisée :

```
junctioncp> create -t ssl [-2] -h nom_hôte
[-p port] point_jonction
```

L'option **-2** oblige Policy Director à communiquer avec le serveur d'arrière-plan avec SSL version 2 exclusivement.

En principe, Policy Director négocie automatiquement la version de protocole SSL utilisée (version 2 ou 3). Policy Director a prévu cette option **-2** dans la mesure où certains serveurs IIS ne permettent pas d'utiliser SSL version 3. Dans cette situation, le montage échoue. Rendre obligatoire l'utilisation de la version 2 résout ce problème.

Exemples de jonction SSL

Pour établir une jonction entre l'hôte ventes.ibm.com sur le point de jonction /ventes qui utilise le protocole SSL, entrez :

```
create -t ssl -h ventes.ibm.com /ventes
```

Pour établir une jonction entre l'hôte admin.ibm.com sur le point de jonction /admin qui utilise le protocole SSL version 2 exclusivement, entrez :

```
create -t ssl -2 -h admin.ibm.com /admin
```

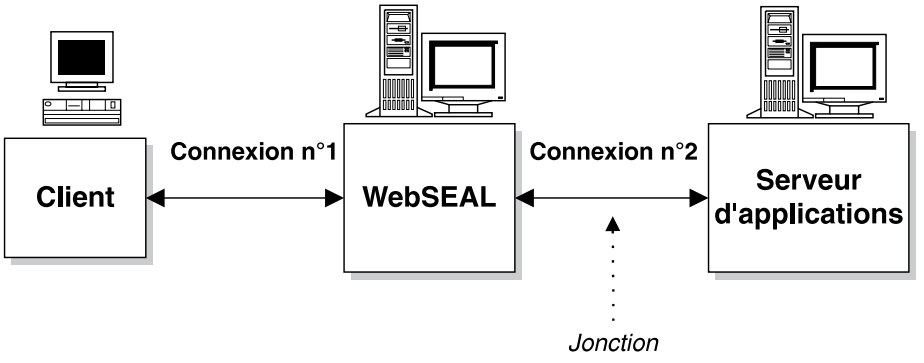
Remarque : Dans ces deux exemples, l'option **-t ssl** spécifie le port par défaut 443.

Pour établir une jonction entre l'hôte voyage_svr, sur le port 4343, au point de jonction /voyage qui utilise le protocole SSL, entrez :

```
create -t ssl -p 4343 -h voyage_svr /voyage
```

Utilisation de la solution SSO de Policy Director

Lorsque vous localisez une ressource protégée sur un serveur d'arrière-plan, le client demandant l'usage de cette ressource peut être amené à établir plusieurs connexions ; une pour le serveur WebSEAL et une autre pour chacun des serveurs d'arrière-plan impliqués dans l'opération. Chacune de ces connexions peut demander un ID de connexion différent.



Le problème que pose la gestion de plusieurs ID de connexion peut être résolu par un mécanisme de connexion unique, ou solution SSO (single sign-on). Une solution SSO permet à l'utilisateur d'accéder à une ressource, quelque soit l'emplacement de celle-ci, à partir de sa seule connexion initiale. Toutes les autres connexions nécessaires à l'opération sont traitées de manière transparente du point de vue de l'utilisateur.

L'administrateur de la sécurité du réseau doit prendre trois décisions importantes lors de la configuration d'une méthode SSO dans Policy Director :

1. Les serveurs d'arrière-plan demandent-ils des données d'authentification ?

   WebSEAL utilise l'en-tête d'authentification de base HTTP pour communiquer les données d'authentification.
2. Si ces données d'authentification sont demandées par les serveurs d'arrière-plan, d'où ces données doivent-elles provenir ? (Quelles informations placer dans l'en-tête HTTP ?).
3. La connexion entre WebSEAL et les serveurs d'arrière-plan doit-elle être sécurisée ? (Jonction TCP ou SSL ?)

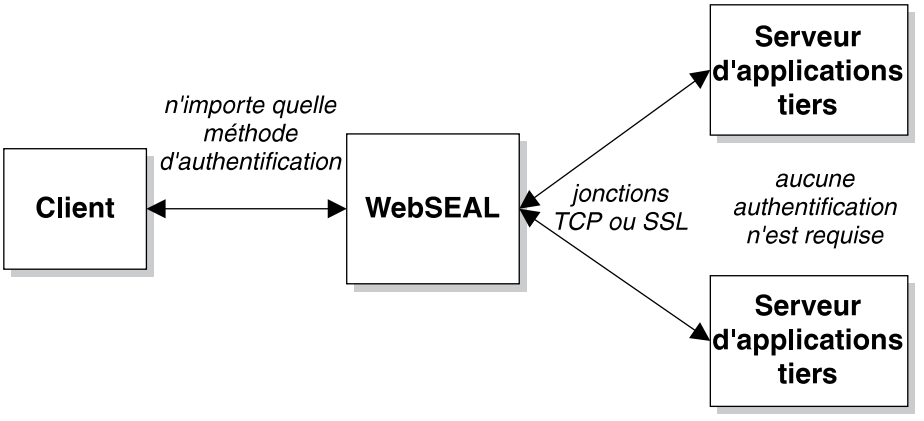
Les sections qui suivent détaillent quelques configurations de connexion unique standard.

Serveurs d'arrière-plan ne demandant pas d'authentification

Si les serveurs d'arrière-plan ne demandent pas de données d'authentification :

- Il est inutile de configurer WebSEAL de manière à transmettre des données d'authentification par le biais de la jonction.
- Vous ne pouvez accéder aux serveurs d'arrière-plan que par l'intermédiaire de WebSEAL.
- WebSEAL gère l'authentification pour le compte de tous les serveurs d'arrière-plan.
- Une option spéciale vous permet de communiquer des données d'identité aux serveurs d'arrière-plan si une autorisation est requise pour une action spécifique. Il s'agit de l'option **-c** de l'utilitaire **junctioncp**.

Reportez-vous à la section «Connexion sans données d'authentification» à la page 209 .

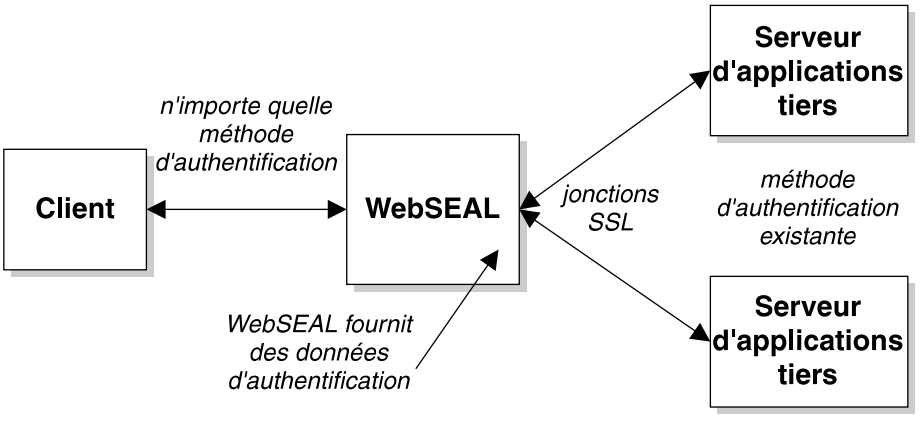


Serveurs d'arrière-plan demandant des données d'authentification

Si les serveurs d'arrière-plan utilisent des procédures d'authentification obligatoires :

- Vous devez configurer WebSEAL de manière à communiquer aux serveurs d'arrière-plan les données d'authentification requises.
- Dans la plupart des cas, ces données d'authentification doivent provenir d'un système de type GSO (solution de connexion globale).

  Reportez-vous à la section «Intégration du serveur GSO et de la solution SSO de WebSEAL» à la page 210.
- Dans la mesure où Policy Director doit communiquer des informations sensibles (nom d'utilisateur et mot de passe) via la jonction, la sécurité de celle-ci ne doit pas être négligée. L'utilisation de jonctions SSL est donc fortement recommandée.



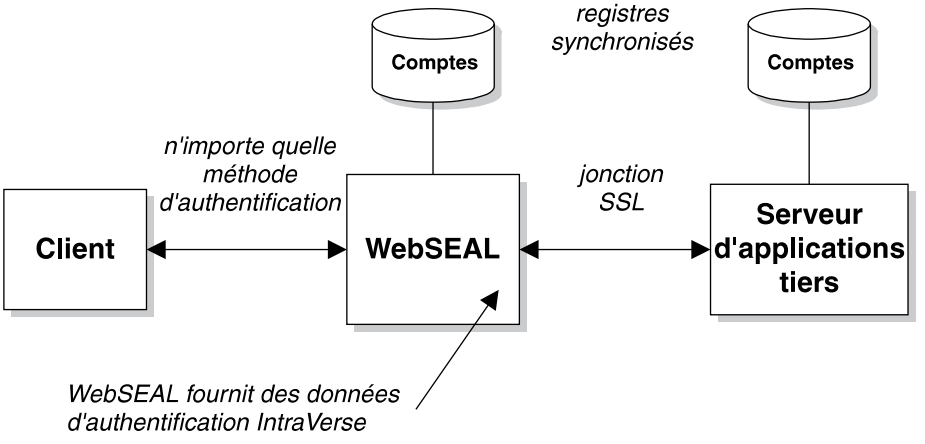
Solution de connexion unique de Policy Director

Lorsque les serveurs d'arrière-plan demandent à Policy Director de fournir des données d'authentification :

- Vous devez configurer WebSEAL de manière à fournir aux serveurs d'arrière-plan le nom d'utilisateur et le mot de passe contenus dans la requête du client initial.

- Les serveurs d'arrière-plan doivent accepter et comprendre l'identité et le mot de passe que Policy Director fournit dans l'en-tête d'authentification de base (AB) HTTP. Il en découle que le registre des utilisateurs de WebSEAL et ceux des serveurs d'arrière-plan doivent être synchronisés.
- Dans la mesure où Policy Director doit communiquer des informations sensibles (nom d'utilisateur et mot de passe) via la jonction, la sécurité de celle-ci ne doit pas être négligée. L'utilisation de jonctions SSL est donc fortement recommandée.

Reportez-vous à la section «Données de l'en-tête AB du client initial» à la page 208.

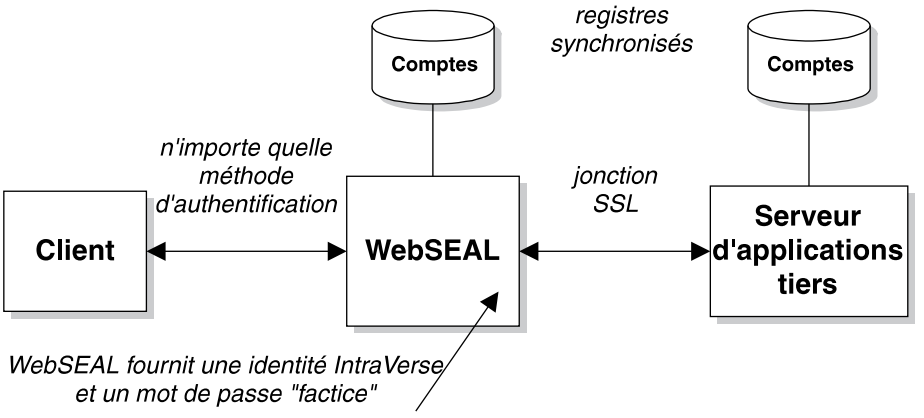


Solution de connexion unique limitée de Policy Director

Policy Director dispose d'une solution SSO limitée avec laquelle l'en-tête AB HTTP contient l'identité Policy Director (le nom d'utilisateur). Un mot de passe générique statique est également communiqué. Cette approche convient bien en cas d'utilisation individuelle des applications dans la mesure où elle ne nécessite pas de gestion continue du mot de passe. Dans cette situation :

- Vous devez configurer WebSEAL de manière à fournir aux serveurs d'arrière-plan le nom d'utilisateur contenu dans la requête du client initial ainsi qu'un mot de passe générique (factice).
- Entrez le mot de passe factice dans le fichier de configuration iv.conf.
- Les serveurs d'arrière-plan doivent comprendre l'identité que Policy Director fournit dans l'en-tête AB HTTP. Il en découle que le registre des comptes de WebSEAL et ceux des serveurs d'arrière-plan doivent être synchronisés.
- Dans la mesure où Policy Director doit communiquer des informations sensibles (nom d'utilisateur et mot de passe) via la jonction, la sécurité de celle-ci ne doit pas être négligée. L'utilisation de jonctions SSL est donc fortement recommandée.

Reportez-vous à la section «Identité Policy Director et mot de passe générique» à la page 207.



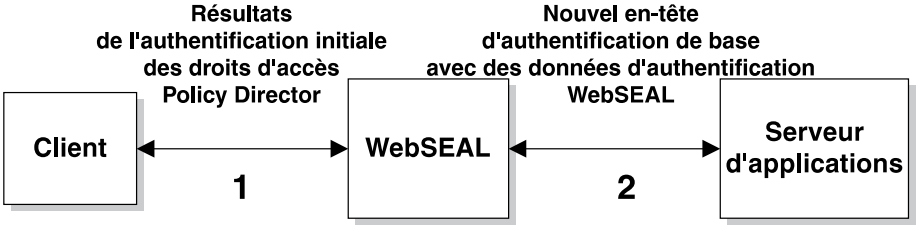
Communication de données d'authentification aux serveurs reliés par jonction

WebSEAL peut communiquer des données d'authentification à un ou plusieurs serveurs d'arrière-plan de plusieurs manières. En tant qu'administrateur, vous devez décider si les données d'authentification placées dans l'en-tête d'authentification de base (AB) de la requête HTTP seront communiquées au serveur d'arrière-plan.

D'où proviennent ces données d'authentification ?

A l'issue de la procédure d'authentification initiale entre le client et WebSEAL, WebSEAL génère un nouvel en-tête AB. La requête utilise ensuite cet en-tête pendant son cheminement à travers la jonction jusqu'au serveur d'arrière-plan. A l'aide des options de l'utilitaire **junctioncp**, vous devez indiquer quelles données d'authentification figurent dans l'en-tête.

Vous devez analyser l'architecture de votre réseau et ses besoins en matière de sécurité, puis choisir quelles données de l'en-tête pourront (le cas échéant) transiter par la jonction.



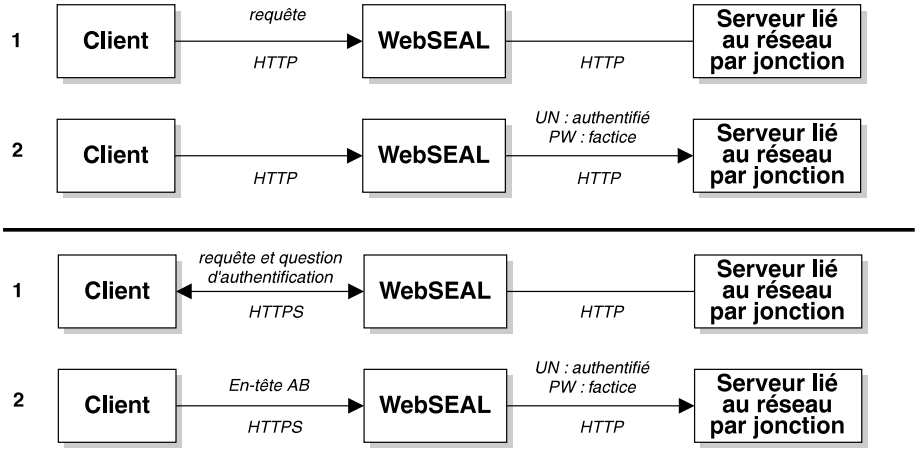
Identité Policy Director et mot de passe générique

Option de junctioncp : -b supply

Cette option demande à WebSEAL de transmettre le nom d'utilisateur authentifié par Policy Director (l'identité d'origine du client) avec un mot de passe générique (factice). Cette approche n'utilise pas le mot de passe initial du client.

Cette méthode part du principe que le serveur d'arrière-plan peut authentifier une requête à partir de l'identité définie par Policy Director. En associant un utilisateur client à une identité reconnue qu'il définit lui-même, Policy Director gère le

processus d'authentification pour le compte du serveur d'arrière-plan. Ce faisant, Policy Director met en oeuvre une solution de connexion unique simple et applicable à l'échelle du domaine.



Limites du système :

Policy Director emploie le même mot de passe factice pour toutes les requêtes, ce qui signifie que tous les utilisateurs ont le même mot de passe dans le registre du serveur d'arrière-plan. Si les clients utilisent toujours WebSEAL pour accéder au serveur relié par jonction, cette configuration ne présente pas de danger pour la sécurité.

L'emploi d'un mot de passe générique évite la gestion de nombreux mots de passe et permet l'utilisation individuelle des applications. Le mot de passe factice est défini par le paramètre **basic_auth_passwd** du fichier de configuration iv.conf.

```
basic_auth_passwd = mot de passe
```

Dans la mesure où cette méthode ne prévoit pas de mesure de sécurité au niveau du mot de passe, le serveur d'arrière-plan doit implicitement se fier à WebSEAL pour vérifier la légitimité du client.

Le serveur doit également comprendre l'identité définie par Policy Director pour l'accepter. Ceci implique la synchronisation du registre du serveur d'arrière-plan avec celui de WebSEAL.

L'utilisation d'un mot de passe factice commun à tous les utilisateurs ne permet pas au serveur d'arrière-plan de prouver lui-même l'authenticité des clients qui l'utilise pour se connecter. Pour cette raison, il est impératif de sécuriser physiquement le serveur d'arrière-plan contre toute autre possibilité d'accès.

Données de l'en-tête AB du client initial

Option junctioncp : -b ignore

Cette option demande à WebSEAL d'ignorer l'en-tête contenant les données d'authentification de base (AB) que le client fournit. En d'autres termes, WebSEAL devra transmettre cet en-tête sans le modifier au serveur tiers. Aucune connexion n'intervient au niveau du serveur WebSEAL.

Cette approche convient bien dans le cas d'un serveur d'arrière-plan qui :

- prend en charge l'authentification de base ;
- n'est pas configuré pour utiliser les services de sécurité de Policy Director ;
- doit gérer des mots de passe fournis par le client.

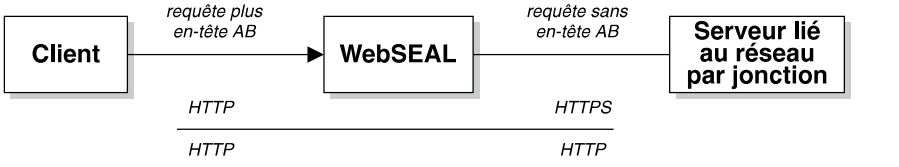
WebSEAL transmet directement la requête du client au serveur d'arrière-plan, sans intervenir davantage.

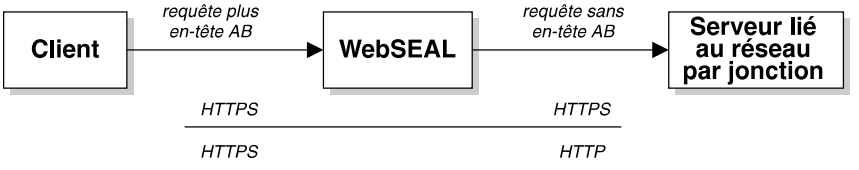
Le serveur d'arrière-plan renvoie une question d'authentification au client. Celui-ci y répond en soumettant son nom d'utilisateur et son mot de passe que le serveur WebSEAL transmet sans les modifier.

Cette méthode ne constitue pas réellement une solution de connexion unique mais permet une connexion semi-directe avec le serveur tiers, transparente du point de vue de WebSEAL.

ATTENTION:
Cette option ne fonctionne pas si WebSEAL a authentifié le client avec l'authentification de base SSL. Dans cette situation, l'en-tête AB est vidé de son contenu (comme avec l'option -b filter) avant de transiter par une jonction potentiellement non sécurisée.

Si le serveur d'arrière-plan utilise l'authentification de base, il renvoie alors une question d'authentification au client. Dans la mesure où les nouvelles données d'authentification de base que le client soumet sont à nouveau supprimées, la requête ne peut jamais aboutir.



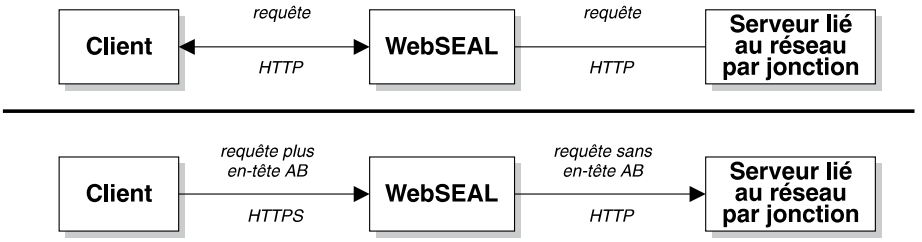


Connexion sans données d'authentification

Option junctioncp : -b filter

Cette option demande à WebSEAL de supprimer les données d'authentification de base des en-têtes des requêtes des clients avant de transmettre ces requêtes aux serveurs d'arrière-plan. WebSEAL devient alors seul responsable de la sécurité du réseau. Cette méthode convient si vous savez que le serveur d'arrière-plan n'utilise pas l'authentification de base.

Vous pouvez combiner cette option avec l'option **-c** pour insérer une identité définie par Policy Director à la place des données initiales de l'en-tête HTTP.
Reportez-vous à la section «Insertion des données d'identité du client (option -c)» à la page 201.



Noms d'utilisateur et mots de passe GSO

Option junctioncp : -b gso

Cette option demande à WebSEAL de communiquer au serveur d'arrière-plan des données d'authentification (nom d'utilisateur et mot de passe) issues du système de connexion globale GSO (global sign-on). Lorsque la sécurité doit être gérée au niveau de WebSEAL comme au niveau des serveurs d'arrière-plan, cette méthode est particulièrement intéressante. Les applications des serveurs d'arrière-plan demandent des noms d'utilisateur et des mots de passe que ne contient pas le registre de WebSEAL.

Reportez-vous à la section «Intégration du serveur GSO et de la solution SSO de WebSEAL» pour une description complète de cette méthode.

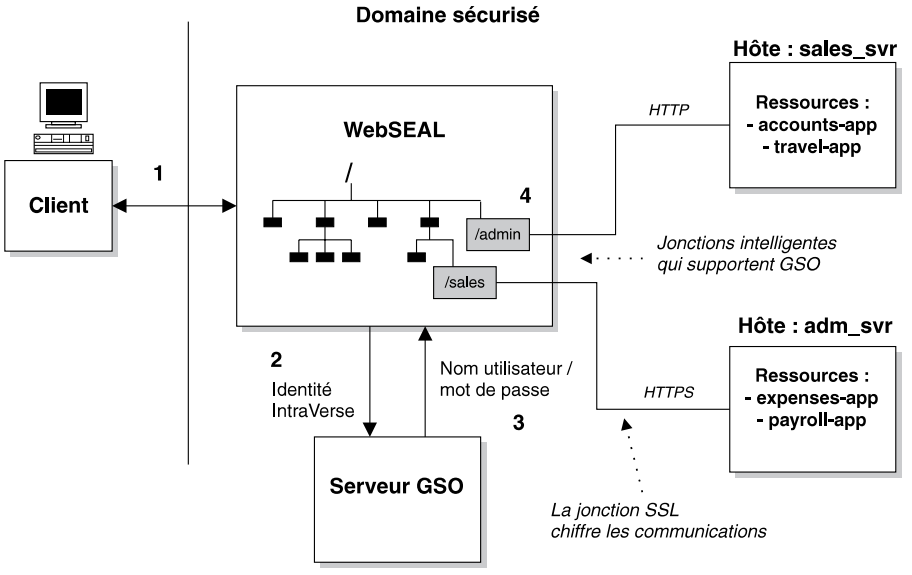
Intégration du serveur GSO et de la solution SSO de WebSEAL

Policy Director supporte une solution de connexion unique, ou SSO (Single Sign-On), plus souple en intégrant la technologie IBM de connexion globale, ou GSO (Global Sign-On). La solution IBM Global Sign-On fait partie de la famille de produits IBM SecureWay. La combinaison de WebSEAL et de GSO produit une solution Web SSO complète qui offre en plus les avantages du chiffrement des données, de l'accessibilité avancée et de la modularité.

L'illustration qui suit décrit comment l'intégration de WebSEAL et GSO permet de récupérer des noms d'utilisateur et des mots de passe pour accéder à des applications de serveur d'arrière-plan.

1. Le client se fait authentifier par WebSEAL dans le cadre d'une requête d'accès à une application d'un serveur d'arrière-plan. Policy Director lui assigne une identité.

   Remarque : Le processus de connexion unique est indépendant de la méthode d'authentification initiale.
2. WebSEAL communique au serveur GSO l'identité définie par Policy Director.
3. GSO renvoie ensuite un nom d'utilisateur et un mot de passe appropriés pour l'utilisateur et la ressource demandée.
4. WebSEAL insère ces données d'identité dans l'en-tête d'authentification de base HTTP de la requête, puis renvoie celle-ci au serveur d'arrière-plan via la jonction.



Obtention de données d'authentification par GSO

L'exemple suivant illustre comment le serveur GSO fournit des données d'authentification au serveur WebSEAL. Lorsque l'utilisateur Michel demande à accéder à la ressource voyage-app, WebSEAL demande ses données d'authentification au serveur GSO.

Le serveur GSO gère une base de données complète contenant des mises en correspondance entre des ressources et des données d'authentification. Le mappage des ressources d'application à des combinaisons nom d'utilisateur/mot de passe produit ce que l'on appelle les droits d'accès des ressources GSO. Ces droits d'accès ne peuvent être créés que pour les utilisateurs enregistrés.

La base de données du serveur GSO contient un droit d'accès de ressources spécifique à l'utilisateur Michel qui associe la ressource "voyage-app" à un couple nom d'utilisateur/mot de passe déterminé.

Le tableau suivant illustre la structure de la base de données des ressources GSO.

Michel	**Paul**

`resource: voyage-app`
`username=michel`
`password=123`
 	
`resource: paie-app`
`username=poirier`
`password=456`
	`resource: voyage-app`
	`username=paul`
	`password=abc`
	
	`resource: paie-app`
	`username=gentil`
	`password=xyz`

Dans cet exemple, le serveur GSO retourne le nom d'utilisateur `michel` et le mot de passe `123`. WebSEAL utilise ces informations pour créer l'en-tête AB HTTP dans la requête transmise via la jonction.

Configuration d'une jonction intelligente compatible GSO

Le support du système GSO par WebSEAL se configure au niveau de la jonction intelligente établie entre WebSEAL et le serveur d'applications d'arrière-plan.

Pour créer une jonction pouvant utiliser le système GSO, utilisez la commande **junctioncp create** avec l'option **-b gso**. L'exemple suivant illustre la syntaxe de la commande create :

```
create -t tcp -h nom_hôte -b gso -T
ressource point_jonction
```

Le tableau suivant répertorie les options de configuration des jonctions intelligentes compatibles GSO :

Options	Description
-b gso	Le serveur GSO devra fournir les données d'authentification de toutes les requêtes transitant par la jonction.
-T ressource	Spécifie le nom de l'application. Le nom de ressource utilisé comme argument de cette option doit correspondre exactement à celui figurant dans la base de données du serveur GSO. Cet argument est obligatoire pour les jonctions GSO.

Comme le décrit la section «Création de jonctions intelligentes SSL sécurisées» à la page 202, vous pouvez sécuriser une jonction utilisée dans une solution WebSEAL/GSO par le biais du protocole SSL. Pour cela, entrez l'option **-t ssl** lors de la création de cette jonction.

Utilisez toujours des jonctions SSL avec GSO pour bénéficier du chiffrement des droits d'accès des ressources GSO et des autres données.

Exemples de jonctions intelligentes compatibles GSO :

Pour établir une jonction avec l'application "voyage-app", sur l'hôte "ventes_svr", sur le point de jonction "/ventes":

```
create -t tcp -b gso -T voyage-app -h ventes_svr /ventes
```

Pour établir une jonction sécurisée par SSL avec l'application "paie-app", sur l'hôte "adm_svr", sur le point de jonction "/admin" :

```
create -t ssl -b gso -T paie-app -h adm_svr /admin
```

Remarque : Dans le dernier exemple, l'option **-t ssl** spécifie le port par défaut 443.

Utilisation des jonctions intelligentes

Chaque serveur d'arrière-plan doit être relié au réseau sur un point de jonction (point de montage) distinct. A mesure que la demande de contenu et de ressources augmente, vous pouvez ajouter d'autres serveurs à l'aide de jonctions intelligentes.

Les procédures ci-dessous se rapportent aux jonctions intelligentes :

- «Montage de plusieurs serveurs sur une même jonction».
- «Filtrage des URL par les serveurs reliés par jonction» à la page 213.
- «Contrôle des processus CGI (droit d'exécution)» à la page 214

Montage de plusieurs serveurs sur une même jonction

Vous pouvez monter plusieurs instances d'un serveur dupliqué sur un même point de jonction. Le nombre de serveurs pouvant être ainsi montés n'est pas limité.

Tous les serveurs montés sur un point de jonction doivent être des répliques (copie miroir des espaces Web) et utiliser le même protocole : HTTP ou HTTPS. Ne tentez pas de monter des serveurs différents sur le même point de jonction.

A partir de l'espace Web du serveur Policy Director primaire, accédez aux pages appartenant aux serveurs reliés par jonction. Vous devez pouvoir accéder à ces pages (sous réserves d'avoir les autorisations requises) et celles-ci doivent s'afficher normalement. S'il arrive qu'une page soit introuvable ou ait été modifiée, ceci signifie que Policy Director ne l'a pas dupliquée comme il convient.

Vérifiez alors que le document existe bien et qu'il est identique dans les deux arborescences des serveurs dupliqués.

Filtrage des URL par les serveurs reliés par jonction

Le filtrage ne s'applique qu'aux documents provenant des serveurs reliés par jonction ayant le type MIME "text" ou "html".

WebSEAL peut modifier deux types d'URL : les URL absolues et les URL de système hôte.

URL de système hôte

Une adresse URL de système hôte indique une position URI par rapport à la racine des documents du serveur relié par jonction. Par exemple :

```
/dir/fichier.html
```

WebSEAL peut changer cette URL pour désigner le point de jonction du serveur relié par jonction. Par exemple :

```
/jct/dir/fichier.html
```

URL absolues

Une adresse URL absolue indique la position URI (Universal Resource Indicator) par rapport à la fois à un nom d'hôte, ou une adresse IP, et à un port de réseau. Par exemple :

```
http://nomserveur[:port]/fichier.html
```

Ou :

```
https://nomserveur[:port]/fichier.html
```

Vous pouvez modifier ces URL en respectant les règles suivantes :

1. Lorsque l'URL est de type HTTP et que le système hôte ou le port correspond à un serveur TCP relié par jonction, l'URL change pour désigner le point de jonction. Par exemple :

   ```
   /jct/...
   ```

2. Lorsque l'URL est de type HTTPS et que le système hôte ou le port correspond à un serveur SSL relié par jonction, l'URL change pour désigner le point de jonction. Par exemple :

   ```
   jct...
   ```

3. Seules les adresses URL définies dans le fichier de configuration iv.conf pour les codes TAG et les paires d'attributs sont filtrées.
4. Filtrez toujours les codes de type META pour les requêtes de régénération. Par exemple :

   ```
   META HTTP-EQUIV="Refresh" CONTENT="5;URL=http://server/url"
   ```

5. Si un code BASE contient l'attribut HREF, ce code sera supprimé de la réponse adressée au client.

La strophe [url-filter] du fichier de configuration iv.conf contient des paramètres qui déterminent comment filtrer les URL transitant par les serveurs reliés par jonction.

La strophe [url-filter]contient une liste de codes HTML. Le serveur WebSEAL filtre ou modifie ces codes en fonction des URL absolues obtenues par un serveur relié par jonction.

Par défaut, Policy Director configure tous les codes HTML couramment utilisés. Concernant les codes HTML contenant des URL, l'administrateur peut être amené à les ajouter explicitement.

Contrôle des processus CGI (droit d'exécution)

Le droit d'exécution (x) défini par Policy Director ne s'applique pas aux jonctions. Il ne permet notamment pas de contrôler l'exécution d'un script CGI sur un serveur d'arrière-plan. WebSEAL n'a aucun moyen de déterminer précisément si un objet demandé sur un serveur d'arrière-plan est un fichier de programme CGI ou un objet HTTP conventionnel. L'accès aux objets via les jonctions est toujours contrôlé par le droit de lecture (r), même pour les programmes CGI.

Utilisation de query_contents avec des serveurs tiers

Vous pouvez protéger les ressources de l'espace Web d'une application tiers au moyen du service de sécurité de Policy Director. Pour cela, vous devez fournir à WebSEAL des informations sur le contenu de cet espace Web.

Ces informations peuvent être obtenues à l'aide d'un programme CGI appelé **query_contents**. Le programme **query_contents** analyse le contenu de l'espace Web tiers et en communique l'inventaire à la console de gestion. Le programme query_contents s'installe en même temps que WebSEAL mais doit être installé manuellement sur le serveur tiers. Il existe en différentes versions pour les serveurs tiers UNIX ou Windows.

Le gestionnaire d'espace objets de la console de gestion exécute automatiquement **query_contents** chaque fois que vous développez la partie de l'espace des objets protégé correspondant à la jonction, dans le panneau de gestion Espace objets. Lorsque la console a pris connaissance du contenu de l'espace des objets de l'application tiers, vous pouvez afficher ces informations et attacher des modèles de règle aux objets appropriés.

Installation de query_contents

Pour installer **query_contents**, vous devez copier un ou deux fichiers du serveur Policy Director sur le serveur tiers, puis modifier un fichier de configuration.

Le répertoire de Policy Director suivant contient un modèle du programme :

UNIX : *répertoire racine*/www/lib/query_contents

Windows : *répertoire racine*\www\lib\query_contents

Ce répertoire contient les fichiers suivants :

Fichier	Description

query_contents.exe	Programme exécutable principal pour les systèmes Win32. Il s'installe dans le répertoire cgi-bin du serveur Web tiers.
query_contents.sh	Programme exécutable principal pour les systèmes UNIX. Il s'installe dans le répertoire cgi-bin du serveur Web tiers.
query_contents.c	Code source du programme. Ce code source est fourni pour le cas où vous auriez besoin de modifier le mode opératoire de **query_contents**. Dans la plupart des cas, cela n'est pas nécessaire.
query_contents.html	Fichier d'aide au format HTML.
query_contents.cfg	Fichier de configuration type qui identifie la racine des documents pour le serveur Web.

Installation de query_contents sur un serveur tiers UNIX

Recherchez le script shell query_contents.sh dans le répertoire suivant :

UNIX : *répertoire_installation*/www/lib/query_contents

Pour installer le programme **query_contents** sur un serveur tiers UNIX :

1. Copiez le fichier query_contents.sh dans un répertoire /cgi-bin sur le serveur Web tiers.
2. Supprimez l'extension .sh.
3. Activez le droit d'exécution UNIX ("execute") pour l'utilisateur propriétaire du serveur Web.

Installation de query_contents sur un serveur tiers Win32

Recherchez le programme exécutable query_contents.exe et le fichier de configuration query_contents.cfg dans le répertoire suivant :

Windows : *répertoire_installation*\www\lib\query_contents

Pour installer le programme **query_contents** sur un serveur tiers Win32 :

1. Vérifiez que le serveur Web tiers contient un répertoire CGI, convenablement configuré.
2. Vérifiez que la racine des documents du serveur Web tiers contient bien un document valide.
3. Copiez le fichier query_contents.exe dans le répertoire CGI du serveur Web tiers.
4. Copiez query_contents.cfg dans le répertoire Windows.

   Le tableau suivant indique les valeurs par défaut de ce répertoire :

Système d'exploitation	Répertoire Windows
Windows 95	c:\windows
Windows NT 3.5x	c:\winnt35
Windows NT 4.x	c:\winnt

5. Ouvrez le fichier query_contents.cfg pour y spécifier le répertoire racine des documents du serveur Web tiers.

   Le fichier contient des exemples d'entrée pour les serveurs de type Microsoft Internet Information Server et Netscape FastTrack. Les lignes du fichier débutant par un point virgule (;) contiennent des commentaires et sont ignorées par le programme **query_contents**.

Test de la configuration

Pour tester la configuration :

1. Sur le serveur Win32, passez dans le répertoire contenant le programme **query_contents**.
2. Ouvrez une ligne de commande DOS et lancez le programme. Tapez la commande ci-dessous:

   ```
   query_contents dirlist=/
   ```

   La sortie doit ressembler à ce qui suit :

   ```
   100
   index.html
   cgi-bin//
   pics//
   ```

   Le nombre 100 est un code d'état indiquant la réussite de l'opération. Il est très important de voir au moins le nombre 100 comme première (et éventuellement seule) valeur affichée.

   Si, au lieu de ce type de sortie, vous obtenez un code d'erreur, le fichier de configuration n'est pas où il devrait être ou contient une entrée de racine des documents incorrecte. Vérifiez le contenu du fichier query_contents.cfg et assurez-vous que la racine des documents existe bien.
3. Entrez l'adresse URL suivante dans votre navigateur :

   ```
   http:
   //nom de la machine Win32/cgi-bin/query_contents.exe?dirlist=/
   ```

   Le résultat devrait être identique à celui de l'étape précédente. Dans le cas contraire, concluez que la configuration CGI de votre serveur Web est incorrecte. Reportez-vous à la documentation de votre serveur pour résoudre le problème.

Configuration d'une jonction intelligente pour utiliser query_contents

Vous pouvez définir l'adresse URL du script **query_contents**. Policy Director recherche le programme **query_contents** dans /cgi_bin/. Si ce répertoire est différent ou que le fichier de **query_contents** a été renommé, utilisez l'option **-q** pour indiquer à WebSEAL sa nouvelle URL.

Si vous créez la jonction intelligente pour un serveur tiers Win32, utilisez la commande **junctioncp** avec l'option **-q** :

```
junctioncp> create -t tcp -h nom_hôte -q
/cgi-bin/query_contents.exe /point_montage
```

Pour une synthèse des options de la commande **junctioncp**, reportez-vous à la section «Création d'une jonction pour un premier serveur» à la page 196.

Exécution du programme query_contents

La tâche du script **query_contents** consiste à identifier et rapporter le contenu des répertoires spécifiés dans une requête d'URL. Par exemple, pour connaître le contenu du répertoire racine de l'espace Web d'un serveur, le navigateur exécute **query_contents** sur une URL par la commande suivante :

```
http://serveur tiers/cgi-bin/query_contents?dirlist=/
```

Le script **query_contents** exécute les opérations suivantes :

1. Le programme lit la valeur de $SERVER_SOFTWARE, une variable d'environnement CGI standard, pour déterminer le type du serveur.

   Policy Director affecte à la variable $DOCROOTDIR une valeur désignant une racine de documents standard, selon le type du serveur Web.
2. Le script lit ensuite la valeur de la variable $QUERY_STRING dans l'URL soumise, pour connaître l'opération demandée et le chemin de l'objet.

   L'opération est indiquée par la variable $OPERATION et le chemin par la variable $OBJPATH. Dans l'exemple précédent, la valeur de $OPERATION est "dirlist" et celle de $OBJPATH est " / ".
3. Le programme query_contents dresse la liste des répertoires (ls) du chemin de l'objet et l'envoie en sortie standard à l'intention du serveur Policy Director. Les entrées correspondant à des sous-répertoires se terminent par une double barre oblique (//).

   La sortie ressemble généralement à ceci :

   ```
   100
   index.html
   cgi-bin//
   pics//
   ```

   Le nombre 100 est un code d'état indiquant la réussite de l'opération.

Personnalisation de query_contents

Pour adapter le script du programme **query_contents** à votre serveur, vous devrez peut-être modifier le paramètre définissant la racine des documents.

Si **query_contents** renvoie un code d'erreur (une valeur autre que 100) et ne donne aucune liste de fichiers, examinez le script. Le cas échéant, modifiez la valeur de la variable $DOCROOTDIR pour refléter la configuration de votre serveur.

Si vous spécifiez comme il convient la racine des documents et que le script échoue encore, l'emplacement du répertoire cgi-bin est peut-être mal défini. Examinez cette fois-ci la variable $FULLOBJPATH et modifiez sa valeur pour indiquer l'emplacement réel du répertoire cgi-bin.

Ajout de fonctions

Le code source du programme **query_contents** (query_contents.c) est fourni avec Policy Director.

Vous pouvez, le cas échéant, ajouter des fonctions supplémentaires à ce programme pour gérer les propriétés de certains serveurs Web tiers. Ces fonctions permettent notamment :

1. le mappage des répertoires, lorsqu'un sous-répertoire non placé sous la racine des documents est relié à l'espace Web ;
2. la création d'un espace Web ne reposant pas sur un système de fichiers.

   Ceci peut notamment concerner les serveurs Web hébergés dans une base de données.

Chapitre 16. WebSEAL - Intégration des applications

WebSEAL gère l'intégration des applications tiers par le biais de variables d'environnement et d'URL dynamiques. WebSEAL étend le nombre de variables d'environnement et d'en-têtes HTTP utilisables pour permettre aux applications tiers d'exécuter des opérations en fonction de l'identité d'un client. De plus, WebSEAL peut effectuer un contrôle d'accès sur les URL dynamiques, notamment celles contenant un texte de requête.

Ce chapitre comprend les sections suivantes :

Prise en charge de la programmation CGI

Pour gérer la programmation CGI, WebSEAL ajoute trois variables d'environnement au jeu de variables CGI standard. Les applications CGI peuvent ensuite utiliser ces variables d'environnement définies sur le serveur WebSEAL local ou sur un serveur d'arrière-plan relié au réseau par une jonction. Ces variables donnent aux applications CGI des informations relatives aux droit d'accès, aux utilisateurs et aux groupes définis par Policy Director.

Sur un serveur WebSEAL local, ces variables d'environnement sont directement générées d'après les données de droit d'accès Policy Director du client à l'origine de la requête.

Sur un serveur tiers relié au réseau par une jonction, les variables d'environnement utilisées par une application CGI sont générées d'après les données de l'en-tête HTTP de la requête. WebSEAL communique les données de l'en-tête HTTP au serveur tiers. Vous devez utiliser la commande **junctioncp** avec l'option **-c** pour créer une jonction. Cette jonction insère ensuite les données d'en-tête définies par Policy Director dans les requêtes HTTP destinées au serveur d'arrière-plan.

Reportez-vous à la section «Insertion des données d'identité du client (option -c)» à la page 201.

Autres variables d'environnement définies par Policy Director

Les autres formats des variables d'environnement CGI de Policy Director sont les suivants :

Variable d'environnement CGI	Description
HTTP_IV_USER	Compte utilisateur défini par Policy Director pour le client à l'origine de la requête.
HTTP_IV_GROUPS	Groupes Policy Director auxquels l'utilisateur appartient. Cette entrée se compose d'une liste de noms de groupe encadrés de doubles guillemets et séparés par des virgules.

HTTP_IV_CREDS	Structure de données codée représentant un droit d'accès Policy Director. Cette entrée communique des droits d'accès aux serveurs distants pour que les applications tiers puissent appeler le service d'autorisation par le biais de l'API d'autorisation. Reportez-vous au manuel Policy Director - Guide de programmation et de référence.

Variable REMOTE_USER (serveur WebSEAL local)

Dans un environnement de serveur local contrôlé par WebSEAL, la valeur de la variable HTTP_IV_USER est la même que celle de la variable standard REMOTE_USER. Notez que cette dernière variable peut également être présente dans l'environnement d'une application CGI installée sur un serveur d'arrière-plan relié au réseau par une jonction. Dans cette situation, WebSEAL ne contrôle pas sa valeur.

Variable d'environnement CGI	**Description**
REMOTE_USER	Contient la même valeur que la variable HTTP_IV_USER.

Prise en charge des applications des serveurs d'arrière-plan

WebSEAL permet également de gérer un code exécutable se présentant sous la forme d'un composant intégré d'un serveur Web d'arrière-plan. Les codes exécutables concernés sont notamment :

- les servlets Java ;
- les cartouches de Oracle Web Listener ;
- les plug-ins du côté serveur.

Pour établir une jonction avec un serveur d'arrière-plan, utilisez l'option **-c** avec la commande **junctioncp**. Une fois la jonction créée, WebSEAL insère les données d'identité et d'appartenance de groupe définies par Policy Director pour le client dans les en-têtes des requêtes HTTP destinées au serveur d'arrière-plan.

Reportez-vous à la section «Insertion des données d'identité du client (option -c)» à la page 201.

Les en-têtes HTTP définis par Policy Director permettent aux applications installées sur les serveurs tiers reliés par jonction d'exécuter des actions basées sur l'identité Policy Director du client.

WebSEAL transmet les données d'en-tête HTTP suivantes :

En-tête HTTP défini par Policy Director	**Description**
iv-user	Nom du client. Devient par défaut "unauthenticated" si le client n'est pas authentifié (est inconnu).
iv-groups	Liste des groupes auxquels le client appartient. Cette entrée se compose d'une liste de noms de groupe encadrés de doubles guillemets et séparés par des virgules.
iv-creds	Structure de données codée représentant un droit d'accès Policy Director. Cette entrée communique des droits d'accès aux serveurs distants pour que les applications tiers puissent appeler le service d'autorisation par le biais de l'API d'autorisation. Reportez-vous au manuel Policy Director - Guide de programmation et de référence.

Ces en-têtes HTTP sont communiqués aux applications CGI sous la forme des variables d'environnement HTTP_IV_USER, HTTP_IV_GROUP et HTTP_IV_CREDS. Pour savoir comment extraire les en-têtes des requêtes HTTP avec d'autres applications (non CGI), reportez-vous à la documentation des produits concernés.

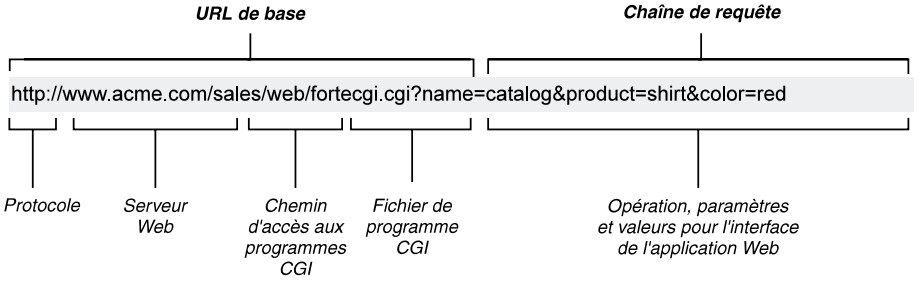
Contrôle d'accès des URL dynamiques

L'environnement Web courant donne aux utilisateurs un accès instantané à des informations en évolution permanente. De nombreuses applications Web génèrent dynamiquement des URL (Uniform Resource Locator) en réponse à chaque requête. Ces URL dynamiques n'existent parfois que sur une brève durée. En dépit de leur nature éphémère, les URL dynamiques nécessitent une sérieuse protection contre l'usage ou l'accès interdit.

Principes des URL dynamiques

Certaines applications Web sophistiquées utilisent des navigateurs Web standard pour communiquer avec des serveurs d'applications via l'interface CGI d'un serveur Web.

Tous ces outils utilisent des URL dynamiques et des éléments dont ils ignorent la nature pour communiquer l'opération demandée (avec ses paramètres) au serveur d'applications. Une URL dynamique ajoute à l'adresse URL conventionnelle des informations sur l'opération demandée et sur ses paramètres. La partie de l'URL qui contient cette chaîne de requête indique à l'interface de l'application Web des opérations, des paramètres et des valeurs.



Mappage des objets d'un espace des noms avec LCA à des URL dynamiques

Pour sécuriser les URL générées dynamiquement (par exemple par des requêtes de base de données), WebSEAL utilise le modèle de l'espace des noms d'objet protégé et les modèles de règle (les listes de contrôle d'accès). Chaque requête adressée à WebSEAL génère un objet dans l'espace des noms en guise de première étape du processus d'autorisation. Une LCA attachée à cet objet détermine les conditions de protection applicables à toute URL dynamique qui lui est associée.

Dans la mesure où les URL dynamiques n'ont qu'une durée d'existence limitée, il n'est pas possible de leur associer des entrées dans une base de données des règles d'autorisation préconfigurées. WebSEAL résout ce problème par une méthode qui mappe plusieurs URL dynamiques à un unique objet protégé statique.

Les correspondances issues des modèles objets/espace des noms sont contenues dans un fichier texte :

UNIX : `/opt/intraverse/www/lib/dynurl.conf`

Windows : `C:\Program Files\IBM\Policy Director\www\lib\dynurl.conf`

Il suffit d'ouvrir ce fichier pour modifier les correspondances. Notez que vous devez créer vous-même ce fichier, qui n'existe pas par défaut. Les entrées du fichier respectent le format :

objet modèle

WebSEAL utilise une forme limitée du modèle de shell UNIX (utilisant les caractères génériques) qui permet de définir le jeu de paramètres caractérisant un objet dans l'espace des noms. WebSEAL mappe toute URL dynamique correspondant à ces paramètres à cet objet. WebSEAL utilise les caractères de correspondance de chaîne suivants :

Caractère	Description
****	Le caractère qui suit la barre oblique inversée fait partie d'une séquence de commande. Par exemple, il peut s'agir du caractère de tabulation.
?	Caractère générique remplaçant n'importe quel caractère unique. Par exemple, la chaîne `abcde` correspond à l'expression `ab?de`.
*****	Caractère générique remplaçant n'importe quelle série de caractères.
[ ]	Définit une série de caractères à rechercher. Par exemple, la chaîne `abcde` correspond à l'expression régulière `ab[cty]de`.
^	Exclue des caractères d'une recherche. Par exemple, à l'expression ^[ab] correspond toute chaîne ne comprenant ni 'a' ni 'b'.

L'exemple suivant illustre le format d'une URL dynamique opérant une consultation de solde bancaire :

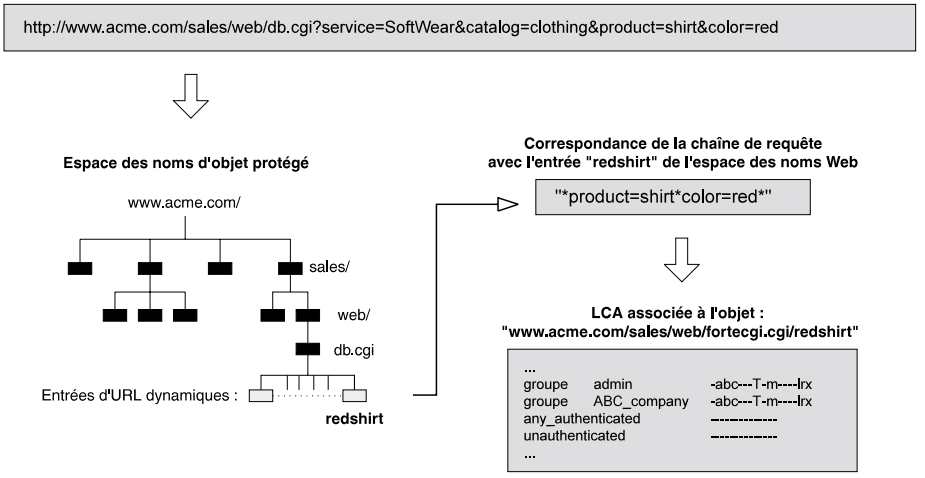
`http://`*`nom_serveur`*`/home-bank/owa/acct.bal?acc=`*`numéro_compte`*

L'objet de l'espace des noms représentant cette URL dynamique se présenterait de la manière suivante :

`http://<nom_serveur>/home-bank/owa/acct.bal?acc=*`

Un examen attentif de cette URL dynamique révèle qu'elle indique un numéro de compte déterminé. L'objet de l'espace des noms associé aux soldes bancaires, dans `home-bank`, est attaché à une liste de contrôle d'accès qui donne des autorisations pour tous les comptes. Ces droits s'appliquent à tous les comptes puisque la dernière partie de l'entrée (`acc=*`) utilise l'astérisque, qui remplace n'importe quelle suite de caractères.

Le schéma ci-dessous illustre une configuration dans laquelle une URL dynamique est mappée à un objet de l'espace des noms protégé (cet exemple n'utilise pas de caractères génériques).



Mise à jour de WebSEAL pour la gestion des URL dynamiques

L'utilitaire **dynurlcp** permet de mettre à jour l'espace des noms d'objet protégé de WebSEAL en ajoutant des entrées dans le fichier de configuration dynurl.conf. Vous devez vous connecter au domaine sécurisé au moyen de la commande dce_login.

Pour mettre à jour l'espace des noms d'objet protégé de WebSEAL avec l'utilitaire **dynurlcp** :

1. Créez, modifiez ou supprimez une entrée d'URL dynamique dans le fichier de configuration dynurl.conf.
2. Une fois les modifications faites, utilisez l'utilitaire **dynurlcp** pour mettre à jour le serveur :

   `dynurlcp -e /.:/subsys/intraverse/secmgr/server/ hôte update`

Conversion des URL dynamiques dans l'espace des noms

La conversion d'une URL dynamique en objet de l'espace des noms dépend de l'ordre des entrées dans le fichier de configuration dynurl.conf.

Le mappage d'une URL dynamique à une entrée de l'espace des noms commence par une analyse de la liste des correspondances contenue dans le fichier de configuration dynurl.conf. Le fichier est analysé du début vers la fin jusqu'à ce qu'une première occurrence soit détectée.

Une fois la première occurrence trouvée, WebSEAL utilise l'entrée d'espace des noms correspondante pour le contrôle d'autorisation suivant. A défaut d'occurrence, WebSEAL utilise l'URL elle-même et y retranche la partie `http://serveur` du chemin.

Placez les correspondances des listes de contrôle d'accès les plus restrictives au début de la liste. Par exemple, l'accès à une procédure de vente de livres (d'une application de gestion des ventes) est réservé à un groupe de responsables de bibliothèque. En revanche, le reste de l'application est accessible à tous les utilisateurs. Dans cette situation, les correspondances répertoriées dans la liste doivent apparaître de la manière suivante :

Entrée de l'espace des noms	Modèle d'URL
/ows/ventes/vtelivres	/ows/db-apps/owa/livre.ventes*

/ows/ventes/général	/ows/db-apps/owa/*

Notez que si les entrées de mappage apparaissaient dans l'ordre inverse, toutes les procédures stockées dans le répertoire /ows/db-apps/owa seraient associées à l'objet de l'espace des noms /ows/ventes/general. Cette conversion erronée pourrait entraîner un risque pour la sécurité.

Méthodes de transmission de données GET et POST

Lorsque vous mappez une expression régulière d'URL à une entrée de l'espace des noms, le format attendu pour cette adresse URL est celui que produit la méthode GET. En réalité, il importe peu que vous ayez utilisé la méthode GET ou POST.

Avec la méthode de transmission de données GET, WebSEAL ajoute les données dynamiques à l'adresse URL. Ces données dynamiques sont, par exemple, les renseignements que l'utilisateur saisit dans un formulaire.

Avec la méthode de transmission de données POST, WebSEAL intègre les données dynamiques dans le corps de la requête.

Evaluation des LCA

Une fois l'URL dynamique convertie en entrée d'espace des noms, le modèle standard d'héritage de LCA de Policy Director s'applique à elle. Ce modèle détermine si la requête doit être autorisée (traitée) ou rejetée (en cas de privilèges insuffisants).

Exemple de traitement des URL dynamiques

L'exemple suivant illustre comment un intranet d'entreprise parvient à sécuriser des adresses URL générées par un serveur d'écoute.

Dans cet exemple, le programme de serveur Web qui crée ces URL dynamiques est Oracle Web Listener. La même technique peut être appliquée à d'autres serveurs Web du même type.

Application

L'entreprise Travel Kingdom propose des services de réservation de voyage sur l'Internet. Elle désire exploiter deux applications de base de données Oracle sur son serveur Web sachant que celles-ci devront être accessibles à partir de côté sécurisé du pare-feu comme à partir de l'Internet.

- **Système de réservation de voyage**

  Les clients autorisés peuvent réserver à distance et consulter leurs réservations en cours. Le personnel de Travel Kingdom peut également enregistrer des réservations passées par téléphone, faire des modifications et bien d'autres transactions. Dans la mesure où les clients paient par carte bancaire, WebSEAL doit sécuriser la transmission de ces informations.

- **Responsable administratif**

  Comme la plupart des sociétés, Travel Kingdom possède une base de données administrative qui contient des informations en rapport avec les salaires, les fonctions et l'ancienneté des salariés. Les données de chaque salarié sont accompagnées d'une photographie.

Interface

Vous pouvez configurer un serveur Web Oracle pour gérer l'accès aux procédures suivantes stockées dans la base de données :

/db-apps/owa/tr.browse	Permet à tous les utilisateurs de consulter les destinations proposées, les prix, etc.
/db-apps/owa/tr.book	Permet de passer une réservation (par un salarié de l'agence ou un client authentifié).
/db-apps/owa/tr.change	Permet d'afficher ou de modifier les réservations en cours.
/db-apps/owa/admin.browse	Permet à tout salarié de l'agence d'accéder aux données de personnel non confidentielles (numéro de poste, adresse e-mail, photographie).
/db-apps/owa/admin.resume	Permet à un salarié défini d'afficher ou de modifier ses renseignements personnels dans la base de données administrative.
/db-apps/owa/admin.update	Permet aux agents administratifs de mettre à jour les données relatives au personnel.

Structure de l'espace Web

Un serveur WebSEAL constitue l'interface sécurisée de l'espace Web de la société Travel Kingdom.

Vous pouvez monter une jonction (/ows) avec le serveur Web Oracle en charge de l'application de réservation de voyage et de l'application d'administration.

Règles de sécurité

Pour apporter la sécurité qui convient aux ressources Web, sans nuire à la convivialité du système, l'entreprise s'est fixée les objectifs suivants :

- Les salariés de l'agence de voyage ont le contrôle complet des réservations.
- Les clients authentifiés peuvent passer et modifier leurs réservations mais ne peuvent pas accéder aux données de voyage des autres clients authentifiés.
- Les membres du personnel d'administration ont un accès complet à toutes les données administratives.
- Les autres employés (non administratifs) de Travel Kingdom peuvent modifier leurs renseignements personnels et afficher certaines des données des autres salariés.

Mappage des URL dynamiques à l'espace des noms

Pour satisfaire les objectifs de sécurité, les URL dynamiques doivent être rattachées (mappées) à des entrées de l'espace des noms, et donc à des listes de contrôle d'accès. N'oubliez pas que l'ordre des correspondances est un aspect important pour la sécurité.

Ces correspondances doivent être définies comme l'indique le tableau ci-dessous :

Entrée de l'espace des noms	Modèle d'URL
/ows/tr/browse	/ows/db-apps/owa/tr.browse\?dest=*&date=??/??/????
/ows/tr/auth	/ows/db-apps/owa/tr.book\?dest=*&depart=??/??/????&return=??/??/????

/ows/tr/auth	/ows/db-apps/owa/tr.change
/ows/admin/forall	/ows/db-apps/owa/admin.resume
/ows/admin/forall	/ows/db-apps/owa/admin.browse\?empid=[th]???
/ows/admin/auth	/ows/db-apps/owa/admin.update\?empid=????

Clients sécurisés

Le client est authentifié par WebSEAL via un canal de communication codé et sécurisé.

Les clients désirant utiliser l'interface Web doivent en plus se faire enregistrer sur le serveur Web de Travel Kingdom pour recevoir un numéro de compte.

Structure des comptes et des groupes

Vous devez créer les groupes suivant sur le système :

Personnel	Membres du personnel de Travel Kingdom.
TKPerso	Agents de voyage de Travel Kingdom.
PersoAdmin	Membres du service administratif de Travel Kingdom. Notez que ces personnes sont également membres du groupe Personnel.
Clients	Clients de Travel Kingdom voulant passer leurs réservations par l'Internet.

Attribuez un compte à chaque utilisateur défini dans le domaine sécurisé de manière à ce que le serveur WebSEAL puisse identifier chacun d'eux. WebSEAL communique l'identité de chaque utilisateur aux serveurs Web Oracle et met en oeuvre une solution de connexion unique (SSO) donnant accès à toutes les ressources Web disponibles.

Contrôle d'accès

La configuration mise en place jusqu'ici a établi les contrôles d'accès suivants :

/ows/tr/browse	unauthenticated	Tr
	any_authenticated	Tr
/ows/tr/auth	unauthenticated	-
	any_authenticated	-
	group TKPerso	Tr
	group Clients	PTr
/ows/admin/forall	unauthenticated	-
	any_authenticated	-
	group Personnel	Tr
/ows/admin/auth	unauthenticated	-
	any_authenticated	-
	group PersoAdmin	Tr

Les membres des groupes Clients et TKPerso ont les mêmes privilèges sur les objets de réservation et de gestion des voyages, à une différence près : les clients doivent coder leurs informations (droit de confidentialité) pour plus de sécurité lors de l'envoi de données sensibles via l'Internet non sécurisé. Ces données sensibles concernent par exemple, les numéros de carte bancaire.

Conclusion

Cet exemple simple illustre les principes de déploiement d'un système capable de :

- sécuriser des informations sensibles ;
- authentifier les utilisateurs ;

- autoriser ou interdire l'accès aux données sensibles.

De plus, les identités des utilisateurs authentifiés du système sont reconnues par le serveur WebSEAL comme par le serveur Web Oracle. Ces identités permettent de mettre en application une solution de connexion unique contrôlable par un système de surveillance (audit).

Chapitre 17. Présentation générale de NetSEAL

Policy Director NetSEAL est une solution de réseau privé virtuel (RPV) permettant de sécuriser toutes les communications TCP/IP en entrée. En tant que gestionnaire de ressources, NetSEAL contrôle la capacité des utilisateurs à se connecter à une application TCP déterminée. NetSEAL assure un contrôle d'accès sur la base du port de destination utilisé par le client et de son identité. NetSEAL intègre tous les serveurs d'applications du réseau au service de sécurité de Policy Director.

Ce chapitre comprend les sections suivantes :

Présentation de NetSEAL

NetSEAL met en place un accès contrôlé aux applications et aux services utilisant TCP dans un domaine sécurisé Policy Director. Les clients Windows peuvent communiquer avec NetSEAL de manière sécurisée par le biais du client Policy Director NetSEAT.

Les communications entre NetSEAT et NetSEAL peuvent être sécurisées au moyen d'un tunnel SSL ou d'un tunnel GSS. Dans les deux cas, la liaison sécurisée établie entre un client NetSEAT et un serveur Policy Director est authentifiée à l'aide du nom d'utilisateur et du mot de passe du client à l'origine de la requête.

- Vous devez utiliser un canal SSL pour sécuriser les communications entre NetSEAT et NetSEAL.
- Vous devez utiliser des tunnels GSS ou des jonctions NetSEAL pour sécuriser les communications entre deux serveurs NetSEAL. Les tunnels GSS établis entre plusieurs serveurs Policy Director sont toujours authentifiés sur la base de l'utilisateur du serveur Policy Director qui établit la connexion pour le compte du client. Les deux serveurs s'authentifient mutuellement via le tunnel GSS, le deuxième ayant la charge du contrôle d'accès sur le client.

Les jonctions NetSEAL déterminent le sens des transmissions pour les communications avec un autre serveur ou réseau Policy Director, via un serveur Policy Director. Vous devez utiliser un tunnel GSS pour sécuriser les communications transitant par une jonction NetSEAL.

NetSEAL opère un contrôle d'accès allégé. Ce contrôle s'effectue jusqu'au port d'écoute de l'application. Les ressources utilisées par cette application ne bénéficient d'aucun contrôle d'accès renforcé.

Ce chapitre détaille plusieurs configurations de réseau utilisant NetSEAL. Les exemples donnés dans les schémas utilisent l'application de connexion à distance TCP TELNET. Dans chaque exemple, NetSEAL répond à une requête selon les paramètres suivants :

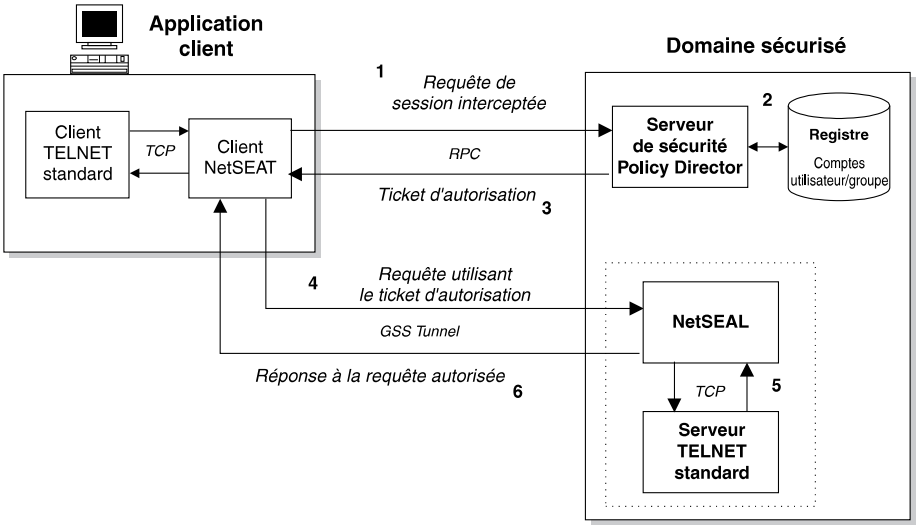
- La source de la requête ;

- Les autorisations détenues sur les objets impliqués (ports de destination et jonctions NetSEAL par exemple) ;
- Les principaux prenant part à la connexion.

Communication GSS entre un client NetSEAT et NetSEAL

Lorsque NetSEAT est configuré pour utiliser un tunnel GSS, il intercepte la requête sortante au moyen d'un RPC (appel de processus à distance) et authentifie le client auprès du serveur de sécurité de Policy Director. De plus, un contrôle d'autorisation est réalisé sur le port associé à l'application demandée.

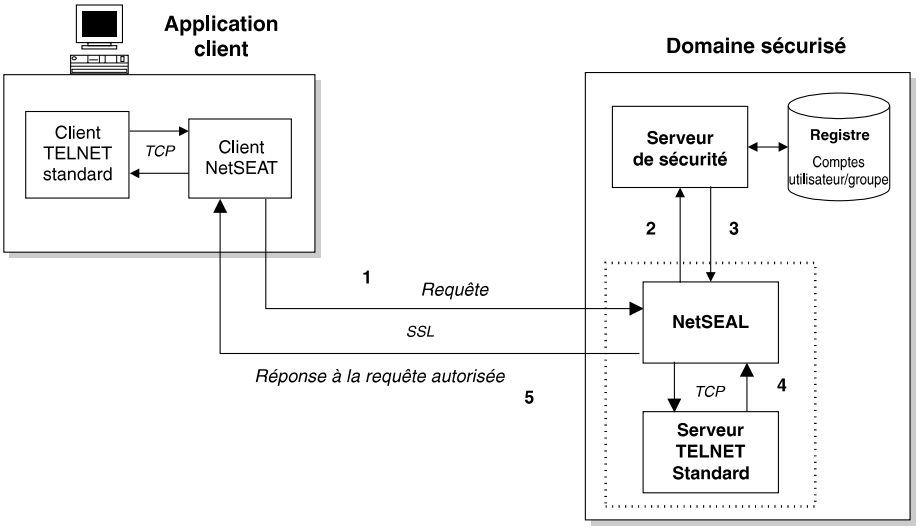
Si les processus d'authentification et d'autorisation aboutissent, un tunnel GSS est établi entre NetSEAT et le serveur NetSEAL. L'accès à l'application TCP à partir de NetSEAL se fait par le biais du protocole TCP.



Communication SSL entre un client NetSEAT et NetSEAL

Lorsque vous configurez NetSEAT de manière à utiliser la couche SSL, les procédures d'authentification et d'autorisation sont partagées entre NetSEAL et les services de sécurité de Policy Director. NetSEAL peut accepter un nom d'utilisateur et un mot de passe comme données d'identité d'un client.

Si ces deux processus valident l'utilisateur, Policy Director traite la requête. Utilisez TCP pour accéder à l'application TCP à partir de NetSEAL.

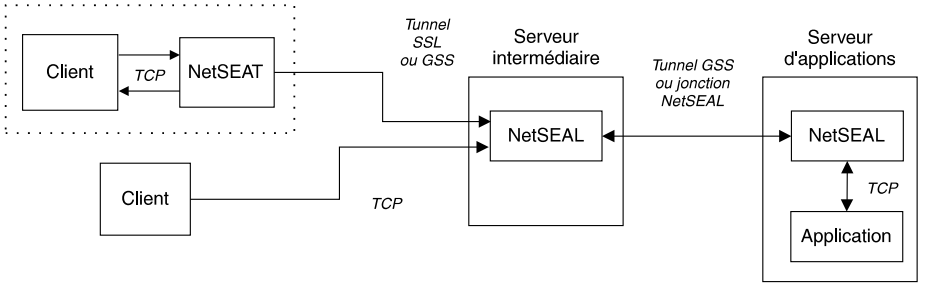


Segments de réseau NetSEAL

Dans le contexte d'une transaction avec NetSEAL, la requête de connexion passe par plusieurs niveaux de protection dans son cheminement à travers le réseau. Comme l'explique la section «Communication SSL entre un client NetSEAT et NetSEAL» à la page 230, le client NetSEAT peut établir une connexion SSL ou GSS avec le serveur NetSEAL.

Remarque : Les connexions entre serveurs NetSEAL sont toujours de type GSS. N'utilisez pas de connexion SSL entre deux serveurs NetSEAL.

La dernière partie de la route entre NetSEAL et le port de l'application TCP locale ou distante utilise toujours TCP.



Le tableau suivant illustre les différents niveaux de protection selon les segments de la connexion :

Segment de la connexion	Protection
Client NetSEAT vers serveur NetSEAL	Tunnel SSL ou GSS
Client TCP vers serveur NetSEAL	Aucune
Serveur NetSEAL vers serveur NetSEAL	Tunnel GSS
Jonctions NetSEAL	Tunnel GSS
Serveur NetSEAL vers port d'application TCP	Aucune

NetSEAL applique le même processus de décision de connexion pour les applications locales ou distantes.

- Le port demandé est-il protégé (par une LCA) ?
- Si oui, l'utilisateur possède-t-il les autorisations requises pour l'accès ?
- Si non, la poursuite de la connexion est autorisée.

NetSEAL sépare aussi la gestion des données entrantes demandées par le gestionnaire de sécurité du traitement de la connexion sortante. En d'autres termes, le gestionnaire de sécurité n'a pas besoin de savoir si le client NetSEAT intercepte la requête de connexion localement ou à distance.

Exemples de services entre un client et NetSEAL

Les exemples suivants illustrent les types d'interaction possible entre un client et une application TCP protégée par NetSEAL. Ces clients peuvent être des clients NetSEAT ou non.

Les approches possibles sont les suivantes :

- «Connexion entrante par tunnel à un serveur Policy Director».
- «Connexion entrante par tunnel à un hôte protégé» à la page 233.
- «Connexion entrante TCP à un serveur Policy Director» à la page 234.

Connexion entrante par tunnel à un serveur Policy Director

Dans cette première approche, vous devez configurer un client NetSEAT pour intercepter les connexions sortantes destinées à une application du serveur Policy Director. Une fois la communication interceptée par le client NetSEAT, un tunnel sécurisé est établi entre le serveur Policy Director et NetSEAL. Dans cet exemple, la requête, adressée au port 23, est acheminée via ce tunnel.

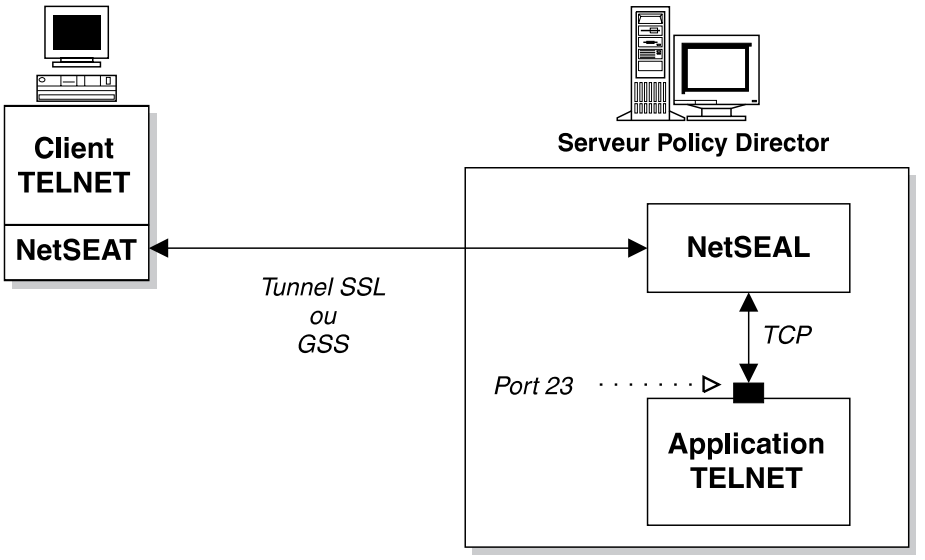
Le processus d'authentification est transparent du point de vue de l'utilisateur.

Le serveur NetSEAL accomplit la transaction en fonction des paramètres suivants :

D'après la LCA du port, l'utilisateur peut-il s'y connecter ?

Oui—Etablir une connexion TCP avec le port demandé.

Non—Rejeter la requête de connexion.



Connexion entrante par tunnel à un hôte protégé

Cet exemple met en scène une application installée sur un serveur distant protégé. Le serveur d'applications peut être un serveur Policy Director ou un serveur tiers. Policy Director utilise toujours GSS pour les communications entre deux serveurs NetSEAL.

NetSEAL peut protéger des applications TCP résidant sur des plates-formes non prises en charge par Policy Director.

Le serveur NetSEAL accomplit la transaction en fonction des paramètres suivants :

1. L'utilisateur peut-il se connecter au port demandé sur le serveur de destination (d'après sa LCA) ?

   Oui—Continuer.

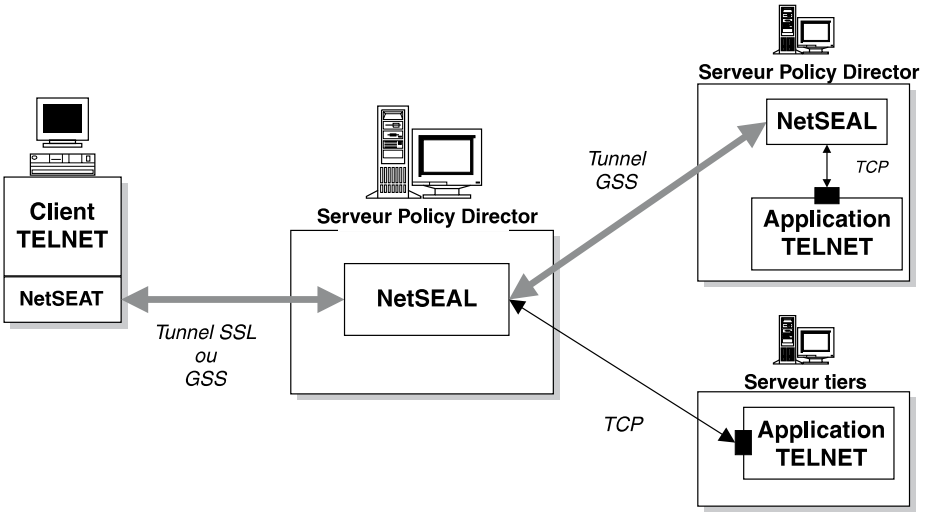
   Non—Rejeter la requête de connexion.

2. Le serveur de destination est-il un serveur Policy Director ?

   Oui—Etablir un tunnel sécurisé avec le serveur et une connexion TCP sur le port demandé.

   Non—Etablir une connexion TCP (non sécurisée) sur le port demandé.

Un serveur d'applications tiers dispose toujours d'une connexion TCP non protégée. Utilisez ce type de configuration dans un environnement de réseau sécurisé.



Connexion entrante TCP à un serveur Policy Director

Cet exemple envisage la situation d'un client TCP autre que NetSEAT. Policy Director associe ces clients au type unauthenticated (non authentifié). Si le port demandé n'est pas protégé (sans LCA), Policy Director y autorise l'accès. Si une liste de contrôle d'accès le protège, le gestionnaire de sécurité la consultera pour connaître les droits d'accès associés au type unauthenticated.

Cette configuration protège l'accès direct aux services du réseau. Un service d'autorisation externe peut ensuite utiliser l'adresse IP du client pour déterminer ses droits d'accès.

Le serveur NetSEAL accomplit la transaction en fonction des paramètres suivants :

1. La requête est-elle interceptée par Policy Director (une LCA est-elle attachée au port) ?

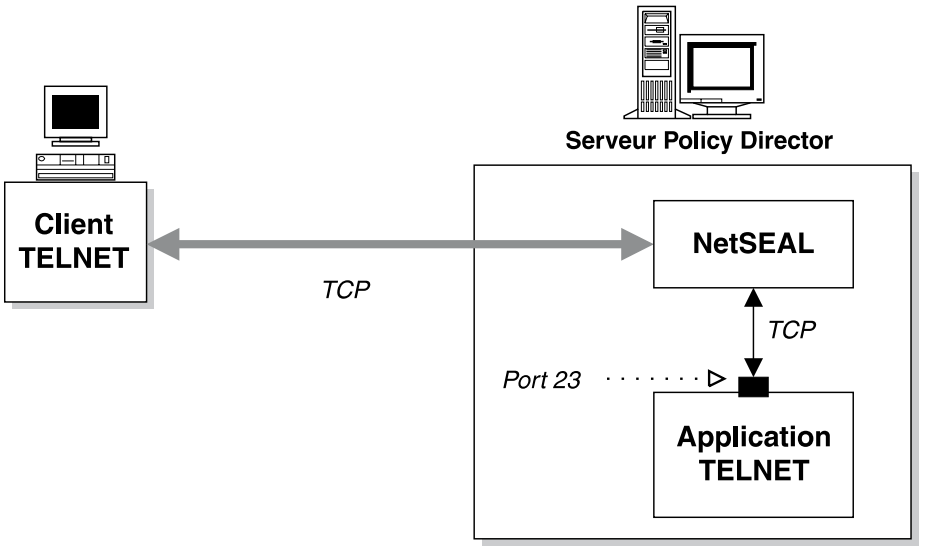
   Oui—Transmettre la requête au gestionnaire de sécurité (secmgrd).

   Non—Autoriser la connexion entrante.

2. Le port accepte-t-il les requêtes non authentifiées ?

   Oui—Etablir une connexion TCP avec le port demandé.

   Non—Rejeter la requête de connexion.



Services entre deux serveurs NetSEAL

Les exemples suivants illustrent les types d'interaction possible entre deux serveurs. Le premier serveur NetSEAL (doté d'un client local) initialise lui-même les connexions au lieu de passer par un client NetSEAT distant.

Le premier serveur NetSEAL (doté d'un client local) initialise lui-même les connexions au lieu de passer par un client NetSEAT distant. Ce client local pourrait opérer à partir de la console du serveur ou le contacter à distance par TELNET. Un serveur NetSEAL d'arrière-plan peut protéger l'application TCP.

Les approches possibles sont les suivantes :

- «Connexion sortante à un serveur Policy Director».
- «Connexion sortante à un hôte protégé» à la page 236.

Connexion sortante à un serveur Policy Director

Vous devez utiliser un tunnel GSS pour établir une connexion entre deux serveurs Policy Director NetSEAL. Le premier serveur NetSEAL (doté d'un client local) initialise lui-même les connexions au lieu de passer par un client NetSEAT distant. Policy Director peut autoriser ou interdire une connexion et la protéger le cas échéant.

Le serveur Policy Director accomplit la transaction en fonction des paramètres suivants :

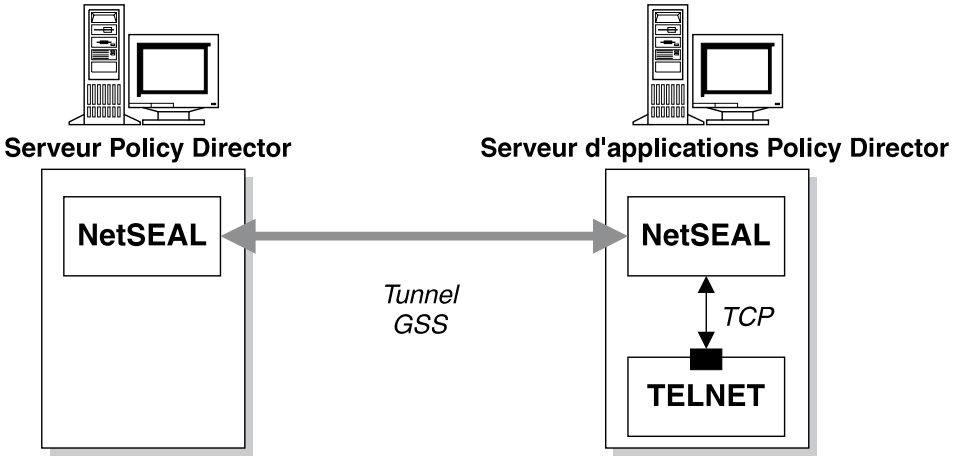
1. Le port demandé sur la machine de destination est-il protégé (par une LCA) ?

   Oui—Transmettre la requête au gestionnaire de sécurité (secmgrd).

   Non—Autoriser la connexion en sortie.
2. Le port accepte-t-il les requêtes non authentifiées ?

   Oui—Etablir un tunnel sécurisé avec le serveur et une connexion TCP sur le port demandé.

   Non—Rejeter la requête de connexion.



Connexion sortante à un hôte protégé

Vous pouvez utiliser TCP pour établir une connexion entre un serveur Policy Director NetSEAL et un serveur tiers. Notez cependant qu'il s'agit alors d'une connexion non sécurisée. Le serveur tiers d'arrière-plan n'héberge pas de serveur NetSEAL. Policy Director ne peut qu'autoriser ou interdire la connexion au serveur d'arrière-plan ; il ne peut pas sécuriser les communications qu'elle dessert.

Le serveur Policy Director accomplit la transaction en fonction des paramètres suivants :

1. Le port demandé sur la machine de destination est-il protégé (par une LCA) ?

   Oui—Transmettre la requête au gestionnaire de sécurité (secmgrd).

   Non—Autoriser la connexion en sortie.
2. L'utilisateur a-t-il l'autorisation d'accéder au port demandé sur le serveur de destination ?

   Oui—Continuer.

   Non—Rejeter la requête de connexion.
3. L'intégrité et la confidentialité sont-elles activées sur le port ?

   Oui—Rejeter la requête de connexion.

   Non—Etablir une connexion TCP sur le port demandé.

Présentation des jonctions NetSEAL

Les jonctions NetSEAL permettent d'établir des communications sécurisées entre un réseau de serveurs Policy Director et un serveur ou un réseau de destination tiers. Les jonctions NetSEAL déterminent le sens de transmission des paquets de données à travers un serveur Policy Director.

Les jonctions NetSEAL sont des routes statiques unidirectionnelles. Ces jonctions unidirectionnelles permettent à l'administrateur de chaque serveur Policy Director de mieux contrôler l'accès aux réseaux. Chaque sens de communication implique une jonction NetSEAL distincte. En revanche, le flux de données transitant par une jonction NetSEAL est toujours bidirectionnel.

Un tunnel GSS a pour objet de sécuriser les communications utilisant une jonction NetSEAL. Le dernier serveur Policy Director défini dans le chemin de

communication utilise, pour sa part, une connexion TCP pour communiquer avec le port de destination. Ce port de destination peut être sur le serveur Policy Director lui-même.

Les jonctions NetSEAL assurent la protection et la sécurité des données communiquées dans une organisation. Vous pouvez segmenter cette organisation selon des critères géographiques ou structurels. Par exemple, les jonctions NetSEAL peuvent répondre aux situations dans lesquelles un réseau non sécurisé sépare deux serveurs Policy Director géographiquement éloignés (particulièrement si ces deux serveurs Policy Director appartiennent au même domaine sécurisé).

Chaque jonction a un serveur Policy Director source, une destination, et un sens de routage. La destination peut être un autre serveur Policy Director ou un réseau. Les jonctions s'adaptent facilement à un pare-feu dans la mesure où toutes les transactions qu'elles acheminent franchissent le pare-feu en un même point d'accès.

Configuration des jonctions NetSEAL

Les jonctions NetSEAL se créent au moyen de l'utilitaire **ivadmin**. Cet utilitaire comprend des commandes permettant d'ajouter, de supprimer et d'afficher les jonctions NetSEAL. Vous pouvez créer des jonctions entre plusieurs serveurs Policy Director ou entre un serveur Policy Director et un réseau.

Reportez-vous à la section «Annexe A. Administration de Policy Director avec l'utilitaire ivadmin» à la page 277.

Jonctions NetSEAL et contrôle d'accès

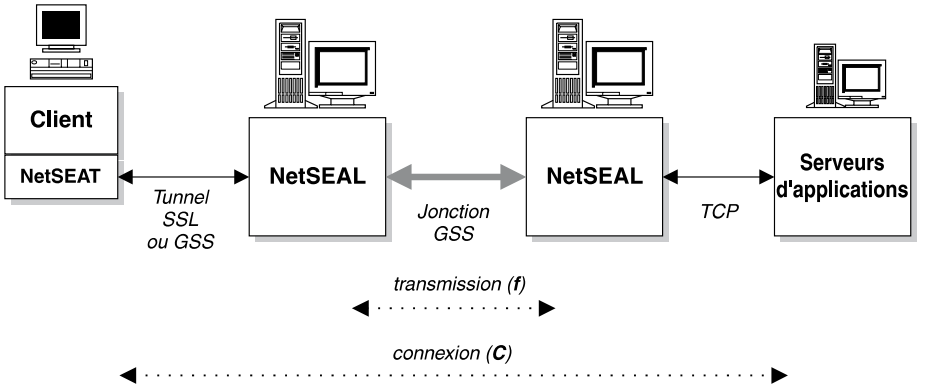
NetSEAL reconnaît deux autorisations de liste de contrôle d'accès (LCA) pour contrôler l'accès au port d'un serveur d'applications.

L'accès à ce port de destination est contrôlé par une LCA définie sur l'objet le représentant dans l'espace des noms protégé. Pour qu'un utilisateur ou un groupe puisse accéder au port, cette LCA doit contenir une entrée avec le droit de connexion (C).

Le trafic de la jonction NetSEAL est contrôlé par une LCA définie sur le serveur Policy Director responsable de la connexion sortante. Pour qu'un utilisateur ou un groupe puisse accéder à la jonction, cette LCA doit contenir une entrée avec le droit de transmission (f).

Vous devez définir, et contrôler, un droit de transmission (f) sur chaque objet de serveur Policy Director membre d'une chaîne de serveurs reliés par jonction.

Autorisations des objets protégés par NetSEAL :	Accès	Description
C	connexion	Autorise l'établissement d'une connexion entre un serveur NetSEAL et un service protégé distant ou local.
f	transmission	Permet d'établir des connexions sortantes via une jonction NetSEAL (de traverser la jonction).



Exemples de services contrôlés par des jonctions NetSEAL

Les jonctions NetSEAL assurent la protection et la sécurité des données communiquées dans une organisation. Vous pouvez segmenter cette organisation selon des critères géographiques ou structurels. Par exemple, les jonctions NetSEAL peuvent répondre aux situations dans lesquelles un réseau non sécurisé sépare deux serveurs Policy Director géographiquement éloignés (particulièrement si ces deux serveurs Policy Director appartiennent au même domaine sécurisé).

Les approches possibles sont les suivantes :

- «Connexion entrante par jonction à un serveur Policy Director».
- «Connexion entrante par jonction à un hôte protégé» à la page 239.
- «Connexion sortante par jonction à un serveur Policy Director» à la page 239.
- «Connexion sortante par jonction à un hôte protégé» à la page 240.

Connexion entrante par jonction à un serveur Policy Director

Cet exemple met en scène une application installée sur un serveur Policy Director distant protégé. La procédure utilisée établit un tunnel GSS entre les serveurs Policy Director sous la forme d'une jonction NetSEAL. Une fois défini, le contrôle d'accès au port de destination vérifie l'existence du droit de transmission.

Le serveur Policy Director accomplit la transaction en fonction des paramètres suivants :

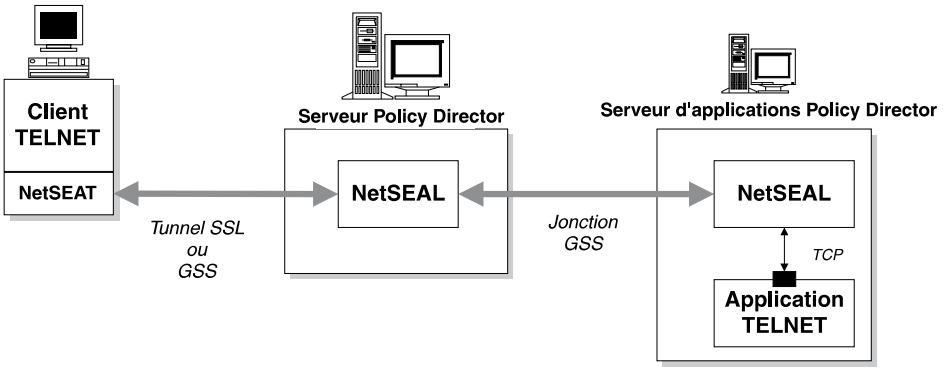
1. L'utilisateur peut-il se connecter au port demandé sur le serveur de destination (d'après sa LCA) ?

   Oui—Continuer.

   Non—Rejeter la requête de connexion.
2. L'utilisateur peut-il transmettre des données via la jonction ?

   Oui—Transmettre la requête via la jonction GSS. Etablir une connexion TCP sur le port demandé.

   Non—Rejeter la requête de connexion.



Connexion entrante par jonction à un hôte protégé

Cet exemple met en scène une application installée sur un serveur tiers distant protégé. La procédure utilisée établit un tunnel GSS entre les serveurs Policy Director sous la forme d'une jonction NetSEAL. Une fois défini, le contrôle d'accès au port de destination vérifie l'existence du droit de transmission.

Le serveur Policy Director accomplit la transaction en fonction des paramètres suivants :

1. L'utilisateur peut-il se connecter au port demandé sur le serveur de destination (d'après sa LCA) ?

   Oui—Continuer.

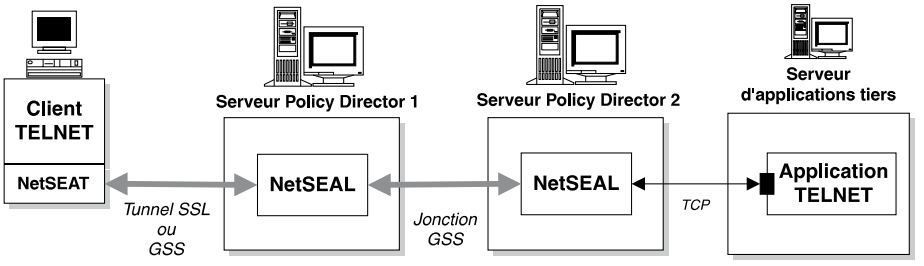
   Non—Rejeter la requête de connexion.

2. L'utilisateur peut-il transmettre des données via la jonction ?

   Oui—Transmettre la requête via la jonction. Etablir une connexion TCP sur le port demandé.

   Non—Rejeter la requête de connexion.

Un serveur d'applications tiers dispose toujours d'une connexion TCP non protégée. Utilisez ce type de configuration dans un environnement de réseau sécurisé.



Connexion sortante par jonction à un serveur Policy Director

Cet exemple met en scène une application installée sur un serveur Policy Director distant protégé. La procédure utilisée établit un tunnel GSS entre les serveurs Policy Director sous la forme d'une jonction NetSEAL. Une fois défini, le contrôle d'accès au port de destination vérifie l'existence du droit de transmission, ce qui procure au serveur assimilé tiers une bonne protection.

Le serveur Policy Director accomplit la transaction en fonction des paramètres suivants :

1. Le port demandé sur la machine de destination est-il protégé (par une LCA) ?

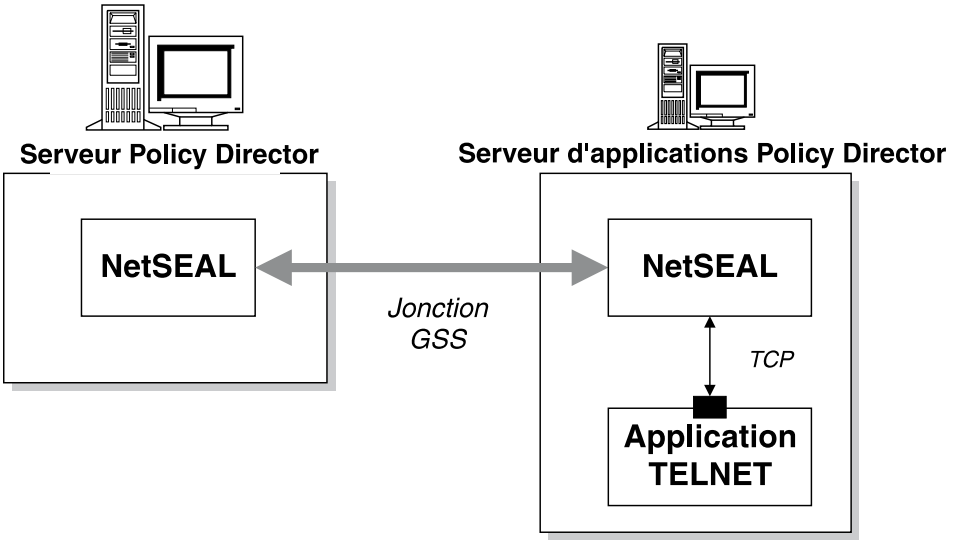
Oui—Transmettre la requête au gestionnaire de sécurité (secmgrd).

Non—Autoriser la connexion en sortie.

2. L'utilisateur peut-il transmettre des données via la jonction ?

   Oui—Transmettre la requête via la jonction. Etablir une connexion TCP sur le port demandé.

   Non—Rejeter la requête de connexion.



Connexion sortante par jonction à un hôte protégé

Cet exemple met en scène une application installée sur un serveur tiers distant protégé. La procédure utilisée établit un tunnel GSS entre les serveurs Policy Director sous la forme d'une jonction NetSEAL. Une fois défini, le contrôle d'accès au port de destination vérifie l'existence du droit de transmission.

Le serveur Policy Director accomplit la transaction en fonction des paramètres suivants :

1. Le port demandé sur la machine de destination est-il protégé (par une LCA) ?

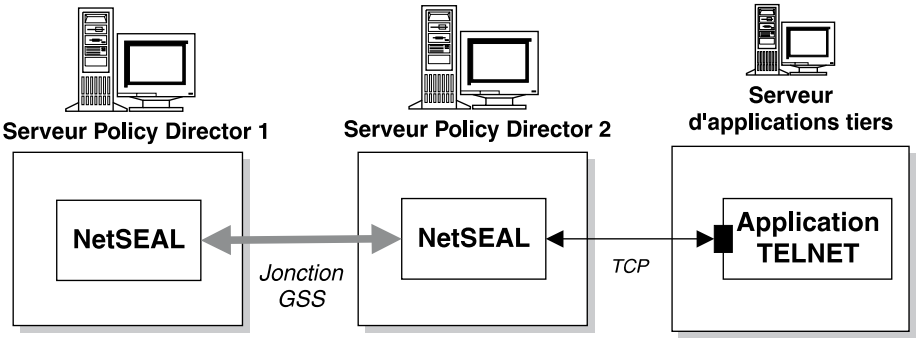
   Oui—Transmettre la requête au gestionnaire de sécurité (secmgrd).

   Non—Autoriser la connexion en sortie.

2. L'utilisateur peut-il transmettre des données via la jonction ?

   Oui—Transmettre la requête via la jonction. Etablir une connexion TCP sur le port demandé.

   Non—Rejeter la requête de connexion.



Protection des services TCP

Les listes de contrôle d'accès définies sur les ports des services TCP contrôlent l'accès à ces ports. L'utilisateur d'un client NetSEAL peut accéder à un service TCP lorsque la LCA attachée à son port contient un droit de connexion (C) pour cet utilisateur.

Pour interdire l'accès à un service TCP donné, il suffit que l'administrateur supprime le droit de connexion dans l'entrée appropriée de la liste de contrôle d'accès.

Les autorisations de LCA peuvent également contrôler le niveau de protection des communications de NetSEAL. Ce niveau de protection peut être déterminé en combinant les droits intégrité et confidentialité. Vous pouvez, de plus, contrôler le niveau de protection des communications sortantes par le biais d'une jonction NetSEAL. Pour contrôler le niveau de protection, les entrées de la liste de contrôle d'accès appliquée au port de destination doivent contenir le droit d'intégrité et le droit de confidentialité.

La liste de contrôle d'accès définie doit être parfaitement adaptée à l'adresse de réseau et au masque de réseau de l'objet à protéger. La présence ou l'absence d'une LCA sur le port de destination n'intervient pas dans la recherche de l'objet sur lequel le contrôle de LCA doit s'effectuer.

Dans l'exemple du tableau ci-dessous, si un client Telnet contacte l'adresse 10.0.0.1, l'accès lui sera accordé en vertu de la liste de contrôle d'accès LCA3. Policy Director accorde l'accès alors que le port 23 du réseau de destination est attaché à une LCA explicite.

10.0.0.0:255.255.255.0	LCA1
10.0.0.0:255.255.255.0/Port 23	LCA2
10.0.0.1:255.255.255.255	LCA3

Chapitre 18. NetSEAL - Tâches d'administration générale

Policy Director NetSEAL est une solution de réseau privé virtuel (RPV) permettant de sécuriser toutes les communications TCP/IP en entrée. En tant que gestionnaire de ressources, NetSEAL contrôle la capacité des utilisateurs à se connecter à une application TCP déterminée. Ce chapitre détaille les tâches d'administration générale que vous devez exécuter pour adapter NetSEAL aux besoins de votre réseau.

Ce chapitre comprend les sections suivantes :

Activation et désactivation de la sécurité NetSEAL

L'utilitaire **ivadmin** permet d'activer et de désactiver NetSEAL.

Activation de NetSEAL

Pour activer NetSEAL sur un serveur Policy Director :

```
ivadmin> server enable /NetSEAL/nom_hôte
```

Où nom d'hôte est le nom du serveur, sans le nom de domaine.

Lorsque le service est déjà activé ou que la spécification de service est incorrecte, Policy Director renvoie un message d'erreur.

Policy Director désactive NetSEAL par défaut, sauf si vous avez installé le composant NetSEAL IVTrap.

Désactivation de NetSEAL

Pour désactiver NetSEAL sur un serveur Policy Director :

```
ivadmin> server disable /NetSEAL/nom_hôte
```

Etat de NetSEAL

Pour connaître l'état du serveur NetSEAL, utilisez la commande **ivadmin server status** :

```
ivadmin> server
status /NetSEAL/nom_hôte
```

Le rapport d'état indique :

- si le serveur NETSEAL est activé ou désactivé ;
- si le serveur NetSEAL est accessible ;

- si les bases de données de configuration des instances du serveur NetSEAL ont été ou non mises à jour.

Utilisation des procédures de contrôle d'accès de NetSEAL

Les autorisations des LCA de Policy Director peuvent protéger les connexions NetSEAL pour :

- permettre l'accès aux ports de destination des services TCP ;
- permettre l'envoi de paquets de données via les jonctions NetSEAL ;
- assurer l'intégrité et la confidentialité des données.

L'accès au port de destination est contrôlé par une LCA définie sur l'objet le représentant dans l'espace des noms protégé. Pour qu'un utilisateur ou un groupe puisse accéder au port, cette LCA doit contenir une entrée avec le droit de connexion (C). Le droit de connexion peut également protéger l'accès à un serveur d'applications résidant sur un réseau protégé.

Le trafic de la jonction NetSEAL est contrôlé par une LCA définie sur le serveur Policy Director responsable de la connexion sortante. Pour qu'un utilisateur ou un groupe puisse accéder à la jonction, cette LCA doit contenir une entrée avec le droit de transmission (f).

Vous devez définir, et contrôler, un droit de transmission (f) sur chaque objet de serveur Policy Director membre d'une chaîne de serveurs reliés par jonction.

	Accès	**Description**
C	connexion	Autorise l'établissement d'une connexion entre un serveur NetSEAL et un service protégé distant ou local.
f	transmission	Permet d'établir des connexions sortantes via une jonction NetSEAL (de traverser la jonction).

Les autorisations de LCA peuvent également contrôler le niveau de protection des communications de NetSEAL. Ce niveau de protection peut être déterminé en combinant les droits intégrité et confidentialité.

Vous pouvez, de plus, contrôler le niveau de protection des communications sortantes par le biais d'une jonction NetSEAL. Les entrées de la LCA attachée au port de destination doivent contenir les droits intégrité (I) et confidentialité (P). Ces deux droits ne peuvent pas être appliqués à un serveur d'applications tiers (non couvert par Policy Director) résidant sur un réseau sécurisé.

Gestion des réseaux protégés

Les réseaux peuvent être considérés comme des serveurs non protégés par Policy Director mais couverts par NetSEAL. L'utilitaire **ivadmin** permet de définir et de gérer des réseaux. Ses commandes permettent d'ajouter, de supprimer et d'afficher les réseaux protégés.

Commande	**Description**
netseal network add réseau masque_réseau **[**alias_réseau**]**	

	Crée un réseau protégé par NetSEAL. Les arguments réseau et masque_réseau indiquent respectivement un code et un masque d'adresse de réseau IP standard. L'argument optionnel alias_réseau peut être renseigné pour mieux identifier ce réseau. A défaut d'alias, le réseau doit être identifié par un code et un masque d'adresse de réseau. Un message d'erreur apparaît si le réseau spécifié existe déjà.
netseal network delete id_réseau	
	Supprime du système le réseau spécifié. L'argument id_réseau admet les valeurs suivantes : • Un couple code/masque de réseau ; • Un alias de réseau. L'argument id_réseau peut prendre la valeur d'un code/masque de réseau ou d'un alias de réseau. Toutes les références à ce réseau seront supprimées dans le système, les jonctions NetSEAL comprises. Un message d'erreur s'affichera si le réseau ne figure pas dans la base de données.
netseal network list	
	Affiche tous les réseaux définis dans la base de données (code, masque et alias du réseau).

Exemple :

```
ivadmin> netseal network add
10.125.0.0 255.255.255.0 ouest
```

Cette commande ajoute les noeuds 10.125.0.0 à 10.125.0.255 à la spécification d'un réseau protégé par NetSEAL. En outre, elle attribue à cette spécification de réseau le nom d'alias `ouest`.

Gestion des jonctions NetSEAL

Les jonctions NetSEAL déterminent le sens des communications transitant par un serveur Policy Director. Vous pouvez créer des jonctions entre deux serveurs Policy Director ou entre un serveur Policy Director et un réseau. L'utilisation d'un tunnel GSS sécurise les communications transitant par une jonction entre deux serveurs Policy Director.

L'utilitaire **ivadmin** permet de définir et de gérer des jonctions NetSEAL. Ses commandes permettent d'ajouter, de supprimer et d'afficher les jonctions NetSEAL.

Commande	Description
netseal junction add nom_hôte destination	
	Crée une jonction entre un serveur NetSEAL et une destination définie. L'argument nom_hôte désigne le serveur NetSEAL (sans le nom de domaine). L'argument destination admet les valeurs suivantes : • Un serveur Policy Director ; • Un couple code/masque de réseau ; • Un alias de réseau. Un message d'erreur s'affiche si la jonction existe déjà, si le système hôte n'existe pas ou si la destination n'existe pas.
netseal junction delete nom_hôtedestination	

	Supprime une jonction entre un serveur NetSEAL et une destination définie. L'argument nom_hôte désigne le serveur NetSEAL (sans le nom de domaine). L'argument destination admet les valeurs suivantes : • Un serveur Policy Director ; • Un couple code/masque de réseau ; • Un alias de réseau. Un message d'erreur s'affiche si la jonction spécifiée n'existe pas. La commande n'a aucun effet sur la connexion active dans ce cas.
netseal junction list nom_hôte	
	Affiche toutes les jonctions NetSEAL associées au serveur NetSEAL spécifié.

Exemple :

```
ivadmin> netseal junction
add clipper ouest
```

Cette commande crée une jonction entre le serveur NetSEAL `clipper` et le réseau désigné par l'alias `ouest`. Elle définit également le sens du routage (de `clipper` vers `ouest`) puisque les jonctions NetSEAL sont unidirectionnelles.

Gestion des ports protégés

Le serveur NetSEAL de Policy Director fournit des services de sécurité à certains ports, hôtes et réseaux. Par exemple, vous pouvez configurer le serveur NetSEAL de manière à sécuriser le trafic TELNET sur un port déterminé.

L'utilitaire **ivadmin netseal** permet de définir la liste des ports que le serveur NetSEAL doit protéger. Ses commandes permettent d'ajouter, de supprimer et d'afficher les ports protégés. Vous pouvez spécifier des ports de serveurs Policy Director ou des ports de réseaux.

Commande	Description
netseal port add destination id_port	
	Cette commande protège les connexions établies avec la destination indiquée sur le port désigné par l'argument id_port. L'argument destination admet les valeurs suivantes : • Un serveur Policy Director ; • Un couple code/masque de réseau ; • Un alias de réseau. L'argument id_port admet les valeurs suivantes : • Un numéro de port ; • Une série de ports ; • Un alias de port. Un message d'erreur s'affiche si le port est déjà protégé, si le serveur n'existe pas ou si l'alias de port n'existe pas.
netseal port delete destination id_port	

	Cette commande interrompt la protection des connexions établies avec la destination indiquée sur le port désigné. L'argument destination admet les valeurs suivantes : • Un serveur Policy Director ; • Un couple code/masque de réseau ; • Un alias de réseau. L'argument id_port admet les valeurs suivantes : • Un numéro de port ; • Une série de ports ; • Un alias de port. Un message d'erreur s'affiche si le port n'est pas protégé, si le serveur n'existe pas ou si l'alias de port n'existe pas.
netseal port list destination	
	Cette commande affiche la liste des ports de la destination indiquée. L'argument destination admet les valeurs suivantes : • Un serveur Policy Director ; • Un couple code/masque de réseau ; • Un alias de réseau. Un message d'erreur s'affiche si le serveur n'existe pas.

Remarque : Une série de ports s'exprime sous la forme de deux numéros de port séparés par un tiret (par exemple, 22–88).

Exemple :

```
ivadmin> port add ouest 23
```

Cette commande définit le numéro de port 23 du réseau désigné par l'alias "ouest" comme un port protégé par NetSEAL.

Gestion des alias des ports protégés

L'utilitaire **ivadmin** permet de définir et de gérer des alias de port. Ses commandes permettent d'ajouter, de supprimer et d'afficher les alias des ports. Vous pouvez utiliser les alias de port pour mieux identifier les séries de ports avec demande d'alerte.

Commande	Description
netseal port-alias add port alias_port	
	Cette commande crée un alias de port pour le port indiqué. L'argument port admet les valeurs suivantes : • Un numéro de port ; • Une série de ports. Un message d'erreur s'affiche si le port ou la série de ports possède déjà un nom d'alias.
netseal port-alias delete id_port	

	Supprime du système l'alias de port spécifié par l'argument id_port. L'argument id_port admet les valeurs suivantes : • Un numéro de port ; • Une série de ports ; • Un alias de port. Un message d'erreur s'affiche si l'alias de port ne figure pas dans la base de données.
netseal port-alias list	
	Affiche la liste des alias de port définis dans la base de données.

Exemples :

```
ivadmin> netseal port-alias add 23 telnet
```

Cette commande crée l'alias de port `telnet` pour le numéro de port `23`.

```
ivadmin> netseal port-alias add 5000-5010 pilote
```

Cette commande crée l'alias de port "pilote" pour la série de ports 5000 à 5010.

Configuration d'hôtes et de réseaux sécurisés

Le serveur NetSEAL de Policy Director fournit des services de sécurité à certains ports, hôtes et réseaux. Par exemple, vous pouvez configurer le serveur NetSEAL de manière à sécuriser le trafic TELNET sur un port déterminé du serveur Policy Director. De plus, le serveur NetSEAL peut sécuriser un système hôte (en faire un hôte sécurisé) ou un groupe de systèmes hôtes (en faire un réseau sécurisé).

Les strophes `[trusted_hosts]` et `[trusted_networks]` du fichier de configuration secmgrd.conf contiennent des paramètres permettant d'identifier des hôtes et des réseaux sécurisés.

Hôtes sécurisés

Votre serveur NetSEAL communique fréquemment avec certains serveurs (systèmes hôtes) hautement sécurisés. Pour optimiser les performances de ces communications, vous pouvez autoriser NetSEAL à dispenser de contrôle d'accès les requêtes provenant de ces serveurs.

Remarque : Désigner des hôtes sécurisés rend votre système plus vulnérable aux tentatives de détournement d'adresse IP. Prenez soin de protéger les hôtes sécurisés contre ce type de risque.

Par défaut, Policy Director n'identifie aucun hôte sécurisé.

Pour identifier un hôte sécurisé, éditez la strophe `[trusted_hosts]` et entrez-y l'adresse IP et le nom de ce serveur.

Par exemple, pour dispenser de contrôle d'accès toutes les requêtes provenant du serveur nommé "typhon", dont l'adresse IP est 220.12.35.102, tapez :

```
[trusted_hosts]
220.12.35.102 = typhon
```

Si vous utilisez la procédure de demande d'alerte NetSEAL pour sécuriser une machine, vous devez pouvoir vous fier à la machine locale qui assure cette procédure. Sécuriser cette machine locale permet la continuité des services qui y

résident. Ces services continuent de fonctionner même lorsque l'accès non authentifié est désactivé sur un port ou sur une série de ports.

Policy Director a besoin des entrées suivantes pour considérer la machine locale comme étant digne de confiance, c'est-à-dire sécurisée :

- Une entrée pour l'hôte local ;
- Une entrée par adresse IP définie pour cette machine.

Par exemple, l'adresse IP du serveur NetSEAL typhon est 220.12.35.102. Un autre processus résidant sur le même serveur peut avoir l'adresse IP d'hôte local 127.0.0.1. Pour sécuriser toutes les requêtes locales émises par les autres processus installés sur le serveur NetSEAL typhon, tapez :

```
[trusted_hosts]
220.12.35.102 = typhon
127.0.0.1 = localhost
```

Habituellement, une machine ne possède qu'une seule adresse IP. Toutefois, certaines machine sont reliées à plusieurs réseaux et peuvent avoir plusieurs adresses.

Réseaux sécurisés

Si votre réseau comprend des sous-réseaux ou des réseaux locaux composés de systèmes sécurisés, vous pouvez spécifier l'ensemble d'un sous-réseau au lieu de désigner individuellement chaque système hôte.

Par défaut, Policy Director n'identifie aucun réseau sécurisé.

Pour identifier un réseau sécurisé, éditez la strophe `[trusted_networks]` et entrez-y l'adresse IP et le masque de réseau du sous-réseau concerné.

Par exemple, pour dispenser de contrôle d'accès toutes les requêtes provenant du sous-réseau 192.96.32.0, tapez :

```
[trusted_networks]
192.96.32.0 = 255.255.255.0
```

Définition des paramètres de délai d'expiration SSL

Les paramètres de délai d'expiration SSL que vous pouvez définir sont les suivants :

- «Définition du délai d'expiration du cache de session SSL».
- «Définition du délai d'expiration des connexions SSL» à la page 250.

Définition du délai d'expiration du cache de session SSL

La strophe `[ssl]` du fichier de configuration contient un paramètre qui permet de définir le délai d'expiration du cache des sessions SSL statiques.

NetSEAL place les données de droit d'accès dans un cache interne. Ce paramètre de délai d'expiration du cache de session détermine la durée pendant laquelle les données de droits d'accès restent en mémoire au niveau de NetSEAL.

Ce paramètre ne définit pas un délai d'expiration pour inactivité. Il définit la durée de vie du droit d'accès plutôt qu'un délai d'expiration de droit d'accès. Son objectif est de renforcer la sécurité en obligeant l'utilisateur à s'authentifier à nouveau une fois atteint le délai d'expiration spécifié.

Le délai d'expiration par défaut du cache (en secondes) est :

```
[ssl]
ssl-cache-timeout = 3600
```

Ajustez cette valeur au mieux pour équilibrer les performances du serveur et la facilité d'emploi en fonction du nombre de requêtes SSL que le serveur doit traiter.

Définition du délai d'expiration des connexions SSL

La strophe [ssl] du fichier de configuration contient un paramètre qui permet de définir le délai d'expiration des connexions SSL.

Lorsque NetSEAL accepte une demande de connexion SSL adressée par un client NetSEAT via son tunnel SSL, un échange de protocoles SSL doit avoir lieu. Le paramètre de délai d'expiration détermine le délai pendant lequel le gestionnaire de sécurité attend que NetSEAT initialise un échange de protocoles SSL au début d'une connexion SSL. Une fois ce délai dépassé, le gestionnaire de sécurité interrompt la connexion.

Le délai d'expiration par défaut des connexions SSL (en secondes) est :

```
[ssl]
ssl-init-connect-timeout = 120
```

Attribution des connexions NetSEAL

Les paramètres d'attribution des connexions NetSEAL se trouvent dans la strophe [netseal] du fichier de configuration secmgrd.conf.

Le paramètre max-connections définit le nombre maximal de connexions simultanément autorisées par NetSEAL.

La valeur par défaut définie à l'installation de Policy Director est :

```
[netseal]
max-connections = 32
```

Cette valeur peut être adaptée aux conditions de trafic de votre réseau. Si vous définissez une valeur trop faible, des demandes de connexion seront rejetées dans les périodes de forte activité. Dans le cas contraire, l'utilisation des ressources et les performances du réseau ne seront pas optimales.

Remarque : La limite inférieure qu'impose ce paramètre de configuration est 20. Si vous tentez d'entrer une valeur inférieure, le paramètre reprend automatiquement la valeur 20.

Chapitre 19. Présentation générale de NetSEAT

Le client NetSEAT de Policy Director permet aux clients Windows de devenir membres d'un domaine sécurisé par Policy Director. NetSEAT propose des fonctions de transmission par tunnel sécurisé entre les clients Windows et les serveurs Policy Director. NetSEAT peut coder les communications au moyen de tunnels GSS ou SSL.

Ce chapitre comprend les sections suivantes :

Présentation du client NetSEAT

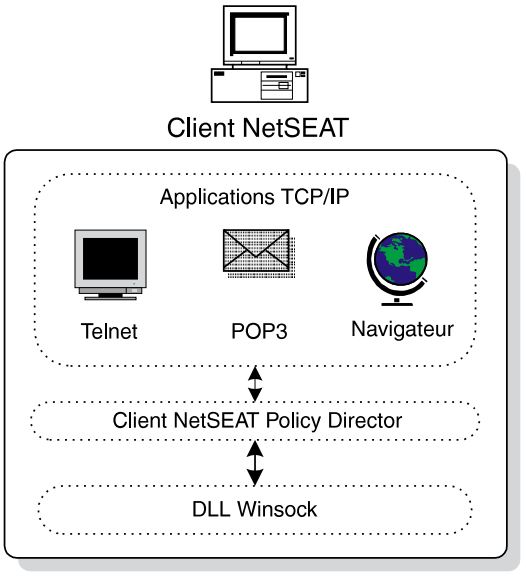
Le client NetSEAT de Policy Director permet aux clients Windows de communiquer en toute sécurité avec des serveurs NetSEAL et avec WebSEAL. Une fois installé sur une station de travail Windows, le client NetSEAT la configure pour en faire un domaine sécurisé par Policy Director. Dans ce domaine sécurisé, NetSEAT peut utiliser les services d'authentification et d'autorisation de Policy Director.

NetSEAT fournit l'authentification et la protection des messages au niveau du protocole de réseau. Une application n'a pas besoin d'être recompilée ou reliée pour utiliser NetSEAT.

NetSEAT sécurise le trafic de réseau entre le client Windows et un serveur Policy Director en interceptant les requêtes avant qu'elles ne traversent la couche Winsock. NetSEAT utilise ses données de configuration pour reconnaître les requêtes émises à partir d'applications génériques TCP/IP. Ces applications génériques TCP/IP comprennent TELNET, POP3 ou HTTP.

Lorsqu'une requête de client est envoyée à une application résidant sur un serveur Policy Director, NetSEAT établit de manière transparente un tunnel sécurisé avec ce serveur, puis oriente la requête vers ce tunnel.

NetSEAT sécurise et code les communications adressées à un serveur Policy Director selon deux méthodes possibles : le tunnel SSL ou le tunnel GSS. Un tunnel SSL utilise la couche SSL pour coder les communications. Un tunnel GSS utilise l'API GSS pour produire le même résultat.



Configurations prises en charge

Vous pouvez installer le client NetSEAT pour différents usages comme le décrivent les sections ci-dessous :

- «Client de réseau privé virtuel (RPV)».
- «Module de support de Policy Director pour Windows NT».
- «Module de support de Policy Director pour la console de gestion» à la page 253.

Client de réseau privé virtuel (RPV)

Vous pouvez configurer NetSEAT comme un client de réseau privé virtuel (RPV) utilisant un tunnel sécurisé pour créer une liaison de communication sécurisée avec un serveur NetSEAL Policy Director.

Dans ce rôle de client RPV, NetSEAT peut coder les communications à l'aide des types de tunnel suivants :

- SSL
- GSS

Module de support de Policy Director pour Windows NT

Policy Director installe NetSEAT comme module de support à chaque installation des composants de Policy Director pour serveur Windows NT. Les versions de Policy Director pour Solaris et AIX ne requièrent pas ce support de la part du client NetSEAT.

Dans ce rôle, le client NetSEAT apporte une fonction d'alerte au noyau à l'usage des services de sécurité de Policy Director.

En tant que module de support de Policy Director pour Windows NT, NetSEAT a besoin des services suivants :

- Répartiteur des services de répertoire
- Tunnel GSS

Utilisez la transmission par tunnel GSS si vous installez le client NetSEAT comme module de support pour Policy Director pour Windows NT ou pour la console de gestion Policy Director sur Windows.

Module de support de Policy Director pour la console de gestion

Si vous utilisez la console de gestion de Policy Director sur un client Windows, vous devez installer NetSEAT comme module de support. Dans cette configuration, NetSEAT autorise un administrateur à utiliser la console de gestion pour effectuer des tâches d'administration à partir d'un système Windows. Les composants du serveur Policy Director n'ont pas besoin d'être installés sur le système Windows.

En tant que module de support de la console de gestion, NetSEAT requiert les services suivants :

- Répartiteur des services de répertoire
- Tunnel GSS

Utilisez la transmission par tunnel GSS si vous installez le client NetSEAT comme module de support pour Policy Director pour Windows NT ou pour la console de gestion Policy Director sur Windows.

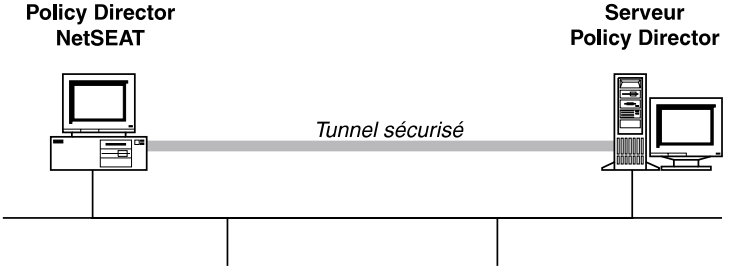
Transmission par tunnel sécurisé

Avant de transmettre une requête de client, NetSEAT contacte le serveur de sécurité de Policy Director au moyen d'un tunnel sécurisé (pour le domaine sécurisé approprié). NetSEAT utilise également ce tunnel sécurisé pour établir l'identité et les droits d'accès du client. Si l'authentification du client aboutit, NetSEAT imbrique la transaction demandée dans un autre tunnel 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 WebSEAL, NetSEAT intercepte la requête de manière transparente. 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, NetSEAT autorise sans le manifester les autres requêtes et tunnels sécurisés sur la base des droits d'accès ainsi établis. Ces droits d'accès permettent à NetSEAT de décider d'autoriser ou non chaque nouvelle requête.

NetSEAT peut établir deux types de tunnel sécurisé comme le décrivent les sections «Utilisation de la transmission par tunnel SSL» et «Utilisation de la transmission par tunnel GSS» à la page 254.



Utilisation de la transmission par tunnel SSL

Le terme tunnel SSL désigne un tunnel sécurisé qui utilise le protocole SSL. NetSEAT utilise la transmission par tunnel SSL lorsqu'il est configuré comme client RPV pour Policy Director NetSEAL. L'utilisation de tunnels SSL simplifie notablement la configuration de NetSEAT. Dans cette situation, l'administrateur n'a

notamment pas besoin de spécifier la configuration des services du DCE à l'intérieur du domaine sécurisé de Policy Director.

Utiliser un tunnel SSL s'apprécie aussi lorsqu'un client veut accéder à des données protégées par un pare-feu. Dans ce mode, NetSEAT utilise un unique port pour toutes les communications avec le serveur Policy Director protégé par le pare-feu. Policy Director imbrique toutes les communications transitant par le port dans un même tunnel sécurisé.

Au cours de la configuration de NetSEAT, vous pouvez spécifier le numéro du port que vous voulez utiliser pour franchir le pare-feu. Ce numéro de port doit correspondre au port configuré sur le serveur NetSEAL.

La transmission par tunnel SSL peut intéresser les utilisateurs authentifiés par le biais d'un registre des utilisateurs LDAP ou DCE.

Utilisation de la transmission par tunnel GSS

Le terme tunnel GSS désigne un tunnel sécurisé qui utilise l'interface de programme d'application des services de sécurité génériques, ou API GSS. NetSEAT utilise un tunnel GSS pour communiquer avec les cellules de l'environnement informatique partagé (le DCE).

Dans ce mode, NetSEAT est un client qui utilise les gestionnaires de sécurité (processus secd) et les serveurs horaires (processus dtsd) installés sur les autres serveurs de la cellule du DCE. NetSEAT utilise également un répartiteur de services de répertoire Policy Director pour déléguer le traitement des requêtes de consultation de l'espace des noms à des services de répertoire de cellules (processus cdsd) situés ailleurs dans la cellule du DCE.

Un tunnel GSS sécurisé est utilisé lorsque vous intégrez, par le biais d'un client Entrust, la clé de connexion PKI d'un utilisateur à son identité, dans le domaine sécurisé Policy Director. Dans cette situation, l'utilisateur se connecte à sa station de travail via un client PKI Entrust. Lorsqu'il tente d'utiliser les services d'autorisation et d'authentification de Policy Director, un tunnel sécurisé est établi entre NetSEAT et les serveurs Policy Director. Ces derniers associent (mappent) automatiquement sa clé de connexion PKI à son identité Policy Director pour prendre les décisions relatives à l'authentification et à l'autorisation.

La transmission par tunnel GSS ne peut pas être utilisée pour les utilisateurs authentifiés par un registre des utilisateurs LDAP.

Accès aux serveurs protégés

Un client NetSEAT peut utiliser le tunnel sécurisé qui le lie à un serveur NetSEAL pour envoyer des requêtes à n'importe quel serveur d'applications distant. Ces serveurs d'applications distants sont protégés par le serveur NetSEAL. Pendant la configuration de NetSEAT, l'administrateur peut spécifier :

- le nom du serveur d'applications ;
- le serveur NetSEAL qui le protège ;
- le type de tunnel sécurisé (SSL ou GSS) établi entre NetSEAT et NetSEAL.

Configuré avec ces données, NetSEAT intercepte les requêtes adressées par le client Windows au serveur d'applications, puis les achemine à un serveur NetSEAL via un tunnel sécurisé.

Vous pouvez également configurer NetSEAT de manière à pouvoir accéder à l'ensemble d'un sous-réseau lorsque celui-ci est protégé par NetSEAL. Cette situation est notamment celle d'un intranet protégé de l'Internet par un serveur NetSEAL Policy Director.

Répartiteur des services de répertoire

Utilisé comme module de support pour des serveurs Policy Director et une console de gestion pour Windows (tunnel GSS), NetSEAT requiert les services d'un répartiteur de services de répertoire (RSR). Un RSR permet de communiquer avec les serveurs Policy Director. Il délègue les consultations de l'espace des noms à un serveur de services de répertoire de cellules localisé dans le même domaine sécurisé.

Policy Director installe automatiquement le répartiteur des services de répertoire avec le module IVMgr (serveur de gestion). Vous devez configurer le client NetSEAT pour qu'il reconnaisse le serveur hébergeant le répartiteur des services de répertoire.

Chapitre 20. NetSEAT - Tâches d'administration générale

Ce chapitre décrit les tâches d'administration de système requises pour configurer le client NetSEAT, pour gérer les contextes de sécurité et pour rechercher et résoudre les incidents éventuels (résolution des incidents).

Ce chapitre comprend les sections suivantes :

Configuration du client NetSEAT

Configurez chaque client NetSEAT dans un domaine sécurisé Policy Director. Vous pouvez configurer ces clients au moment de l'installation ou après. L'utilitaire de configuration de NetSEAT propose une interface utilisateur graphique qui facilite cette tâche.

Accomplissez toutes les tâches de configuration nécessaires dans le domaine sécurisé dont le client NetSEAT est devenu membre.

Certaines de ces tâches ne concernent que les configurations utilisant un type de tunnel sécurisé déterminé (GSS ou SSL). NetSEAT utilise les tunnels sécurisés pour communiquer avec les serveurs Policy Director. Les clients NetSEAT, qui ne sont encore que des clients SSL dédiés aux serveurs NetSEAL, ne demandent qu'un nombre de tâches de configuration limité.

Le tableau suivant présente les tâches de configuration associées à chaque type de tunnel sécurisé :

Types de tunnel	Tâches de configuration
GSS et SSL	• «Ajout de NetSEAT dans un domaine sécurisé» à la page 258 • «Configuration des serveurs NetSEAL» à la page 260 • «Interdiction d'accès à des ressources de réseau» à la page 267

GSS	• «Ajout de serveurs DCE» à la page 259 • «Définition des propriétés du serveur DCE» à la page 260 • «Configuration de la connexion intégrée» à la page 263 • «Configuration de la connexion avancée (intégration de la clé PKI)» à la page 265. • «Définition du retardement maximum» à la page 267
SSL	«Configuration d'un serveur relais SSL» à la page 268

NetSEAT fournit des extensions à plusieurs utilitaires de sécurité de DCE et possède un outil qui permet de contrôler la disponibilité des services du DCE.

Ces utilitaires ne s'emploient que si l'on configure NetSEAT de manière à utiliser la transmission par tunnel GSS.

Les sections suivantes décrivent ces utilitaires :

- Utilisation des utilitaires de sécurité de NetSEAT (reportez-vous à la section «Utilisation des utilitaires de sécurité de NetSEAT» à la page 268).
- Recherche et résolution des incidents avec **netseat_ping** (reportez-vous à la section «Résolution des incidents avec netseat_ping» à la page 270.)

Démarrage de l'utilitaire de configuration de NetSEAT

L'utilitaire de configuration de NetSEAT permet de reconfigurer NetSEAT à sa convenance après l'installation et la configuration initiales. Il permet aussi de configurer NetSEAT si vous ne l'avez pas fait pendant l'installation initiale.

L'utilitaire de configuration de NetSEAT peut s'exécuter de deux façons :

- Pour démarrer l'utilitaire de configuration de NetSEAT depuis le bureau Windows, cliquez sur **Démarrage→ Programmes → Policy Director → NetSEAT → Configuration de NetSEAT**
- Pour démarrer l'utilitaire de configuration de NetSEAT à partir de l'icône **NetSEAT**, avec le bouton droit, cliquez sur cette icône, puis sélectionnez **Propriétés**.

Ajout de NetSEAT dans un domaine sécurisé

Pour ajouter NetSEAT dans un domaine sécurisé :

1. Exécutez l'utilitaire de configuration de NetSEAT. Au lancement, l'utilitaire de configuration de NetSEAT affiche l'onglet **Domaines sécurisés** dans la fenêtre de configuration de NetSEAT.
2. Cliquez sur **Ajout**.

   La boîte de dialogue Nouveau domaine sécurisé apparaît.
3. Tapez le nom du domaine sécurisé auquel NetSEAT appartient.
4. Sélectionnez les protocoles pris en charge par ce domaine, puis cliquez sur **OK**.
   - Si vous avez sélectionné **Activer GSS**, passez à la section «Ajout de serveurs DCE» à la page 259.
   - Si vous avez sélectionné uniquement **Activer SSL**, passez à la section «Configuration des serveurs NetSEAL» à la page 260.
5. **Tunnel GSS uniquement**—Si vous avez configuré plusieurs domaines, revenez à l'onglet **Domaines sécurisés**. Mettez en évidence le domaine utilisé par défaut pour les sessions des utilisateurs. Cliquez sur **Par défaut**.

Si vous n'en avez configuré qu'un, ce domaine devient automatiquement le domaine par défaut.

6. Cliquez sur **OK**.

Ajout de serveurs DCE

Si vous configurez un domaine pour activer l'utilisation des tunnels sécurisés GSS, vous devez définir d'autres options de configuration.

Pour définir le domaine sécurisé (ou cellule) que NetSEAT rejoint, identifiez les noms des serveurs de sécurité Policy Director membres de la cellule. Identifiez aussi les services de sécurité de base fournis par chaque système. Pour chaque serveur, déterminez la présence des services suivants :

- **Sécurité** — services de sécurité (secd)
- **Heure** — services horaires (dtsd)
- **RSR** — répartiteur des services de répertoire (dsb)
- **SRC** — services de répertoire de cellules (cdsd)

  NetSEAT a uniquement besoin de connaître l'emplacement des SRC si le répartiteur des services de répertoire (RSR) fonctionne sur le client NetSEAT. De manière générale, le répartiteur des services de répertoire (RSR) est installé sur le même serveur que le serveur de gestion Policy Director (IVMgr).

Une fois l'entrée du nouveau domaine sécurisé créée, la boîte de dialogue Propriétés du domaine sécurisé apparaît.

1. Cliquez sur **Ajout**.

   La boîte de dialogue Ajout d'un serveur DCE s'affiche dans la fenêtre.
2. Entrez le nom d'un serveur fournissant les services de DCE dans ce domaine sécurisé.
3. Sélectionnez un ou plusieurs des services suivants pour chacun des serveurs : **Sécurité**, **Heure**, **RSR** ou **SRC**.
4. Le cas échéant, cliquez sur **Avancés** pour définir les propriétés avancées de ce serveur DCE.

   Reportez-vous à la section «Définition des propriétés du serveur DCE» à la page 260.
5. Cliquez sur **OK** pour valider la configuration des services pris en charge sur le serveur DCE spécifié.

   La boîte de dialogue Propriétés du domaine sécurisé réapparaît.
6. Acceptez les valeurs par défaut suivantes :
   - Support de connexion intégrée : **Désactivé**
   - Connexion avancée : **ID DCE uniquement**

   Le cas échéant, pour configurer le support de connexion intégrée et la connexion avancée pour le domaine sécurisé, reportez-vous aux sections suivantes :
   - Configuration de la connexion intégrée (section «Configuration de la connexion intégrée» à la page 263).
   - Configuration de la connexion avancée (section «Configuration de la connexion avancée (intégration de la clé PKI)» à la page 265).
7. Une fois le serveur DCE configuré, cliquez sur **OK**.

   La fenêtre Domaine sécurisé réapparaît. Vous avez accompli les tâches de configuration obligatoires pour ajouter un serveur DCE.

Définition des propriétés du serveur DCE

Pendant la configuration d'un serveur DCE, vous pouvez définir les valeurs suivantes dans la boîte de dialogue Propriétés avancées du serveur DCE. Cette tâche de configuration est facultative.

Protocoles et ports

Pour chaque serveur DCE, vous pouvez spécifier le protocole utilisé (TCP ou UDP) par chacun des services de sécurité. Vous pouvez utiliser cette faculté pour définir le mode opératoire vis-à-vis des pare-feu tels que IBM SecureWay Firewall Version 4.1 (composant du produit IBM SecureWay Boundary Server).

Vous pouvez, par exemple, annuler l'accès UDP pour les services du DCE et indiquer les numéros des ports TCP configurés par l'administrateur du pare-feu.

Niveaux de priorité

Lorsque vous définissez des domaines disposant de plusieurs instances d'un ou plusieurs services, vous pouvez choisir l'ordre dans lequel NetSEAT accédera à chacun de ces services. Pour cela, il suffit d'associer à chaque service un entier qui caractérise son niveau de priorité. Plus haute est sa valeur, plus élevé son niveau de priorité.

Pour optimiser les performances, l'administrateur peut amener NetSEAT à choisir en premier le service le plus proche dans la configuration électronique. Si ce service n'est pas disponible, NetSEAT se rend par défaut sur l'instance du service ayant la priorité immédiatement au-dessous.

1. Pour configurer les propriétés avancées, ouvrez la boîte de dialogue Ajout d'un serveur DCE.
2. Sélectionnez l'onglet **Serveur DCE**.
3. Cliquez sur **Avancés**.

   La boîte de dialogue Propriétés avancées du serveur DCE s'affiche.
4. Pour imposer un protocole lors des contacts avec un service DCE, utilisez les cases à cocher placées à côté du service DCE concerné. Invalidez la sélection des cases à cocher correspondant aux protocoles à désactiver.
5. Si nécessaire, entrez les numéros de port dans le champ requis, à côté du service DCE concerné.
6. Définissez le niveau de priorité de chaque service DCE.
7. Cliquez sur **OK**.

Configuration des serveurs NetSEAL

Pour configurer NetSEAT de manière à pouvoir communiquer avec un serveur NetSEAL :

1. Cliquez sur l'onglet **Serveurs NetSEAL** et sélectionnez le domaine sécurisé désiré dans la liste déroulante.
2. Cliquez sur **Ajout**.

   La boîte de dialogue Ajout d'un serveur NetSEAL s'affiche dans la fenêtre.
3. Entrez le nom de la machine hébergeant le serveur NetSEAL.
4. Si NetSEAL utilise d'autres ports que ceux définis par défaut pour la transmission par tunnel SSL ou GSS, entrez ces numéros de port dans les champs prévus à cet effet. Dans le cas contraire, acceptez les valeurs par défaut.

- Les protocoles n'ayant pas été activés lors de la création de l'entrée du domaine sécurisé apparaissent oblitérés.
- Ne sélectionnez pas la case à cocher **Indiquer nom principal** si la transmission par tunnel GSS est activée. N'utilisez cette fonction que pour assurer la compatibilité amont avec les versions antérieures.

5. Si vous utilisez la transmission par tunnel SSL et que la configuration de NetSEAT comprend un serveur relais SSL, Policy Director sélectionne automatiquement la case à cocher **Utiliser un serveur relais**.

   Si vous n'avez pas activé de serveur relais SSL, la case à cocher **Utiliser un serveur relais** est inactive (non sélectionnée et oblitérée). Pour activer un serveur relais SSL dans la configuration de NetSEAT, reportez-vous à la section «Configuration d'un serveur relais SSL» à la page 268.

6. Cliquez sur **OK**.

   L'onglet **Serveur NetSEAL** réapparaît. Le serveur NetSEAL est à présent ajouté à la configuration de NetSEAT.

Ajout d'un serveur protégé

Vous pouvez configurer NetSEAT de manière à spécifier un canal de communication avec les serveurs d'applications protégés par un serveur NetSEAL.

Cette option est proposée lorsque le client NetSEAT utilise la transmission par tunnel GSS ou SSL.

Une fois un serveur d'applications ajouté à la configuration de NetSEAT, NetSEAT intercepte les requêtes envoyées par le client Windows à ce serveur d'applications, puis les achemine à un serveur NetSEAL via un tunnel sécurisé.

Pour ajouter un serveur protégé à la configuration de NetSEAT, indiquez les informations suivantes :

Champ	Définition
Nom de la machine	Nom désignant le serveur d'applications dans le domaine TCP/IP.
Destination du tunnel	Nom du serveur NetSEAL protégeant le serveur d'applications.
Série de ports	Numéro du port du serveur protégé, sécurisé par le serveur NetSEAL. Pour spécifier ce port, ou cette série de ports, sur le serveur NetSEAL, utilisez la commande ivadmin.
Protocole	Protocole de tunnel. Vous pouvez activer à la fois GSS et SSL pour le domaine sécurisé. Choisissez SSL pour Policy Director. La transmission par tunnel GSS s'utilise pour les connexions entre serveurs NetSEAL.

Pour configurer NetSEAT de manière à reconnaître les requêtes adressées à un serveur protégé :

1. Cliquez sur l'onglet **Sécurité de l'hôte**.
2. Cliquez sur **Ajout**.

   La boîte de dialogue Ajout d'un serveur protégé s'affiche dans la fenêtre.

3. Entrez le nom de la machine d'un serveur protégé par un serveur NetSEAL dans le champ **Nom de la machine**.

   Un serveur d'applications ne peut être protégé que par un seul serveur NetSEAL.

4. Pour le champ **Destination du tunnel**, sélectionnez dans la liste déroulante le serveur NetSEAL chargé de la protection du serveur d'applications.
5. Si nécessaire, sélectionnez aussi dans la liste déroulante le protocole de tunnel approprié.
6. Cliquez sur **Ajout**.

   La boîte de dialogue Ajout d'une série de ports apparaît.
7. Indiquez le port ou la série de ports, sur le serveur NetSEAL, que NetSEAL utilise pour communiquer avec le serveur d'applications protégé.
8. Cliquez sur **OK**.

   La boîte de dialogue Ajout d'un serveur protégé réapparaît.

   A titre d'exemple, les entrées ci-dessous définissent les valeurs suivantes :
   - Un serveur NetSEAL nommé "sunshine" protège un serveur d'applications nommé "thunder"
   - Le serveur sunshine protège les communications adressées à thunder sur les ports 5000 à 5005.
   - Policy Director établit un tunnel sécurisé entre le client NetSEAT et le serveur NetSEAL "sunshine".
   - Le tunnel sécurisé est de type SSL.
9. Cliquez sur **OK**.

   L'onglet **Sécurité de l'hôte** réapparaît.

   Policy Director ajoute le serveur protégé à la configuration de NetSEAT.

Ajout d'un sous-réseau protégé

Vous pouvez configurer NetSEAT de manière à spécifier un canal de communication avec un sous-réseau protégé par un serveur NetSEAL. Cette option est proposée lorsque le client NetSEAT utilise la transmission par tunnel GSS ou SSL.

Une fois un sous-réseau d'applications ajouté à la configuration de NetSEAT, NetSEAT intercepte les requêtes envoyées par le client Windows à ce sous-réseau d'applications, puis les achemine à un serveur NetSEAL via un tunnel sécurisé.

Pour ajouter un sous-réseau protégé à la configuration de NetSEAT, indiquez les informations suivantes :

Champ	Définition
Nom d'une machine du sous-réseau	Nom de n'importe quel serveur membre du sous-réseau protégé.
Masque de réseau	Masque de réseau du sous-réseau (par exemple, 255.255.0.0).
Destination du tunnel	Nom du serveur NetSEAL protégeant le sous-réseau.
Protocole	Protocole de tunnel. Vous pouvez activer à la fois GSS et SSL pour le domaine sécurisé. Choisissez SSL pour Policy Director. La transmission par tunnel GSS s'utilise pour les connexions entre serveurs NetSEAL.

Pour configurer NetSEAT de manière à reconnaître les requêtes adressées à un sous-réseau protégé par un serveur NetSEAL :

1. Cliquez sur l'onglet **Sécurité du sous-réseau**.
2. Sélectionnez le domaine sécurisé contenant le serveur NetSEAL qui protège le sous-réseau.

3. Cliquez sur **Ajout**.

   La boîte de dialogue Ajout d'un sous-réseau protégé s'affiche dans la fenêtre.
4. Entrez le nom de n'importe quelle machine membre du sous-réseau protégé par le serveur NetSEAL.

   Un sous-réseau d'applications ne peut être protégé que par un seul serveur NetSEAL.
5. Entrez le masque de réseau du sous-réseau.
6. Pour le champ **Destination du tunnel**, sélectionnez dans la liste déroulante le serveur NetSEAL chargé de la protection du sous-réseau d'applications.
7. Si nécessaire, sélectionnez aussi dans la liste déroulante le protocole de tunnel approprié.

   A titre d'exemple, les entrées ci-dessous permettent à NetSEAT d'accéder au sous-réseau ayant le masque de réseau 255.255.0.0. Le système "thunder" réside dans le sous-réseau. Le serveur NetSEAL "sunshine", qui est également la destination du tunnel SSL, protège le sous-réseau :

   Nom d'une machine du sous-réseau : `thunder`

   Masque de réseau : `255.255.0.0`

   Destination du tunnel `sunshine`

   Protocole `SSL`
8. Cliquez sur **OK**.

   L'onglet **Sécurité du sous-réseau** réapparaît.

   Policy Director a configuré le client NetSEAT pour qu'il puisse communiquer avec le sous-réseau protégé.

Configuration de la connexion intégrée

Vous pouvez, si vous le désirez, installer le support de connexion intégrée pendant l'installation de NetSEAT. Le programme d'installation de NetSEAT modifie alors le registre de Windows NT pour prendre en charge la connexion intégrée.

Une fois le support de connexion intégrée installé, l'utilitaire de configuration de NetSEAT permet d'activer ou désactiver la connexion intégrée pour chaque domaine sécurisé.

Vous pouvez configurer la connexion intégrée pendant l'installation et la configuration initiales de NetSEAT. Vous pouvez aussi le faire plus tard si vous le souhaitez. La connexion intégrée doit être définie séparément pour chaque domaine sécurisé.

Avant de configurer la connexion intégrée, l'utilisateur de NetSEAT doit accomplir les tâches suivantes :

- Obtenir un compte dans chaque domaine sécurisé nécessitant une connexion automatique.
- Configurer le client NetSEAT comme membre de chaque domaine sécurisé.
- Synchroniser le nom d'utilisateur et le mot de passe utilisés pour se connecter au domaine sécurisé avec ceux utilisés dans le domaine Windows NT.

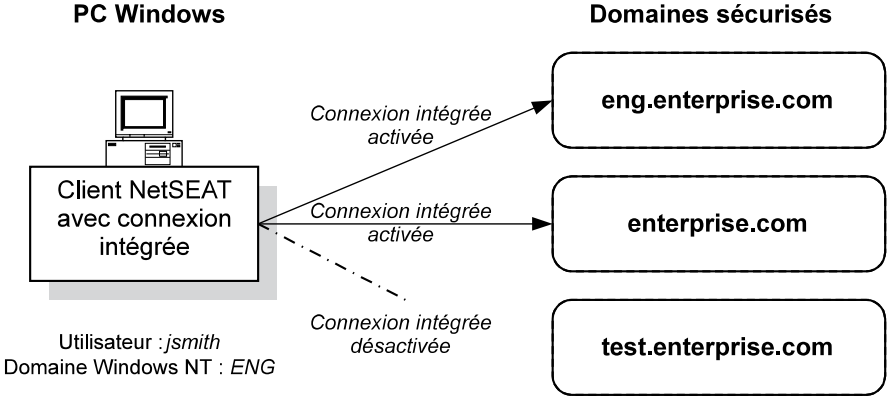
Exemple de configuration avec connexion intégrée

Un ingénieur nommé Jean Simon se connecte habituellement au domaine Windows NT nommé ENG, sous le nom d'utilisateur jsimon. Il accède à plusieurs domaines sécurisés de la manière suivante :

Nom du domaine sécurisé	Compte utilisateur	Description du domaine sécurisé
eng.entreprise.com	jsimon	Domaine sécurisé de la division ingénierie.
entreprise.com	ENG/jsimon	Domaine sécurisé de l'entreprise.
test.entreprise.com	test_user	Petit domaine sécurisé exclusivement utilisé pour des opérations d'évaluation. La cellule de test ne possède pas de registre des utilisateurs. Ces derniers y accèdent sous l'ID générique test_user.

Jean Simon configure la connexion intégrée pour chaque domaine sécurisé à l'aide de l'utilitaire de configuration de NetSEAT :

Domaine sécurisé	Configuration de la connexion intégrée
eng.entreprise.com	Connexion intégrée activée et configurée de manière à mapper le nom d'utilisateur Windows NT jsimon au nom d'utilisateur du domaine sécurisé jsimon, et à connecter automatiquement cet utilisateur au domaine eng.entreprise.com.
entreprise.com	Connexion intégrée activée et configurée de manière à mapper le nom d'utilisateur Windows NT jsimon au nom d'utilisateur du domaine sécurisé ENG/jsimon, et à connecter automatiquement cet utilisateur au domaine entreprise.com.
test.entreprise.com	Connexion intégrée désactivée puisque l'utilisateur jsimon doit se connecter manuellement à cette cellule sous le nom d'utilisateur test_user.



Configuration de la connexion intégrée

Pour configurer la connexion intégrée :

1. Exécutez l'utilitaire de configuration de NetSEAT.

   L'onglet **Domaines sécurisés** apparaît.
2. Sélectionnez le domaine sécurisé pour lequel vous voulez configurer la connexion intégrée.
3. Cliquez sur **Edition**.

La fenêtre Propriétés du domaine sécurisé apparaît à l'écran.

4. Sélectionnez l'une des options proposées pour le **Support de connexion intégrée**.

   Si l'option **Support de connexion intégrée** est oblitérée, cela signifie que vous n'avez pas installé le support de connexion intégrée et que ne pouvez, par conséquent, pas activer la connexion intégrée pour ce domaine sécurisé.

   - Sélectionnez **Désactivé** pour désactiver le support de connexion intégrée pour ce domaine sécurisé.
   - Sélectionnez **Activé—Le nom d'utilisateur DCE est le nom d'utilisateur Windows**, si le nom d'utilisateur utilisé dans ce domaine sécurisé est identique au nom d'utilisateur Windows.
   - Sélectionnez **Activé—Le nom d'utilisateur DCE est le nom de domaine/utilisateur Windows**, si le nom d'utilisateur utilisé dans ce domaine sécurisé comprend le nom du domaine Windows.

5. Cliquez sur **OK**.

   L'onglet **Domaines sécurisés** apparaît.

6. Cliquez sur **OK**.

Configuration du mode de notification de la connexion intégrée

Votre mot de passe de domaine sécurisé peut être différent de votre mot de passe de domaine Windows NT. Dans ce cas, l'entrée du registre Windows détermine si les tentatives de connexion au domaine sécurisé échouent avec notification ou sans (mode silencieux). Le système peut également vous demander votre mot de passe actuel pour accéder au domaine sécurisé (mode interactif). En mode silencieux, Policy Director connecte l'utilisateur au domaine Windows NT mais pas au domaine sécurisé. En mode interactif, vous pouvez synchroniser votre mot de passe de domaine sécurisé avec votre mot de passe Windows.

Pour changer de mode de notification, éditez l'entrée du registre Windows suivante à l'aide de l'éditeur du registre :

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetSEAT\Parameters
```

Modifiez la valeur qui suit :

```
InfoLevel:
0x00000001 (1)
```

InfoLevel peut prendre l'une des valeurs suivantes :

Valeur de registre	Mode	Description
0	silencieux	Les tentatives de connexion ne sont jamais notifiées à l'utilisateur, qu'elles aboutissent ou non.
1	Interactif	Les tentatives de connexion ne sont notifiées à l'utilisateur qu'en cas d'échec. Un message demande l'action à entreprendre.
2	Commentaire	Les tentatives de connexion sont systématiquement notifiées à l'utilisateur, qu'elles aboutissent ou non.

Configuration de la connexion avancée (intégration de la clé PKI)

Cette tâche de configuration est facultative et ne s'applique qu'aux clients NetSEAT utilisant le type de tunnel GSS.

Vous pouvez configurer NetSEAT de manière à combiner la clé de connexion PKI (Public Key Infrastructure) d'un utilisateur et sa clé de connexion NetSEAT (Kerberos).

Par défaut, l'intégration de la clé PKI est désactivée. Vous devez exécuter l'utilitaire de configuration de NetSEAT pour l'activer. L'activation ou la désactivation de la connexion par clé PKI se fait séparément pour chaque domaine sécurisé dont le client NetSEAT est membre.

Versions PKI prise en charge

NetSEAT prend en charge l'intégration d'un ID de connexion utilisateur avec la version Entrust 4.0 uniquement.

Remarque : Le client Entrust Version 4.0 doit être installé avant de configurer la connexion PKI pour NetSEAT.

Utilisation de l'utilitaire Connexion à NetSEAT

L'utilitaire **Connexion à NetSEAT**, que l'on appelle à partir du menu **Démarrage** de Windows, affiche une case à cocher **ID PKI** au moment de la connexion. Cette case à cocher affiche le paramètre de connexion avancée configuré pour le domaine sécurisé courant.

Utilisation de la case à cocher ID PKI

Au cours de la connexion à NetSEAT, un utilisateur peut utiliser la case à cocher **ID PKI** pour modifier la configuration de la clé PKI, uniquement pour la session en cours. Cette faculté peut servir si vous avez sélectionné **ID PKI avec renvoi sur l'ID DCE** pendant la configuration. Vous pouvez ainsi remplacer la tentative de connexion PKI par une tentative de connexion DCE. Dans cette situation, vous devez invalider la sélection de la case à cocher **ID PKI** pour obtenir une connexion DCE.

Si vous avez choisi la case à cocher **ID PKI uniquement** pendant la configuration, annuler la sélection de la case **ID PKI** n'a aucun effet.

Si vous avez choisi la case à cocher **ID DCE uniquement** pendant la configuration, sélectionner la case **ID PKI** déclenche l'affichage d'un message d'erreur.

Connexion par l'icône NetSEAT

Vous pouvez utiliser l'icône **NetSEAT** pour établir une connexion avec NetSEAT. Sélectionnez le domaine auquel vous voulez accéder dans la liste déroulante. Si la connexion par clé PKI a été configurée, l'invite de connexion Entrust apparaît à l'écran.

Si la connexion par clé PKI échoue et que vous avez sélectionné **ID PKI avec renvoi sur l'ID DCE**, Policy Director vous demande d'établir une connexion à partir du DCE.

Configuration de la connexion avancée

Pour intégrer la connexion par clé PKI et la connexion à NetSEAT :

1. Exécutez l'utilitaire de configuration de NetSEAT.

   L'onglet **Domaines sécurisés** apparaît.
2. Sélectionnez le domaine sécurisé pour lequel vous voulez configurer la connexion par clé PKI.
3. Cliquez sur **Edition**.

La boîte de dialogue Nouveau domaine sécurisé apparaît.

4. Cliquez sur **Configuration**.

   La fenêtre Propriétés du domaine sécurisé apparaît à l'écran.

5. Dans la zone Connexion avancée, sélectionnez l'une des options de la liste déroulante.
   - Sélectionnez **ID DCE uniquement** pour autoriser l'utilisateur à se connecter au domaine sécurisé de Policy Director avec un nom d'utilisateur et un mot de passe (clé Kerberos).
   - Sélectionnez **ID PKI avec renvoi sur l'ID DCE** pour autoriser l'utilisateur à tenter une connexion avec sa clé PKI. Si la tentative de connexion échoue, NetSEAT demande à l'utilisateur d'entrer un nom d'utilisateur et un mot de passe pour établir une connexion DCE.
   - Sélectionnez **ID PKI uniquement** pour obliger l'utilisateur à se connecter avec un certificat X.509.

6. Cliquez sur **OK**.

   La boîte de dialogue Nouveau domaine sécurisé apparaît.

7. Cliquez sur **OK**.

   L'onglet **Domaines sécurisés** réapparaît.

Définition du retardement maximum

Cette tâche de configuration est facultative et ne s'applique qu'aux clients NetSEAT utilisant la console de gestion de Policy Director et les serveurs Windows NT pour Policy Director.

Configuré pour utiliser la transmission par tunnel GSS, NetSEAT fait appel à des services horaires distants. Vous pouvez configurer l'écart maximal autorisé entre l'heure du domaine sécurisé et l'horloge du système NetSEAT. Vous pouvez aussi accepter la valeur par défaut (15 minutes).

Pour définir le retardement maximum :

1. Cliquez sur l'onglet **Général**.
2. Entrez une valeur dans le champ **Retardement maximum**.
3. Cliquez sur **OK** ou sur **Appliquer**.

Interdiction d'accès à des ressources de réseau

Cette tâche de configuration est facultative et ne s'applique qu'aux clients NetSEAT utilisant le type de tunnel GSS ou SSL.

Vous pouvez interdire à un utilisateur toute possibilité d'envoyer des requêtes non sécurisées TELNET, RLOGIN ou HTTP à partir d'un poste de travail. Configurez le client NetSEAT de manière à interdire ou limiter l'accès à ce type de service de réseau. Le poste de travail du client devra utiliser exclusivement les canaux de communication de Policy Director sécurisés et codés pour les transactions de réseau.

Cette fonction est désactivée par défaut. Vous ne devez l'activer que pour les réseaux spécialisés hautement sécurisés.

Pour interdire l'accès aux services de réseau non protégés :

1. Sélectionnez l'onglet **Général**.

2. Sélectionnez la case à cocher **Interdire l'accès aux services de réseau non protégés**.
3. Cliquez sur **OK** ou sur **Appliquer**.

Configuration d'un serveur relais SSL

Cette tâche de configuration est facultative et ne s'applique qu'aux clients NetSEAT utilisant le type de tunnel SSL.

Lorsque les requêtes du client NetSEAT doivent transiter par le serveur relais SSL de votre réseau, vous pouvez configurer le client NetSEAT de manière à ce qu'il utilise ce serveur relais. La case à cocher **Activer serveur relais** de l'onglet **Général** permet d'activer le serveur relais SSL afin que tous les serveurs NetSEAL puissent l'utiliser.

Si vous désélectionnez cette case à cocher, aucun des serveurs NetSEAL ajoutés à la configuration de NetSEAT ne pourra accéder au serveur relais.

Pour spécifier un serveur relais SSL :

1. Cliquez sur l'onglet **Général**.
2. Si vous le désirez, modifiez la valeur du champ **Retardement maximum**. La valeur par défaut est de 15 minutes.
3. Prenez soin de ne pas sélectionner la case à cocher **Interdire l'accès aux services de réseau non protégés**.
4. Sélectionnez la case à cocher **Activer serveur relais**.
5. Entrez le nom de la machine dans le champ **Nom de la machine du serveur relais**.
6. Entrez le numéro de port du serveur relais dans le champ **Port du serveur relais**.
7. Cliquez sur **OK** ou sur **Appliquer**.

Utilisation des utilitaires de sécurité de NetSEAT

Le client NetSEAT propose tous les utilitaires de service de sécurité du DCE que l'on trouve habituellement dans une solution d'environnement informatique partagé. L'architecture unique de NetSEAT permet d'étendre les fonctions standard pour chacun de ces utilitaires : **klist**, **kdestroy** et **dce_login**.

klist

La commande **klist** affiche l'utilisateur primaire (le principal) et les droits d'accès contenus dans le cache des droits d'accès par défaut. Si vous lui ajoutez l'option **-c**, cette commande affichera l'utilisateur et les droits d'accès contenus dans le cache dont vous aurez indiqué le nom.

NetSEAT exécute les options standard de la commande **klist** et y ajoute des options avancées.

Les options standard sont les suivantes :

Option	Description
-c nom_cache	Affiche le contenu du cache désigné par nom_cache au lieu de celui du cache par défaut.

-e	Affiche en plus les droits d'accès arrivés à expiration. Sans cette option, seuls les droits d'accès actifs sont affichés.
-f	Affiche les valeurs des options des droits d'accès.

Les options avancées sont les suivantes :

Option	Description
-C nom_cellule	Affiche l'utilisateur primaire et les droits d'accès détenus par lui dans la cellule du DCE désignée par nom_cellule.
-m	Affiche l'utilisateur primaire et les droits d'accès détenus par lui dans toutes les cellules du DCE pour lesquelles il possède un contexte de connexion.
-s	Affiche la synthèse de toutes les cellules auxquelles l'utilisateur est connecté ainsi que son nom de connexion pour chacune de ces cellules.

kdestroy

La commande **kdestroy** supprime le contexte de connexion d'un utilisateur ainsi que ses droits d'accès. Tant que Policy Director n'a pas rétabli ses droits d'accès, l'utilisateur et tous les processus qu'il crée sont limités à l'accès non authentifié.

Le client NetSEAT gère les options standard de la commande **kdestroy** et lui ajoute des options avancées.

Les options standard sont les suivantes :

Option	Description
-c nom_cache	Supprime le contexte de connexion et les droits d'accès contenus dans le cache désigné par nom_cache au lieu de ceux contenus dans le cache par défaut.

Les options avancées sont les suivantes :

Option	Description
-C nom_cellule	Supprime le contexte de connexion et les droits d'accès associés pour la cellule désignée par nom_cellule.
-m	Supprime le contexte de connexion et les droits d'accès de l'utilisateur pour toutes les cellules dans lesquelles il possède un contexte de connexion.

dce_login

La commande **dce_login** valide l'identité d'un utilisateur, extrait ses droits d'accès au réseau et établit un contexte de connexion au DCE.

L'utilisateur doit fournir son nom de principal (nom d'utilisateur) et son mot de passe. S'il ne les entre pas comme arguments de ligne de commande, la commande **dce_login** affiche un message qui les demande.

Le client NetSEAT gère les options standard suivantes pour la commande **dce_login** :

Option	Description

-exec chaîne_commande	Exécute la commande spécifiée par chaîne_commande une fois la connexion établie. Si l'argument chaîne_commande ne précise pas de nom de chemin absolu, le préfixe de chemin est obtenu à l'issue d'une analyse des répertoires conduite d'après la valeur de la variable PATH.
-k fichier_clés	Extrait le nom de l'utilisateur (principal) et son mot de passe à partir du fichier de clés désigné par fichier_clés.
-r	Régénère le contexte de connexion DCE de l'utilisateur avant l'expiration de ses droits d'accès.

Policy Director prend en charge les options avancées suivantes pour la commande dce_login :

Option	Description
-C nom_cellule	Demande l'établissement d'une connexion avec la cellule désignée par nom_cellule au lieu de la cellule par défaut.

Remarque : Le client NetSEAT ne gère pas l'option **dce_login -c**.

Résolution des incidents avec netseat_ping

L'utilitaire **netseat_ping** du client NetSEAT permet d'obtenir des données d'état sur les services DCE d'une ou plusieurs cellules. Vous pouvez utiliser **netseat_ping** pour savoir si les services suivants sont disponibles :

- Services de sécurité
- Services horaires
- Services de répertoire de cellules
- Répartiteur des services de répertoire

Pour connaître l'état des services existant dans toutes les cellules où l'utilisateur possède un contexte de connexion, tapez :

```
netseat_ping
```

Par exemple, si vous configurez un client NetSEAT comme membre de la cellule `redback`, la sortie obtenue sera celle-ci :

```
/.../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[ ] est disponible (v3.0)
                    ncacn_ip_udp:redback[ ] est disponible (v3.0)
```

Policy Director prend en charge les options suivantes de **netseat_ping** :

Option	Description
-C nom_cellule	Affiche la liste exhaustive des liaisons définies par l'utilisateur entre la cellule nom_cellule et des serveurs.

-t -C nom_cellule	Affiche les liaisons définies entre la cellule nom_cellule et le serveur horaire.
-s -C nom_cellule	Affiche les liaisons définies entre la cellule nom_cellule et le serveur de sécurité.
-c -C nom_cellule	Affiche les liaisons définies entre la cellule nom_cellule et le serveur SRC.
-d -C nom_cellule	Affiche les liaisons définies entre la cellule nom_cellule et le serveur RSR.

Si la cellule héberge plusieurs instances du serveur de sécurité, du serveur horaire, du serveur SRC ou du serveur RSR, **netseat_ping** tente de contacter chacune d'elles.

Chapitre 21. NetSEAT - Répartiteur des services de répertoire (RSR)

Ce chapitre propose une présentation générale du Répartiteur des services de répertoire (RSR) et décrit comment personnaliser sa configuration en fonction de votre environnement.

Ce chapitre comprend les sections suivantes :

Présentation générale du répartiteur des services de répertoire (RSR)

Le client Policy Director NetSEAT peut utiliser le répartiteur des services de répertoire pour suppléer l'interface ISN RPC. Le RSR fonctionne comme un serveur de services de répertoire de cellules (également appelés services d'annuaire de cellules) assimilé à un serveur tiers.

Le client NetSEAT dirige les requêtes d'emplacement de ressource et de services vers le RSR. A son tour, le répartiteur des services de répertoire contacte les services de répertoire de cellules (SRC) du domaine sécurisé afin qu'ils répondent à la requête. Ensuite, le RSR renvoie la réponse de la requête au système d'où le client NetSEAT l'avait émise.

Pendant son installation, Policy Director installe et configure automatiquement le répartiteur des services de répertoire (RSR). Le programme RSR est fourni avec Policy Director comme composant du module Serveur de gestion (IVMgr). L'utilisation du RSR ne nécessite aucune procédure particulière.

- Utilisés comme module de support pour les serveurs Policy Director et la console de gestion, les clients NetSEAT utilisent le répartiteur des services de répertoire.
- En revanche, s'ils utilisent les tunnels SSL, les clients NetSEAT n'utilisent pas le répartiteur des services de répertoire.

Le RSR est utilisable par un grand nombre de clients NetSEAT. Pour les plus grands domaines sécurisés, vous pouvez optimiser les performances en installant le RSR sur un serveur fournissant aussi des services de répertoire de cellules.

Pour procurer une accessibilité avancée et équilibrer la charge dans les très grands réseaux, un administrateur peut vouloir installer plusieurs RSR dans un même domaine sécurisé. Ces RSR peuvent s'installer et se configurer manuellement.

Option de configuration du répartiteur des services de répertoire

Le RSR peut s'exécuter comme un démon ou comme un service. Vous pouvez le configurer pour qu'il démarre automatiquement à l'amorçage du système. Dans la plupart des situations, le RSR ne nécessite pas d'administration spécifique.

Pour plus d'informations sur la définition des paramètres de configuration du RSR, reportez-vous aux sections suivantes :

- «Définition de l'emplacement du fichier journal du RSR».

Définition du numéro de port du RSR

A l'écoute d'un port, le RSR détecte les requêtes entrantes. Par défaut, il choisit ce port de manière aléatoire.

S'il le souhaite, l'administrateur peut spécifier le numéro du port d'écoute en entrant une valeur dans l'un des fichiers suivants :

UNIX : `/etc/services`

Windows : *`chemin_installation`*`\system32\drivers\etc\services`

Par exemple, pour que le RSR installé sur un système UNIX écoute le port 5000, insérez l'entrée suivante dans le fichier /etc/services :

```
dsb                5000/tcp              # Répartiteur des services de répertoire
```

Définition de l'emplacement du fichier journal du RSR

Le RSR utilise les fichiers journaux de mise en service du DCE pour consigner les messages d'information, d'erreur, d'avertissement et d'erreur fatale. Si votre DCE utilise ces messages de mise en service, le RSR consignera les siens dans un ou plusieurs de ces fichiers journaux. Les fichiers journaux de mise en service du DCE résident dans le répertoire DCELOCAL/var/svc. La variable DCELOCAL désigne le répertoire d'installation du DCE.

Un message d'information, d'erreur ou d'avertissement peut être consigné dans plusieurs fichiers. Pour choisir l'emplacement de ces fichiers, insérez des entrées dans le fichier de routage DCELOCAL/var/svc/routing.

Par exemple :

```
NOTICE:FILE:DCELOCAL/var/svc/notice
```

Vous pouvez également indiquer cet emplacement au moyen de la variable d'environnement SVC_NOTICE. La valeur de la variable d'environnement se substitue à la spécification du fichier de routage. Par exemple, pour définir une variable d'environnement UNIX afin de spécifier l'emplacement des fichiers des messages d'information, entrez la commande suivante :

```
export SVC_NOTICE=FILE:DCELOCAL/var/svc/notice
```

Exemple de ligne de commande :

Définissez la variable NOTICE dans un fichier de routage et initialisez le RSR à partir d'une ligne de commande, de la manière suivante :

```
SVC_NOTICE=FILE:DCELOCAL/var/dsb/dsb.log dsb -q -f -U cell_admin -P *****
```

Le répartiteur des services de répertoire :

- se configure et s'initialise en mode silencieux ;
- consigne tous les messages d'information dans le fichier journal DCELOCAL/var/dsb/dsb.log ;
- consigne tous les messages d'erreur, d'avertissement et d'erreur fatale selon la spécification contenue dans le fichier de routage ;
- n'affiche aucune sortie de journalisation.

Pour plus d'informations sur le format des fichiers de routage et sur l'utilisation des variables d'environnement du groupe SVC, reportez-vous aux sections relatives à la mise en service du DCE. Vous trouverez les documents suivants consacrés à l'installation et à la configuration du DCE sur le CD-ROM de IBM Policy Director - Services de sécurité, dans le répertoire /doc :

- DCE22_QuickBeginnings_AIX.pdf
- DCE22_QuickBeginnings_NT.pdf
- DCE20_InstallGuide_Solaris.pdf
- DCE20_ReleaseNotes_Solaris.pdf

Options de ligne de commande du répartiteur des services de répertoire

Le tableau suivant décrit les options de ligne de commande du répartiteur des services de répertoire :

Option	Description
-d	Exécute le RSR en avant-plan au lieu de l'initialiser comme démon UNIX ou comme service Windows NT. Cette option s'utilise essentiellement pour le débogage.
-f	Reconfigure les entrées de sécurité du DCE définies pour le RSR. Cet attribut crée le groupe Policy Director/dsb-servers (sauf s'il existe déjà), le fichier du tableau des clés et le principal (utilisateur) intraverse/dsb/default/nom_DNS-complet (l'argument nom_DNS_complet désigne le système hébergeant le RSR). Cette option est utilisée à l'initialisation du RSR. Elle peut être appelée plusieurs fois sans qu'il soit nécessaire de supprimer préalablement l'entrée du principal, l'entrée du groupe ou les fichiers de clés.
-h	Message relatif à la syntaxe de la ligne de commande.
-q	Envoie la sortie vers un fichier journal au lieu de la sortie standard ou de la sortie d'erreur standard. Les messages ne s'afficheront pas à l'écran.
-r	Annule la configuration du RSR. Cette option supprime les entrées de sécurité du DCE définies pour le RSR (revoir l'option **-f**). L'attribut **-r** peut être utilisé seul ou avec **-q**. Aucun autre attribut de ligne de commande ne peut être utilisé avec **-r**.
-t	Indique le nombre d'unités d'exécution de serveur que le RSR peut utiliser. Cette valeur détermine le nombre de requêtes de clients pouvant être traitées simultanément.
-P mot_de_passe	Indique le mot de passe de connexion du principal (utilisateur) au DCE. Exclusivement utilisé avec l'attribut **-U**.

-U nom_principal	Nom de principal (utilisateur) de DCE utilisé pour la configuration du RSR. Utilisez cette option pour désigner tout utilisateur ayant reçu l'autorité requise pour créer les entrées de sécurité du RSR (revoir l'option **-f**).
-b	Option pour Microsoft Windows uniquement—Indique que le fichier de l'exécutable du RSR est un fichier binaire. Utilisez cette option si le RSR est installé dans un emplacement autre que celui prévu par défaut. Cette option enregistre l'emplacement du RSR dans le registre Microsoft Windows NT. Windows NT utilise cette information lors de la configuration du RSR comme service Windows NT.
-v	Option pour Microsoft Windows uniquement—Affiche la version du RSR et un message du fabricant du DCE.

Annexe A. Administration de Policy Director avec l'utilitaire ivadmin

L'utilitaire de ligne de commande **ivadmin** est un équivalent de la console de gestion qui permet de conduire les tâches d'administration de Policy Director.

Ce chapitre comprend les sections suivantes :

- «Présentation de l'utilitaire ivadmin» (cette page).
- «Utilisation des commandes de ivadmin».

Présentation de l'utilitaire ivadmin

L'utilitaire de ligne de commande **ivadmin** est l'équivalent de la console de gestion. Les administrateurs désireux d'automatiser certaines fonctions peuvent le faire en créant des scripts utilisant les commandes d'**ivadmin**.

Plusieurs des commandes **ivadmin** exécutent des fonctions également accessibles par la console de gestion. Toutefois, **ivadmin** gère, en plus, des fonctions de gestion avancées que la console de gestion ne propose pas. Le module IVBase, installé sur tout système contenant Policy Director, installe également cet utilitaire d'une manière automatique.

Démarrage de l'utilitaire ivadmin

Pour démarrer l'utilitaire **ivadmin**, connectez-vous au domaine sécurisé via la commande **dce_login**. Tapez ensuite :

UNIX : `# ivadmin`

Windows : `ivadmin`

L'invite de la commande **ivadmin** apparaît :

```
ivadmin>
```

Tapez les commandes, options et arguments appropriés à la suite de cette invite. Reportez-vous aux tableaux des commandes de la section «Utilisation des commandes de ivadmin».

Par exemple, pour afficher les messages d'aide de l'utilitaire **ivadmin**, tapez :

```
ivadmin> help
```

Sortie de l'utilitaire ivadmin

Pour quitter l'utilitaire ivadmin et revenir à l'invite de commande, tapez la commande :

```
ivadmin> exit
```

Utilisation des commandes de ivadmin

Les commandes de l'utilitaire **ivadmin** sont les suivantes :

- «Commandes de serveur» à la page 278
- «Commande de gestion des objets» à la page 279
- «Commandes d'action» à la page 280

Remarque : Toutes les commandes d'**ivadmin** doivent être saisies sur une seule ligne, comme une unique commande (même si certaines peuvent apparaître sur deux lignes dans ce manuel).

Commandes de serveur

Les commandes **ivadmin server** gèrent des fonctions que la console de gestion n'offre pas actuellement :

Commande	Description
server flush_logs nom_serveur	
	Transfère les fichiers journaux des serveurs WebSEAL de la mémoire vers le disque dur. Permet le suivi immédiat des événements des serveurs.
server list	
	Affiche la liste des serveurs configurés.
server resume nom_serveur	
	Relance un serveur WebSEAL suspendu.
server show nom_serveur	
	Affiche les propriétés du serveur indiqué, notamment son nom, sa description, son nom d'hôte, son emplacement NS, son principal et son adresse URL racine.
server start nom_serveur	
	Démarre le serveur indiqué. Exécute les processus secmgrd (NetSEAL et WebSEAL) et ivacld.
server stop nom_serveur	
	Arrête le serveur indiqué. Arrête les processus secmgrd (NetSEAL et WebSEAL) et ivacld.
server suspend nom_serveur	
	Suspend le serveur WebSEAL indiqué. Cette commande s'utilise surtout à l'occasion des opérations de maintenance des serveurs.

Les commandes **ivadmin server** suivantes étendent les fonctions de la console de gestion :

Commande	Description
server delete /ExternAuthzn/nom_serveur	
	Supprime un serveur d'autorisation externe (exclusivement). Cette commande est souvent utilisée de manière non interactive par les programmes de désinstallation. **Remarque :** N'utilisez pas cette commande pour supprimer d'autres serveurs.

server modify nom_serveur **baseurl** point_montage	
	Spécifie la branche de l'espace des LCA que le serveur désigné doit utiliser. Cette commande s'utilise pour les serveurs WebSEAL dupliqués. Elle désigne le point de montage de la branche désignée où commence la branche maîtresse utilisée par la console de gestion pour l'administration des listes de contrôle d'accès. Les LCA contenues dans cette branche sont appliquées à toutes les instances de serveur montées sur ce point de jonction ; ces instances de serveur répercutent instantanément les modifications des listes de contrôle d'accès. Notez que le point de montage se situe par rapport à l'objet conteneur /WebSEAL et doit résider dans le répertoire WebSEAL (et non pas dans l'un de ses sous-répertoires).
server register externauth nom_serveur emplacement_ns principal_serveur car_action nom_action	
	Enregistre l'existence d'un serveur d'autorisation externe. Utilisez cette commande pour notifier au service d'autorisation de Policy Director que ce serveur d'autorisation externe existe et qu'il doit être consulté pour la détermination des autorisations associées aux objets protégés.
server status nom_serveur	
	Détermine si le serveur est actif ou arrêté et si sa base de données des LCA a été mise à jour ou non.

Remarques :

Pour afficher les propriétés du serveur WebSEAL installé sur la machine `chevelle`, tapez :

```
ivadmin> server show /WebSEAL/chevelle
Type : WebSEAL Server
Nom : /WebSEAL/chevelle
Description : chevelle
Nom d'hôte : chevelle
Emplacement NS : /.:/subsys/intraverse/secmgr/server/chevelle
Principal : secmgr/chevelle Root URL: /chevelle
```

Notez que vous devez entrer l'argument nom_serveur en respectant le format exact de la sortie de la commande **ivadmin server list**.

Par exemple :

```
ivadmin> server list
         /WebSEAL/chevelle
         /NetSEAL/chevelle
         /ExternAuthzn/timechecker
```

Commande de gestion des objets

Les commandes **ivadmin object** suivantes correspondent aux taches de gestion du panneau Espace objets de la console de gestion :

Commande	Description
object list nom_répertoire	
	Affiche la liste des objets contenus dans le répertoire indiqué, avec le nom des LCA associées à chacun d'eux. Notez que cette commande n'explore pas l'arborescence au delà de ce répertoire.
object show nom_objet	

	Affiche les caractéristiques de l'objet désigné par nom_objet, ainsi que le nom des LCA qui lui sont attachées. Faute de liste de contrôle d'accès définie sur cet objet, la phrase `Aucune LCA` apparaît.

Commandes d'action

Utilisez les commandes **ivadmin action** suivantes pour définir des autorisations supplémentaires sur la console de gestion.

Par exemple, utilisez les commandes **ivadmin action** pour ajouter une action d'autorisation externe (un droit personnalisé) à la liste des droits de LCA disponibles.

Les commandes **ivadmin action** gèrent des fonctions que la console de gestion n'offre pas actuellement :

Commande	Description
action create nom description type_action	
	Définit une nouvelle action d'autorisation dans Policy Director. Cette commande crée un nouveau code de droit de LCA pour représenter cette action dans la console de gestion. L'argument nom désigne le caractère symbolisant ce nouveau droit. L'argument description correspond à l'étiquette de la nouvelle case à cocher qui apparaîtra dans la console de gestion. L'argument type_action indique l'étiquette de la catégorie d'action qui s'affichera dans la console de gestion. Exemple : `ivadmin> action create k time Ext-Authzn`
action delete nom	
	Supprime une action d'autorisation initialement créée par la commande **action create**. Exemple : `ivadmin> action delete k`
action list	

	Affiche la liste des actions de LCA existantes dans le format suivant : nom
	d'autorisation description type d'action
	
	Exemple :
	`ivadmin> action list`
	
	La sortie ressemble à ceci :
	`r read WebSEAL`
	`...`

Commandes de gestion des LCA

Les commandes **ivadmin acl** suivantes correspondent aux taches de gestion du panneau **LCA** de la console de gestion :

Commande	Description
acl attach nom_objet nom_lca	

	Attache un modèle de LCA à un objet.
acl create nom_lca	
	Crée un modèle de LCA dans une base de données de modèles de LCA. Notez que cette commande ne crée pas d'entrées de LCA.
acl delete nom_lca	
	Supprime un modèle de LCA dans une base de données de modèles de LCA.
acl detach nom_objet	
	Détache le modèle de LCA courant de l'objet désigné. Notez que cette commande ne supprime le modèle de LCA de la base de données des modèles de LCA.
acl find nom_lca	
	Recherche et affiche tous les objets auxquels le modèle de LCA indiqué est appliqué.
acl list	
	Affiche la liste des modèles de LCA contenus dans une base de données de modèles de LCA.
acl modify nom_lca **description** description	
	Permet de créer ou de modifier les champs de la description du modèle de LCA indiqué. Cette description apparaît notamment dans la zone de définition des LCA du panneau LCA de la console de gestion.
acl modify nom_lca **remove user** nom_utilisateur	
	Supprime une entrée de LCA du type user dans la définition du modèle de LCA indiqué.
acl modify nom_lca **remove group** nom_groupe	
	Supprime une entrée de LCA du type group dans la définition du modèle de LCA indiqué.
acl modify nom_lca **remove any-other**	
	Supprime l'entrée de LCA du type any-authenticated dans la définition du modèle de LCA indiqué.
acl modify nom_lca **remove unauthenticated**	
	Supprime l'entrée de LCA du type unauthenticated dans la définition du modèle de LCA indiqué.
acl modify nom_lca **set user** nom_utilisateur autorisations	
	Permet de créer ou de modifier une entrée de LCA de type user (`pubs`) dans la définition du modèle de LCA indiqué (les autorisations désignées par l'argument (autorisations sont `bPTr`). Exemple : `ivadmin> acl modify pubs set user pierre bPTr`
acl modify nom_lca **set group** nom_groupe autorisations	
	Permet de créer ou de modifier une entrée de LCA de type group dans la définition du modèle de LCA indiqué. Exemple : `ivadmin> acl modify pubs set group ventes Tr`
acl modify nom_lca **set any-other** autorisations	

	Permet de créer ou de modifier une entrée de LCA du type any-authenticated (`pubs`) dans la définition du modèle de LCA indiqué. Exemple : `ivadmin> acl modify pubs set any-other r`
acl modify nom_lca **set unauthenticated** autorisations	
	Permet de créer ou de modifier une entrée de LCA du type unauthenticated dans la définition du modèle de LCA indiqué. Exemple : `ivadmin> acl modify pubs set unauthenticated r`
acl show nom_lca	
	Affiche l'ensemble des entrées composant la définition du modèle de LCA indiqué. `ivadmin> acl show pubs`

Commandes NetSEAL

L'utilitaire **ivadmin** permet de conduire les tâches d'administration suivantes sur NetSEAL :

- «Gestion des réseaux protégés».
- «Gestion des jonctions NetSEAL».
- «Gestion des ports protégés» à la page 283.
- «Gestion des alias des ports protégés» à la page 284.

Gestion des réseaux protégés

Les réseaux peuvent être considérés comme des serveurs non protégés par Policy Director mais couverts par NetSEAL. Utilisez les commandes **ivadmin netseal** pour ajouter, supprimer et afficher les réseaux protégés.

Commande	Description
netseal network add réseau masque_réseau **[**alias_réseau**]**	
	Crée un réseau protégé par NetSEAL. Les arguments réseau et masque_réseau indiquent respectivement un code et un masque d'adresse de réseau IP standard. L'argument optionnel alias_réseau peut être renseigné pour mieux identifier ce réseau. A défaut d'alias, le réseau doit être identifié par un code et un masque d'adresse de réseau. Un message d'erreur apparaît si le réseau spécifié existe déjà.
netseal network delete id_réseau	
	Supprime du système le réseau spécifié. L'argument id_réseau admet les valeurs suivantes : • Un couple code/masque de réseau ; • Un alias de réseau. Un message d'erreur s'affiche si le réseau ne figure pas dans la base de données.
netseal network list	
	Affiche tous les réseaux définis dans la base de données (code, masque et alias du réseau).

Gestion des jonctions NetSEAL

Les jonctions NetSEAL déterminent le sens des communications transitant par un serveur Policy Director. Vous pouvez créer des jonctions entre deux serveurs Policy

Director ou entre un serveur Policy Director et un réseau. Utilisez un tunnel GSS pour sécuriser les communications transitant par une jonction entre deux serveurs Policy Director.

Utilisez les commandes **ivadmin netseal junction** pour ajouter, supprimer et afficher les jonctions NetSEAL.

Commande	Description
netseal junction add nom_hôte destination	
	Crée une jonction entre un serveur NetSEAL et une destination définie. L'argument nom_hôte désigne le serveur NetSEAL (sans le nom de domaine). L'argument destination admet les valeurs suivantes : • Un serveur Policy Director ; • Un couple code/masque de réseau ; • Un alias de réseau. Un message d'erreur s'affiche si la jonction existe déjà, si le système hôte n'existe pas ou si la destination n'existe pas.
netseal junction delete nom_hôte **destination**	
	Supprime une jonction entre un serveur NetSEAL et une destination définie. L'argument nom_hôte désigne le serveur NetSEAL (sans le nom de domaine). L'argument destination admet les valeurs suivantes : • Un serveur Policy Director ; • Un couple code/masque de réseau ; • Un alias de réseau. Un message d'erreur s'affiche si la jonction spécifiée n'existe pas. La commande n'a aucun effet sur la connexion active dans ce cas.
netseal junction list nom_hôte	
	Affiche toutes les jonctions NetSEAL associées au serveur NetSEAL spécifié.

Gestion des ports protégés

Le serveur NetSEAL de Policy Director fournit des services de sécurité à certains ports, hôtes et réseaux. Par exemple, vous pouvez configurer le serveur NetSEAL de manière à sécuriser le trafic TELNET sur un port déterminé.

Utilisez les commandes **ivadmin netseal port** pour ajouter, supprimer et afficher les ports protégés. Vous pouvez spécifier des ports de serveurs Policy Director ou des ports de réseaux.

Commande	Description
netseal port add destination id_port	
	Cette commande protège les connexions établies avec la destination indiquée sur le port désigné par l'argument id_port. L'argument destination admet les valeurs suivantes : • Un serveur Policy Director ; • Un couple code/masque de réseau ; • Un alias de réseau. L'argument id_port admet les valeurs suivantes : • Un numéro de port ; • Une série de ports ; • Un alias de port. Un message d'erreur s'affiche si le port est déjà protégé, si le serveur n'existe pas ou si l'alias de port n'existe pas.

netseal port delete destination id_port	
	Cette commande interrompt la protection des connexions établies avec la destination indiquée sur le port désigné. L'argument destination admet les valeurs suivantes : • Un serveur Policy Director ; • Un couple code/masque de réseau ; • Un alias de réseau. L'argument id_port admet les valeurs suivantes : • Un numéro de port ; • Une série de ports ; • Un alias de port. Un message d'erreur s'affiche si le port n'est pas protégé, si le serveur n'existe pas ou si l'alias de port n'existe pas.
netseal port list destination	
	Cette commande affiche la liste des ports de la destination indiquée. L'argument destination admet les valeurs suivantes : • Un serveur Policy Director ; • Un couple code/masque de réseau ; • Un alias de réseau. Un message d'erreur s'affiche si le serveur n'existe pas.

Remarque : Une **série de ports** s'exprime sous la forme de deux numéros de port séparés par un tiret (par exemple, 22-88).

Gestion des alias des ports protégés

Utilisez les commandes **ivadmin port-alias** pour ajouter, supprimer et afficher les alias des ports. Vous pouvez utiliser les alias de port pour mieux identifier les séries de ports avec demande d'alerte.

Commande	**Description**
netseal port-alias add port alias_port	
	Cette commande crée un alias pour le port indiqué. L'argument port admet les valeurs suivantes : • Un numéro de port ; • Une série de ports. Un message d'erreur s'affiche si le port ou la série de ports possède déjà un nom d'alias.
netseal port-alias delete id_port	
	Supprime du système l'alias du port spécifié par l'argument id_port. L'argument id_port admet les valeurs suivantes : • Un numéro de port ; • Une série de ports ; • Un alias de port. L'argument id_port peut désigner un port, une série de ports ou un alias de port. Un message d'erreur s'affiche si l'alias de port ne figure pas dans la base de données.
netseal port-alias list	
	Affiche la liste des alias de port définis dans la base de données.

Commandes de gestion de la configuration

Les commandes de gestion de configuration **ivadmin admin** affichent des informations sur le serveur.

Commande	Description
admin show configuration	

	Indique si le registre des utilisateurs est contenu dans le système LDAP ou dans le DCE.
	
	Exemple :
	`ivadmin> admin show configuration`
	
	La sortie ressemble à ceci :
	`LDAP: TRUE`
	`SECAUTHORITY: Default`
	`GSO: TRUE`

Commandes de gestion des utilisateurs

Les commandes **ivadmin user** suivantes correspondent aux taches de gestion du panneau **Utilisateurs** de la console de gestion : Cette série de commandes de gestion permet de contrôler les entrées définissant les utilisateurs dans le registre LDAP par défaut.

Un simple utilisateur est un utilisateur de Policy Director. Un utilisateur GSO est un utilisateur de Policy Director pouvant, de surcroît, utiliser des ressources Web telles que des serveurs Web.

Commande	Description
user create [-gsouser] nom_utilisateur dn cn sn mdp	

	Cette commande crée un nouveau compte d'utilisateur Policy Director (secUser) dans le registre des utilisateurs LDAP. Le nom distinctif (DN) de cet utilisateur ne doit pas déjà exister dans la base de données du registre LDAP par défaut.
	
	L'argument **-gsouser** est facultatif. Les commandes optionnelles doivent être précédées d'un tiret (-). Si vous spécifiez l'argument -gsouser, l'utilisateur créé devient aussi un utilisateur GSO.
	
	L'argument nom_utilisateur définit le nom de l'utilisateur créé. Ce nom doit être unique.
	
	L'argument dn indique le nom distinctif (DN) affecté à l'utilisateur créé dans le registre LDAP (par exemple, `cn=Diana Lucas,ou=Arles,o=Chaussons SA,c=FR`). Ce DN doit être unique.
	
	L'argument cn indique le nom commun (CN) affecté à l'utilisateur créé (par exemple, `Diana Lucas`).
	
	L'argument sn indique le nom d'usage (SN) affecté à l'utilisateur créé (par exemple, `Lucas`).
	
	L'argument mdp correspond au mot de passe défini pour ce nouvel utilisateur. Les mots de passe doivent respecter les règles de format définies par l'administrateur de Policy Director (par exemple `monmotdepasse`).
	
	Exemple :
	`ivadmin> user create -gsouser dlucas`
	`cn=Diana Lucas,ou=Arles,o=Chaussons SA,c=FR`
	`"Diana Lucas" Lucas` *`monmotdepasse`*
	
	Pour que le compte utilisateur soit tout-à-fait opérationnel, vous devez activer l'utilisateur manuellement en modifiant ses propriétés. Vous devez notamment associer l'attribut account-valid à la valeur "yes".
	
	Pour lui ajouter une description, utilisez la commande **ivadmin modify user** et modifiez les données de son compte comme il convient.

user import [-gsouser] nom_utilisateur dn	

	Actualise les données d'un utilisateur dont le DN existe déjà dans la base de données du registre LDAP par défaut, à partir d'informations de Policy Director, pour en faire un membre du domaine sécurisé.
	
	Exemple :
	`ivadmin> user import -gsouser mlucaser`
	`cn=Michel Lucaser,ou=Arles,o=Chaussons SA,c=FR`

user modify nom_utilisateur description description	

	Ajoute aux données de l'utilisateur une description facilitant son identification.
	
	Exemple :
	`ivadmin> user modify dlucas description`
	`"Diana Lucas, Service des crédits HCUS"`

user modify nom_utilisateur password mot_de_passe	

	Remplace l'ancien mot de passe de l'utilisateur par un nouveau mot de passe. Il n'est pas demandé de confirmer ce nouveau mot de passe. Exemple : `ivadmin> user modify dlucas password` *`nouveaumotdepasse`*
user modify nom_utilisateur authentication-mechanism méthode	
	Change la méthode d'authentification utilisée. Exemple : `ivadmin> user modify dlucas authentication-mechanism dce`
user modify nom_utilisateur account-valid {yes | no}	
	Détermine si un compte est actif ou inactif. Pour activer le compte, sélectionnez "yes". Pour le désactiver, sélectionnez "no". Exemple : `ivadmin> user modify dlucas account-valid yes`
user modify nom_utilisateur password-valid {yes | no}	
	Détermine si un mot de passe est actif ou inactif. Pour activer le mot de passe, sélectionnez "yes". Pour le désactiver, sélectionnez "no". Exemple : `ivadmin> user modify dlucas password-valid no`
user modify nom_utilisateur gsouser {yes | no}	
	Détermine si l'utilisateur indiqué est aussi un utilisateur GSO ou non. Si vous voulez en faire un utilisateur GSO, sélectionnez "yes". Dans le cas contraire, sélectionnez "no". Exemple : `ivadmin> user modify dlucas gsouser no`
user delete nom_utilisateur	
	Supprime un compte utilisateur dans le registre des utilisateurs LDAP. Notez que supprimer un compte utilisateur Policy Director supprime également les données du compte utilisateur GSO rattaché, dans le registre LDAP par défaut. Exemple : `ivadmin> user delete dlucas` Tous les droits d'accès de ressource associés à un compte utilisateur supprimé sont automatiquement supprimés en même temps que ce compte.
user show nom_utilisateur	
	Affiche les caractéristiques du compte de l'utilisateur désigné. Exemple : `ivadmin> user show dlucas`
user show-dn dn	

	Affiche des informations supplémentaires sur l'utilisateur.
	
	Exemple :
	`ivadmin> user show-dn`
	`cn=Diana Lucas,ou=Arles,o=Chaussons SA,c=FR`

user show-groups nom_utilisateur	

	Affiche les groupes dont l'utilisateur indiqué est membre.
	
	Exemple :
	`ivadmin> user show-groups dlucas`
	
	La sortie ressemble à ceci :
	`ventes`
	`crédit`
	`ingénierie`

user list modèle sortie_max	

	Affiche la liste des comptes utilisateur définis, par nom d'utilisateur et selon un modèle de recherche spécifié. La liste affiche les comptes dans l'ordre de leur création.
	
	L'argument modèle permet de spécifier un critère de recherche. Pour définir ce modèle, vous pouvez utiliser une combinaison de caractères génériques et de constantes, en distinguant les majuscules et les minuscules (par exemple, `*luca*`).
	
	L'argument sortie_max détermine le nombre d'occurrences pouvant être renvoyées pour une même requête (par exemple, `2`). Ce nombre dépend également de la configuration du serveur LDAP qui permet de spécifier le nombre maximum d'occurrences pouvant être renvoyées à l'issue d'une recherche. Policy Director renvoie au moins le nombre d'occurrences défini par sortie_max et par la valeur configurée au niveau du serveur LDAP.
	
	Exemple :
	`ivadmin> user list *luca* 2`
	
	La sortie ressemble à ceci :
	`dlucas`
	`mlucaser`

user list-dn modèle sortie_max	

	Si seule une partie du DN est connue, cette commande affiche la liste des comptes utilisateur définis, par DN. La liste affiche les comptes dans l'ordre de création des noms d'utilisateur.
	
	Le caractère générique remplace la partie `cn=` du DN de l'utilisateur.
	
	La valeur de l'argument sortie_max dépend également de la configuration du serveur LDAP qui permet de spécifier le nombre maximum d'occurrences pouvant être renvoyées à l'issue d'une recherche. Policy Director renvoie au moins le nombre d'occurrences défini par sortie_max et par la valeur configurée au niveau du serveur LDAP.
	
	Exemple :
	`ivadmin> user list-dn *luca* 2`
	
	La sortie ressemble à ceci :
	`Diana Lucas,ou=Arles,o=Chaussons SA,c=FR`
	`Michel Lucaser,ou=Arles,o=Chaussons SA,c=FR`

Remarques :

Vous devez spécifier l'argument dn des commandes **user show-dn** et **user show-groups-dn** dans le format qui convient. Utilisez des doubles guillemets (″) si la valeur de l'argument dn contient des espaces.

Par exemple :

```
cn=Diana Lucas,ou=Arles,o=Chaussons SA,c=FR
```

Les commandes **user show** et **user show-dn** affichent les informations suivantes pour l'utilisateur `Diana Lucas` :

```
ID
de connexion : dlucas
DN LDAP : cn=Diana Lucas,ou=Arles,o=Chaussons SA,c=FR
CN LDAP : Diana Lucas
SN LDAP : Lucas
Description : Diana Lucas, Service des crédits HCUS
Est SecUser : vrai
Est utilisateur GSO : faux
Validation du compte : vrai
Validation du mot de passe : vrai
Méthode d'autorisation :
Par défaut : LDAP
```

Commandes de gestion des groupes

Les commandes **ivadmin group** suivantes correspondent aux taches de gestion du panneau **Groupes** de la console de gestion. Cette série de commandes de gestion contrôle les entrées de type group dans le registre du répertoire LDAP.

Un groupe rassemble des comptes d'utilisateur dotés de caractéristiques semblables. L'existence des groupes permet à l'administrateur d'indiquer un nom de groupe dans une liste de contrôle d'accès (LCA) au lieu d'y spécifier individuellement tous les utilisateurs.

Vous pouvez supprimer ou modifier n'importe quelle entrée de groupe. Vous pouvez afficher des informations sur un groupe ou sur une appartenance de groupe. En tant qu'administrateur, vous pouvez aussi afficher la liste de tous les groupes définis.

Commande	Description
group create nom_groupe dn cn	
	Crée un nouveau groupe Policy Director (SecGroup) dans le registre des utilisateurs LDAP. L'argument nom_groupe définit le nom du groupe créé. Ce nom doit être unique. L'argument dn indique le nom distinctif (DN) affecté au groupe créé dans le registre LDAP (par exemple, `cn=crédit,ou=Arles,o=Chaussons SA,c=FR`). L'argument cn indique le nom commun (CN) affecté au groupe créé (par exemple, `Crédit`). Exemple : `ivadmin> group create crédit cn=crédit,ou=Arles,o=Chaussons SA,c=FR Crédit`
group import nom_groupe dn	
	Crée un groupe Policy Director à partir de données de groupe importées depuis le registre LDAP. Ce groupe doit déjà exister dans le registre LDAP pour que l'importation de ses données, puis la création du groupe puissent avoir lieu. Le nom du groupe créé doit être unique. Exemple : `ivadmin> group import ingénierie cn=ingénierie,ou=Arles,o=Chaussons SA,c=FR`
group modify nom_groupe description description	
	Ajoute une description au groupe spécifié pour le rendre plus facilement identifiable par l'administrateur de Policy Director. Exemple : `ivadmin> group modify crédit description "Service des crédits HCUS"`
group modify nom_groupe add nom_utilisateur	
	Ajoute un nouvel utilisateur au groupe indiqué. Exemple : `ivadmin> group modify ingénierie add dlucas`
group modify nom_groupe remove nom_utilisateur	
	Supprime un utilisateur dans le groupe indiqué. Exemple : `ivadmin> group modify ingénierie remove dlucas`
group delete nom_groupe	
	Supprime un groupe et toutes les entrées de groupe qui lui sont associées. Exemple : `ivadmin> group delete ingénierie`
group show nom_groupe	

	Affiche les propriétés du groupe indiqué. Exemple : `ivadmin> group show crédit`
group show-dn dn	

	Affiche le nom du groupe désigné par l'argument dn.
	
	Exemple :
	`ivadmin> group show-dn`
	`cn=crédit,ou=Arles,o=Chaussons SA,c=FR`

group show-members nom_groupe	

	Affiche la liste des membres du groupe indiqué, dans l'ordre des DN.
	
	Exemple :
	`ivadmin> group show-members crédit`
	
	La sortie ressemble à ceci :
	`dlucas`
	`mlucaser`

group list modèle sortie_max	

	Affiche la liste des groupes définis, par nom de groupe et selon un modèle de recherche spécifié.
	
	L'argument modèle permet de spécifier un critère de recherche. Pour définir ce modèle, vous pouvez utiliser une combinaison de caractères génériques et de constantes, en distinguant les majuscules et les minuscules (par exemple, `*Austin*`).
	
	L'argument sortie_max détermine le nombre d'occurrences pouvant être renvoyées pour une même requête (par exemple, `2`). Ce nombre dépend également de la configuration du serveur LDAP qui permet de spécifier le nombre maximum d'occurrences pouvant être renvoyées à l'issue d'une recherche. Policy Director renvoie au moins le nombre d'occurrences défini par sortie_max et par la valeur configurée au niveau du serveur LDAP.
	
	La sortie ressemble à ceci :
	`crédit`
	`marketing`

group list-dn modèle sortie_max	

	Si une partie du DN est connue, cette commande affiche la liste des groupes définis, par DN et selon un modèle de recherche spécifié.
	
	Le caractère générique remplace la partie `cn=` du nom distinctif du groupe.
	
	La valeur de l'argument sortie_max dépend également de la configuration du serveur LDAP qui permet de spécifier le nombre maximum d'occurrences pouvant être renvoyées à l'issue d'une recherche. Policy Director renvoie au moins le nombre d'occurrences défini par sortie_max et par la valeur configurée au niveau du serveur LDAP.
	
	Exemple :
	`ivadmin> group list-dn *t* 2`
	
	La sortie ressemble à ceci :
	`cn=crédit,ou=Arles,o=Chaussons SA,c=FR`
	`cn=marketing,ou=Brives,o=Ventes Arles,c=FR`

Remarques :

Vous devez entrer l'argument dn en respectant le format exact de la sortie de la commande **group show-dn**. Utilisez des doubles guillemets (″) si la valeur de l'argument dn contient un espace.

Par exemple :

```
cn=crédit,ou=Arles,o=Chaussons SA,c=FR
```

Les commandes **group show** et **group show-dn** affichent les informations suivantes pour le groupe `crédit` :

```
ID groupe :
crédit
DN LDAP : cn=crédit,ou=Arles,o=Chaussons SA,c=FR
Description : Service des crédits HCUS
CN LDAP : crédit
Est SecGroup : vrai
```

Commandes de gestion des ressources

Les commandes **ivadmin** suivantes de Policy Director permettent de contrôler les opérations impliquant les ressources.

Ces opérations sont notamment les suivantes :

- «Gestion des ressources»
- «Gestion des groupes de ressources» à la page 293
- «Gestion des droits d'accès des ressources» à la page 295

Gestion des ressources

Les commandes **ivadmin rsrc** suivantes permettent de gérer différentes ressources, notamment les serveurs Web utilisés par les utilisateurs GSO.

Une ressource GSO est un serveur Web. L'identifiant **-T** apparaissant dans une définition de jonction intelligente caractérise un serveur Web.

Une commande **ivadmin rsrc** identifie le nom de la ressource Web.

Les commandes **ivadmin rsrc** suivantes correspondent aux taches de gestion du panneau **Ressources GSO** de la console de gestion :

Commande	Description
rsrc create nom_ressource [-desc description]	
	Crée et nomme une ressource serveur Web. L'argument nom_ressource désigne le nom attribué à la ressource Web pour l'identifier (par exemple, `engwebs01`). L'argument description permet d'entrer une description facultative afin d'identifier plus facilement la ressource. Tout paramètre facultatif doit être précédé d'un tiret (-). Les descriptions contenant des espaces doivent être encadrées par des doubles guillemets ("). `ivadmin> rsrc create engwebs01 -desc "Serveur Web Ingénierie - Salle 4807"`
rsrc delete nom_ressource	
	Supprime la ressource désignée ainsi que sa description. Un message d'erreur s'affiche si la ressource spécifiée n'existe pas. Exemple : `ivadmin> rsrc delete engwebs01`
rsrc list	

	Affiche les noms des ressources Web définies dans le répertoire LDAP, par nom de ressource.
	
	Exemple :
	
	`ivadmin> rsrc list`
	
	La sortie ressemble à ceci :
	
	`engwebs01`
	`engwebs02`
	`engwebs03`

rsrc show nom_ressource	

	Affiche les caractéristiques de la ressource Web désignée.
	
	Un message d'erreur s'affiche si la ressource spécifiée n'existe pas.
	
	Exemple :
	
	`ivadmin> rsrc show engwebs01`
	
	La sortie ressemble à ceci :
	
	`Nom de la ressource Web : engwebs01`
	`Description : Serveur Web Ingénierie - Salle 4807`

Gestion des groupes de ressources

Les commandes **ivadmin rsrcgroup** suivantes correspondent aux tâches de gestion du panneau **Groupes de ressources GSO** de la console de gestion. Elles permettent de gérer les différents attributs des groupes de ressources.

Un groupe de ressources est un groupe de serveurs Web utilisant tous les mêmes séries d'ID utilisateur et de mots de passe. Vous pouvez créer un droit d'accès unique pour toutes les ressources membres du groupe de ressources. Policy Director utilise un seul droit d'accès pour un groupe de ressources au lieu d'en affecter un séparément à chacune des ressources membres du groupe.

Les commandes **ivadmin rsrcgroup** suivantes correspondent aux taches de gestion du panneau **Groupes de ressources GSO** de la console de gestion :

Commande	Description
rsrcgroup create nom_groupe_ressources [-desc description]	

	Crée et nomme un groupe de ressources Web.
	
	L'argument nom_groupe_ressources désigne le nom attribué au groupe de ressources.
	
	L'argument description permet d'entrer une description facultative afin d'identifier le groupe de ressources. Le paramètre facultatif **-desc** doit être précédé d'un tiret (-). Les descriptions contenant des espaces doivent être encadrées par des doubles guillemets (″).
	
	Exemple :
	`ivadmin>`
	`rsrcgroup create webs4807 -desc "Serveurs`
	`Web, Salle 4807"`

rsrcgroup delete nom_groupe_ressources	
	Supprime le groupe de ressources désigné ainsi que sa description. Ce groupe de ressources doit exister pour que l'opération aboutisse. Exemple : `ivadmin> rsrcgroup delete webs4807`
rsrcgroup modify nom_groupe_ressources add rsrcname nom_ressource	
	Ajoute une ressource Web dans un groupe de ressources. Ce groupe de ressources doit exister pour que l'opération aboutisse. Exemple : `ivadmin> rsrcgroup modify webs4807 add rsrcname engwebs02`
rsrcgroup modify nom_groupe_ressources remove rsrcname nom_ressource	

	Supprime une ressource Web dans un groupe de ressources.
	
	Exemple :
	`ivadmin> rsrcgroup`
	`modify webs4807 remove rsrcname engwebs02`

rsrcgroup list	

	Affiche les noms des groupes de ressources Web définis dans le répertoire LDAP. Les données qui suivent "list" sont ignorées.
	
	Exemple :
	`ivadmin> rsrcgroup list`
	
	La sortie ressemble à ceci :
	`webs4807`
	`websbld3`
	`websbld4`

rsrcgroup show nom_groupe_ressources	

	Affiche les caractéristiques du groupe de ressources Web désigné.
	
	Un message d'erreur s'affiche si le groupe de ressources spécifié n'existe pas.
	
	Exemple :
	`ivadmin> rsrcgroup show webs4807`
	
	La sortie ressemble à ceci :
	`Nom du groupe de ressources : webs4807`
	`Description : Serveurs Web, Salle 4807`
	`Membres du groupe de ressources :`
	`engwebs01`
	`engwebs02`
	`engwebs03`

Gestion des droits d'accès des ressources

Les commandes **ivadmin rsrccred** suivantes permettent de gérer les différents attributs des droits d'accès des ressources.

Un droit d'accès de ressource associe un nom d'utilisateur et un mot de passe à une ressource destinée aux utilisateurs GSO, par exemple, un serveur Web ou un groupe de serveurs Web.

Seuls les types de ressource "web" et "group" peuvent être spécifiés avec les commandes **ivadmin rsrccred**.

Remarque : La ressource ou le groupe de ressources doivent exister pour que l'on puisse leur appliquer des commandes de droit d'accès.

Commande	Description
rsrccred create nom_ressource rsrcuser id_ressource rsrcpwd mdp_ressource rsrctype {web | group} user nom_utilisateur	
	Crée et nomme un droit d'accès de ressource. L'utilisateur et la ressource (ou le groupe de ressources) désignés doivent exister pour que l'opération aboutisse. Un message d'erreur s'affiche si l'utilisateur, la ressource ou le groupe de ressources n'existent pas. Les types de ressource admis sont "web" ou "group". L'argument nom_ressource désigne le nom attribué à la ressource lors de sa création (par exemple, `engwebs01`). L'argument id_ressource désigne l'identification utilisateur unique (ID utilisateur) associé à l'utilisateur sur le serveur Web (par exemple, `4807ws01`. L'argument mdp_ressource désigne le mot de passe associé à l'utilisateur sur le serveur Web (par exemple, *`mdprsrc`*) L'argument nom_utilisateur désigne l'utilisateur auquel le droit d'accès de ressource créé s'applique (par exemple `dlucas`). Exemple : `ivadmin> rsrccred create engwebs01 rsrcuser 4807ws01 rsrcpwd` *`mdprsrc`* `rsrctype web user dlucas`

rsrccred modify nom_ressource rsrctype {web | group} set [-rsrcuser id_ressource] [-rsrcpwd mdp_ressource] user nom_utilisateur	
	Modifie les données d'ID utilisateur et de mot de passe du droit d'accès de la ressource spécifiée. Pour modifier ou réinitialiser l'ID utilisateur ou le mot de passe du droit d'accès de la ressource, les commandes optionnelles doivent être précédées d'un tiret (-). La ressource ou le groupe de ressources et l'utilisateur doivent exister pour que cette opération aboutisse. Le type de ressource indiqué doit refléter celui défini lors de la création de la ressource ("web" ou "group"). Exemple : `ivadmin> rsrccred modify engwebs01 rsrctype group set -rsrcuser 4807ws01 -rsrcpwd` *`nouvmdp`* `user dlucas`
rsrccred delete nom_ressource rsrctype {web | group} user nom_utilisateur	
	Supprime les données du droit d'accès de ressource rattachées à l'utilisateur indiqué. Le type de ressource indiqué doit refléter celui défini lors de la création de la ressource ("web" ou "group"). Exemple : `ivadmin> rsrccred delete engwebs01 rsrctype group user dlucas`
rsrccred list user nom_utilisateur	

	Affiche le nom et le type des ressources pour lesquelles l'utilisateur indiqué possède un droit d'accès.
	
	Exemple :
	
	`ivadmin> rsrccred list user dlucas`
	
	La sortie ressemble à ceci :
	
	`Nom de la ressource : engwebs01`
	`Type de ressource : group`
	`Nom de la ressource : engwebs02`
	`Type de ressource : web`

rsrccred show nom_ressource rsrctype {web | group} user nom_utilisateur	

	Affiche les droits d'accès de ressource détenus par l'utilisateur indiqué.
	
	Un message d'erreur s'affiche si l'utilisateur n'existe pas ou s'il ne possède aucun droit d'accès de ressource.
	
	Exemple :
	
	`ivadmin> rsrccred show webs4807 rsrctype group user dlucas`
	
	La sortie ressemble à ceci :
	
	`Nom de la ressource : engwebs01`
	`Type de ressource : group`
	`ID de l'utilisateur de la ressource : dlucas`

Commandes de gestion des règles du registre

Les commandes **ivadmin policy** permettent de contrôler les données générales des règles appliquées aux utilisateurs de Policy Director. L'administrateur peut gérer les attributs de règle de sécurité suivants :

- «Gestion des règles de sécurité des connexions».
- «Gestion des règles de sécurité des mots de passe»

Les règles de sécurité définissent les contraintes appliquées aux comptes utilisateur et aux mots de passe pour améliorer la sécurité globale du système. Ces contraintes peuvent s'imposer d'une manière générale (globalement à tous les utilisateurs présents dans le système) ou spécifique (uniquement à un utilisateur déterminé). Dans le cas de règles de sécurité spécifiquement appliquées à un utilisateur, ces règles sont prioritaires par rapport aux règles générales éventuellement définies par ailleurs. Cette priorité s'applique, que les règles spécifiques soient plus restrictives que les règles générales ou non.

Gestion des règles de sécurité des connexions

Les commandes **ivadmin policy** suivantes permettent à l'administrateur de gérer les règles de sécurité applicables aux connexions.

Les commandes ivadmin **policy** dédiées aux connexions permettent de créer ou de copier des règles de sécurité pour les connexions. Elles permettent aussi d'afficher des informations sur les règles de connexion applicables à un compte utilisateur.

S'agissant des tâches de gestion des règles de sécurité des connexions, Policy Director définit l'heure relative sous la forme JJJ-hh:mm:ss, et l'heure absolue sous la forme AAAA-MM-JJ-hh:mm:ss.

Commande	Description
policy {set | get} max-account-age [heure_relative] [-user nom_utilisateur]	

	Définit (set) ou affiche (get) le délai maximal (en jours et en heures) avant l'arrivée à expiration du compte de l'utilisateur.
	Exemples :
	`ivadmin> policy set max-account-age 031-12:30:00 dlucas`
	Ou :
	`ivadmin> policy get max-account-age dlucas`

policy {set | get} account-expiry-date [heure_absolue] [-user nom_utilisateur]	

	Définit (set) ou affiche (get) la date et l'heure (absolue) d'arrivée à expiration du compte de l'utilisateur. Cette commande peut aussi définir le moment de l'arrivée à expiration de tous les comptes utilisateur.
	Exemples :
	`ivadmin> policy set account-expiry-date 1999-12-30-23:30:00 dlucas`
	Ou :
	`ivadmin> policy get account-expiry-date dlucas`

Gestion des règles de sécurité des mots de passe

Les commandes **ivadmin policy** suivantes permettent à l'administrateur de gérer les règles de sécurité applicables aux mots de passe.

S'agissant des tâches de gestion des règles de sécurité des mots de passe, Policy Director définit l'heure relative sous la forme JJJ-hh:mm:ss.

Commande	Description
policy {set | get} min-password-length [valeur]	

	Définit la longueur minimale, en caractères, d'un mot de passe. L'argument valeur indique cette longueur.
	
	Exemples :
	`ivadmin> policy set min-password-length 8`
	
	Ou :
	`ivadmin> policy get min-password-length`

Annexe B. 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.

Les informations fournies dans le présent document sont susceptibles d'être modifiées avant la disponibilité du produit.

Le présent document contient des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Pour les illustrer de la manière la plus complète possible, ces exemples mentionnent des noms de personnes, de sociétés, de marques ou de produits, à des fins explicatives uniquement. Ces noms sont fictifs et toute ressemblance avec une société ou des données réelles serait purement fortuite.

LICENCE DE COPYRIGHT :

Le présent logiciel contient des exemples de programmes d'application en langage source destinés à illustrer les techniques de programmation sur différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquelles ils ont été écrits ou aux interfaces de programmation IBM.

Ces exemples de programmes n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes.

Chaque copie, partie ou produit dérivé issu de ces programmes d'exemple doit comprendre les informations légales suivantes :

© (nom de votre société) (année). Certaines parties de ce programme sont issues d'échantillons fournis par IBM Corp. © Copyright IBM Corp. entrez la ou les années. Tous droits réservés.

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

Marques

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

AIX
DCE
IBM
FirstSecure
Global Sign-On
GSO
LDAP
Policy Director
SecureWay

D'autres sociétés sont propriétaires des autres marques, noms de produits ou logos qui pourraient apparaître dans ce document.

AuthAPI	DASCOM Inc.
DASCOM	DASCOM Inc.
IntraVerse	DASCOM Inc.
Internet Information Server (IIS)	Microsoft Corporation
Internet Explorer	Microsoft Corporation
Netscape et logos Netscape	Netscape Communications Corporation
Logos Netscape	Netscape Communications Corporation
Netscape FastTrack	Netscape Communications Corporation
Netscape Navigator	Netscape Communications Corporation
NetSEAL	DASCOM Inc.
NetSEAT	DASCOM Inc.
Smart Junctions	DASCOM Inc.
Solaris	Sun Microsystems Inc
WebSEAL	DASCOM Inc.

La marque Java et toutes les marques dérivées de Java sont des marques de Sun Microsystems Inc. déposées aux Etats-Unis et/ou dans d'autres pays.

Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation déposées aux Etats-Unis et/ou dans d'autres pays.

UNIX est une marque déposée aux Etats-Unis et/ou dans d'autres pays. Unix est distribué sous licence exclusive de X/Open Company Limited.

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Glossaire

Ce glossaire définit les termes et acronymes utilisés dans ce manuel, en particulier les termes nouveaux, peu usités ou ayant un intérêt spécifique. Il comprend des termes et définitions issus des ouvrages suivants :

- IBM Dictionary of Computing, New York, McGraw-Hill, 1994.
- American National Standard Dictionary for Information Systems, ANSI X3.172–1990, American National Standards Institute (ANSI), 1990.
- Answers to Frequently Asked Questions, Version 3.0, California, RSA Data Security Inc., 1998.

A

AC : Autorité de certification.

AC racine : Autorité de certification située au sommet d'une hiérarchie d'AC PKI.

AE : Autorité d'enregistrement.

algorithme de signature numérique : Algorithme de clé publique utilisé dans la norme DSS (Digital Signature Standard). Cet algorithme ne peut pas être utilisé pour le chiffrement des données mais uniquement pour les signatures numériques.

American National Standard Code for Information Interchange (ASCII) : Code standard utilisé pour l'échange des données entre les systèmes de traitement ou de communication de données et les équipements connexes. Le système ASCII utilise un jeu de caractères composé de caractères codé sur 7 bits (plus un huitième bit pour le contrôle de parité). Le jeu de caractères comprend des caractères de contrôle non imprimables et des caractères graphiques.

American National Standards Institute (ANSI) : Organisme chargé de l'élaboration des procédure encadrant la création et l'utilisation des normes industrielles en vigueur aux Etats-Unis. Cet organisme regroupe des fabricants, des consommateurs et des groupements d'intérêts.

ANSI : American National Standards Institute.

API : Application program interface (interface de programme d'application).

applet : Programme informatique écrit sous Java, qui s'exécute dans le cadre d'un navigateur Web compatible Java. Egalement appelé ″applet Java″.

applet Java : Voir applet. S'oppose àapplication Java.

application Java : Programme autonome élaboré avec le langage de programmation Java. Ce programme s'exécute en dehors du contexte d'un explorateur Web.

ASCII : American National Standard Code for Information Interchange (code standard américain pour l'échange de données).

authentification : Processus consistant à établir de manière certaine l'identité d'une partie impliquée dans une communication.

authentification des utilisateurs : Processus consistant à attester que l'émetteur d'un message est bien le propriétaire identifiable et autorisé de ce message. L'authentification atteste également que vous êtes bien en communication avec l'utilisateur final ou le système que vous avez voulu contacter.

autorisation : Permission d'accéder à une ressource.

autorité de certification (AC) : Logiciel chargé d'appliquer les règles de sécurité élaborées par une organisation et d'attribuer des identités électroniques sécurisées sous la forme de certificats. L'autorité de certification peut traiter les requêtes des autorités d'enregistrement (AE) pour délivrer, renouveler et révoquer les certificats. L'AC utilise l'autorité d'enregistrement du produit IBM SecureWay Trust Authority pour publier les certificats délivrés et révoqués dans l'annuaire des certificats. Voir aussicertificat numérique.

autorité d'enregistrement (AE) : Dans le contexte de Policy Director, il s'agit du produit IBM SecureWay Trust Authority. L'AE administre les certificats numériques dans le but de faire appliquer les règles de sécurité d'une organisation, depuis la réception initiale d'une requête d'inscription jusqu'à la révocation du certificat.

B

base de données d'enregistrement : Contient des informations en rapport avec les requêtes de certificat et les certificats délivrés. La base de données contient des informations relatives aux inscriptions et aux modifications apportées aux certificats au cours de leur existence.

bibliothèque de stockage de données : Module permettant d'accéder aux données permanentes des certificats, des listes de révocations de certificat, des clés, des règles et d'autres objets en rapport avec la sécurité.

C

certificat d'AC : Certificat accepté par votre navigateur Web, à votre demande explicite, provenant d'une autorité de certification non reconnue. Le navigateur peut ensuite utiliser ce certificat pour authentifier les communications avec des serveurs dotés de certificats délivrés par cette même autorité de certification.

certificat de navigateur : Certificat numérique également appelé certificat de côté client. Ce certificat est délivré par une autorité de certification (AC) par le biais d'un serveur Web SSL. Les clés (codes) contenues dans un fichier codé permettent au détenteur du certificat de coder, décoder et signer des données. Habituellement, ces clés sont stockées au niveau du navigateur Web. Certaines applications permettent d'enregistrer ces clés sur des cartes à puce ou sur d'autres supports. Voir aussicertificat numérique.

certificat de serveur : Certificat numérique délivré à un serveur Web par une autorité de certification pour lui permettre de réaliser des transactions utilisant le protocole SSL. Lorsqu'un navigateur se connecte au serveur via le protocole SSL, le serveur lui communique sa clé publique. Celle-ci permet au navigateur d'authentifier le serveur et de lui transmettre des informations codées. Voir aussicertificat d'AC, certificat numérique,etcertificat de navigateur.

certificat de site : Identique à un certificat d'AC mais d'une validité limitée à un site WEB déterminé. Voir aussicertificat d'AC.

certification : Processus par lequel un tiers sécurisé délivre un droit d'accès électronique qui garantit l'intégrité de l'identité d'une personne, d'une entreprise ou d'une organisation.

certification numérique : Voir certification.

certification réciproque : Modèle de sécurisation dans lequel une autorité de certification délivre à une autre AC un certificat contenant la clé publique associée à sa clé de signature privée. Un certificat réciproquement authentifié permet aux systèmes clients ou aux entités finales d'un domaine administratif de communiquer de manière sécurisée avec les systèmes clients ou les entités finales d'un autre domaine.

certificat numérique : Droit d'accès électronique délivré par un tiers sécurisé à une personne ou à une entité. Chaque certificat est signé par la clé privée de l'autorité de certification. Le certificat garantit l'identité d'une personne, d'une entreprise ou d'une organisation.

En fonction des attributions de l'autorité de certification, le certificat peut attester de l'habilitation de son détenteur à exercer un commerce électronique sur l'Internet. Dans une certaine mesure, le certificat numérique équivaut à un permis de conduire pour un conducteur, ou à un diplôme de fin d'étude pour un médecin. Il certifie que le détenteur de la clé privée correspondante est habilité à exercer certaines activités de commerce électronique.

Un certificat contient des informations sur l'entité qu'il certifie, qu'il s'agisse d'une personne, d'une machine ou d'un programme informatique. Ces informations comprennent la clé publique certifiée de cette entité.

certificat X.509 : Norme de certificat largement acceptée et conçue pour assurer une gestion et une distribution sécurisées des certificats numériques entre les réseaux Internet sécurisés. Le certificat X.509 définit des structures de données qui appliquent les procédures de distribution des clés publiques portant les signatures numériques de tiers sécurisés.

certificat X.509 version 3 : Le certificat X.509 v3 contient des structures de données étendues pour le stockage et l'extraction des données relatives aux applications de certification, à la distribution et à la révocation des certificats, aux règles et aux signatures numériques.

Les processus de certificat X.509 v3 créent des listes de révocations de certificat avec horodates pour tous les certificats. A chaque utilisation d'un certificat, les fonctions X.509 v3 permettent à l'application de vérifier sa validité. Il permet également à l'application de vérifier si le certificat figure dans une liste des révocations de certificat (LRC). Les LRC X.509 v3 peuvent être élaborées pour une période de validité spécifique. Elles peuvent également reposer sur d'autres circonstances entraînant l'invalidation d'un certificat. Par exemple, si un salarié quitte une organisation, son certificat entrera dans la liste des révocations de certificat.

CGI : Common Gateway Interface (interface de passerelle standard).

chiffrement : Transformation des informations visant à permettre exclusivement à une personne détenant la clé de déchiffrement appropriée de leur rendre leur forme d'origine. Synonyme de codage.

chiffrement/déchiffrement : Processus consistant, pour l'émetteur, à chiffrer des données à l'aide de la clé publique du destinataire et, pour ce destinataire, à déchiffrer ces données à l'aide de sa clé privée.

chiffrement en base 64 : Méthode standard de transmission des données binaires avec MIME.

classe : Dans le contexte de la conception ou de la programmation orientée objet, une classe représente un groupe d'objets ayant une définition commune et, par conséquent, des propriétés, des fonctions et un mode opératoire communs.

clé : Valeur utilisée en cryptographie pour chiffrer ou déchiffrer (coder/décoder) les informations.

clé de chiffrement de document : Habituellement, une clé de chiffrement/déchiffrement symétrique telle qu'une clé DES.

clé privée : Clé de la paire de clés publique/privée utilisable exclusivement par son propriétaire. Elle permet à son propriétaire de réceptionner une transaction privée ou de créer une signature numérique. Les données signées par une clé privée ne peuvent être vérifiées qu'avec la clé publique associée. S'oppose àclé publique. Voir aussipaire de clés publique/privée.

clé publique : Clé de la paire de clés publique/privée pouvant être communiquée aux tiers. La clé publique permet aux tiers d'acheminer une transaction jusqu'à son propriétaire et de vérifier une signature numérique. Les données codées avec la clé publique ne peuvent être décodées qu'avec la clé privée associée. S'oppose àclé privée. Voir aussipaire de clés publique/privée.

client : (1) Unité fonctionnelle destinataire des services partagés d'un serveur. (2) Ordinateur ou programme demandant à accéder à un service fourni par un autre ordinateur ou programme.

client/serveur : Modèle d'architecture informatique décentralisée selon lequel un programme résidant dans un site envoie une requête à un autre programme résidant dans un autre site et en attend une réponse. Le programme à l'origine de la requête est appelé le client, celui qui réceptionne la requête et y répond est appelé le serveur.

commerce électronique : Ce terme couvre les transactions commerciales passées au moyen de réseaux et d'ordinateurs, à l'exclusion des transferts de fonds. Il désigne les achats et ventes de biens et services (impliquant des clients, des fournisseurs, des fabricants, etc.) réalisés sur l'Internet. Le commerce électronique est la composante principale du e-business.

Common Cryptographic Architecture (CCA) : Logiciel IBM permettant d'appliquer une méthode de chiffrement homogène sur les principales plates-formes informatiques IBM. Ce logiciel s'adapte à des programmes d'application élaborés avec différents langages de programmation. Les programmes d'application peuvent appeler les services CCA pour une grande variété de fonctions de chiffrement, notamment pour le chiffrement DES et RSA.

Common Gateway Interface (CGI) : Interface de passerelle standard. Méthode standard de transmission des données entre les pages Web et les serveurs Web.

confidentialité : Non-divulgation des informations à des tiers non autorisés.

contestation : Contestation d'un fait ou d'un événement. Par exemple, nier avoir envoyer un message ou soumis une requête donnée.

contrôle d'intégrité : Contrôle des rapports d'audit attachés aux transactions réalisées avec des composants externes.

cryptographie : Dans le contexte de la sécurité informatique, les principes, moyens et méthodes de chiffrement et de déchiffrement des données.

cryptographique : Lié à un processus de transformation des données ayant pour objectif de masquer leur signification.

D

Data Encryption Standard (DES) : Norme de chiffrement des données. Méthode de chiffrement par bloc. Définie et validée par les autorités américaine en 1977 comme une norme officielle, cette méthode a été développée par IBM à l'origine. Le standard DES a été longuement étudié depuis sa création et est à présent un système cryptographique largement reconnu et utilisé.

Le DES est un système cryptographique symétrique : utilisé pour les communications, l'émetteur comme le destinataire doivent reconnaître la même clé secrète. Cette clé permet de coder et de décoder le message. Le DES peut aussi être utilisé pour un usage personnel, par exemple, pour enregistrer des fichiers sur un disque dur sous une forme codée. Le DES utilise une taille de bloc de 64 bits et une clé de 56 bits pour le chiffrement. Il fut conçu à l'origine pour être utilisé sur les matériels. Le NIST (organisme en charge des normes aux USA) renouvelle l'homologation officielle du DES tous les cinq ans.

déchiffrement : Inversion du processus de chiffrement. Synonyme de décodage.

délai de publication des LRC : Défini dans le fichier de configuration de l'autorité de certification, il s'agit du délai séparant deux publications de la liste des révocations de certificat dans le répertoire.

démon : Programme chargé d'exécuter des tâches en arrière-plan. Ce programme est appelé de façon implicite lorsqu'une condition définie se réalise. L'utilisateur n'a pas besoin d'être informé du déclenchement d'un démon dans la mesure où le système l'initialise automatiquement. Un démon peut avoir une durée d'existence illimitée ou être périodiquement régénéré par le système.

Le terme démon trouve son origine dans la mythologie. Décliné par la suite en un acronyme plus rationnel, le terme anglais DAEMON signifie depuis Disk And Execution MONitor (contrôleur d'exécution et de disque).

DER : Distinguished Encoding Rules (règles de codage des DN).

DES : Data Encryption Standard (norme de chiffrement des données)

Distinguished Encoding Rules (DER) : Le système DER sélectionne un type de chiffrement parmi ceux admis par les règles de chiffrement en éliminant toutes les options de l'émetteur.

distinguished name (DN) : Nom distinctif. Nom unique de l'entrée de données stockée dans le répertoire. Le DN identifie de manière unique la position d'une entrée dans la structure hiérarchique du répertoire.

DN : Distinguished name (nom distinctif).

domaine : Voirdomaine de sécurité etdomaine d'enregistrement.

domaine d'enregistrement : Ensemble de ressources, de règles et d'options de configuration rattachées à certains processus d'enregistrement des certificats. Le nom du domaine est compris dans l'adresse URL utilisée pour exécuter l'application d'enregistrement.

domaine de sécurité : Groupe (une société, un groupe de travail, une université ou une administration) dont les membres possèdent des certificats homologués par la même autorité de certification. Les utilisateurs dont le certificat a été signé par une autorité de certification donnée peuvent accepter l'identité d'un autre utilisateur doté d'un certificat signé par la même AC.

domaine sécurisé : Ensemble d'entités dont les certificats ont été homologués par la même autorité de certification.

droit d'accès : Informations confidentielles permettant de prouver son identité dans le contexte d'un processus d'authentification. Dans les environnements informatiques en réseau, le type de droit d'accès le plus répandu est le certificat, créé, signé et délivré par une autorité de certification.

E

e-business : Ce terme désigne les transactions commerciales passées au moyen de réseaux et d'ordinateurs. Il recouvre les achats et ventes de biens et services, et les transferts de fonds par communications électroniques.

entité finale : Sujet d'un certificat autre qu'une autorité de certification.

extension de certificat : Fonction optionnelle du format de certificat X.509 v3 qui permet l'insertion de champs supplémentaires dans le certificat. Il existe des extensions standard et des extensions définies par l'utilisateur. Les extensions standard concernent les données de règles et de clés, les attributs de sujet et d'émetteur et les contraintes de chemin de certification.

extranet : Réseau externe inspiré de la technologie de l'Internet. Certaines sociétés commencent à intégrer les outils de communication du Web, le commerce électronique, la messagerie et les applications de travail en groupe à l'usage de leurs clients, partenaires ou salariés.

F

fichier d'audit : Données indiquant un chemin logique reliant une suite d'événements. Le processus d'audit permet le suivi des transactions et la gestion de l'historique d'une activité donnée.

File Transfer Protocol (FTP) : Protocole d'architecture client-serveur utilisé sur Internet pour le transfert de fichiers entre ordinateurs.

FTP : File Transfer Protocol.

H

historique des actions : Somme des événements intervenus au cours de l'existence d'un droit d'accès.

HTML : Hypertext Markup Language.

HTTP : Hypertext Transaction Protocol.

hypertexte : Texte contenant des mots, phrases ou graphiques sur lesquels l'utilisateur peut cliquer pour extraire et afficher un autre document. Ces mots, phrases ou graphiques sont appelés des liens hypertexte ou hyperliens. L'extraction des documents liés est appelée la récupération de liens.

Hypertext Markup Language (HTML) : Langage de marquage utilisé pour le chiffrement des pages Web. Le langage HTML est dérivé du langage SGML.

Hypertext Transaction Protocol (HTTP) : Protocole de communication client-serveur Internet utilisé pour le transfert de fichiers hypertexte sur le Web.

I

ID de requête : Valeur, composée de 24 à 32 caractères ASCII, qui identifie de manière unique une requête de certificat vis-à-vis de l'autorité d'enregistrement. Cette valeur communiquée pendant la transaction peut être utilisée pour extraire le statut de la requête de certificat ou le certificat associé.

instance : Dans le contexte de DB2, une instance est un environnement de gestion de base de données logique qui permet de stocker les données et d'exécuter les applications. Cet environnement permet de définir un jeu de paramètres de configuration communs pour

plusieurs bases de données. Dans le contexte de Policy Director, une instance de base de données est une copie de la base de données du registre des utilisateurs et une instance de serveur est une copie d'un serveur dupliqué.

intégrité : Un système protège l'intégrité des données s'il empêche leur modification par une personne non autorisée. S'oppose à la confidentialité des données, qui vise à empêcher leur divulgation à une personne non autorisée.

interface de programme d'application (API) : Dans le contexte de Policy Director, il s'agit d'une interface d'exploitation permettant à un programme d'application écrit dans un langage haut niveau d'utiliser les fonctions de Policy Director. L'API d'autorisation standard de Policy Director permet aux applications d'appeler le service d'autorisation centralisé de Policy Director. Cette faculté évite aux développeurs de devoir élaborer un code d'autorisation pour chaque nouvelle application. L'API d'autorisation de Policy Director permet de standardiser toutes les applications avec un système d'autorisation sécurisé. Elle permet également aux entreprises de mieux contrôler l'accès aux ressources proposées par leurs réseaux. Pour une information et une description complètes de l'API d'autorisation de Policy Director, reportez-vous au manuel Policy Director - Guide de programmation et de référence.

Internet : Structure internationale reliant des réseaux et permettant d'établir des connexions électroniques entre ordinateurs. Le réseau mondial Internet permet aux ordinateurs de communiquer entre eux à l'aide de logiciels tels que les navigateurs Web ou les programmes de messagerie électronique. Des universités, des entreprises et autres organisations, disposent de réseaux qui, reliés à d'autres réseaux de même nature, constituent l'Internet.

intranet : Réseau interne d'entreprise habituellement protégé des communications provenant de l'extérieur par un ou plusieurs pare-feu. Ce type de réseau est inspiré de la technologie de l'Internet. Sur un plan technique, un intranet est une simple extension de l'Internet. Le langage HTML et le protocole HTTP y sont fréquemment employés.

IPSec : Internet Protocol Security. Protocole de communication Internet standard développé par le IETF. Le protocole IPSec est un protocole de réseau conçu pour apporter des services de sécurité cryptographiques permettant de combiner des processus d'authentification et de contrôle d'accès tout en assurant l'intégrité et la confidentialité des données. Ses fonctions d'authentification performantes l'ont fait adopter par plusieurs concepteurs de réseaux privés virtuels pour les connexions bilatérales sécurisées sur l'Internet.

J

Java : Ensemble de technologies d'informatique de réseau indépendantes des plate-formes développées par Sun Microsystems. L'environnement Java comprend le système d'exploitation Java OS, les machines virtuelles correspondant aux différentes plates-formes, le langage de programmation orientée objet Java et plusieurs bibliothèques de classes d'objets.

Java Virtual Machine (JVM) : Machine virtuelle Java. Composant de l'environnement d'exploitation Java chargé de l'interprétation des octets des codes.

journal d'audit : Table d'une base de données contenant un enregistrement par événement contrôlé.

L

langage Java : Langage de programmation développé par Sun Microsystems pour les besoins des applets et des applications d'agent.

LCA : Liste de contrôle d'accès.

LCD : Liste des certificats délivrés.

LDAP : Lightweight Directory Access Protocol (protocole simplifié d'accès à l'annuaire).

Lightweight Directory Access Protocol (LDAP) : Protocole d'accès à l'annuaire.

liste de contrôle d'accès (LCA) : Dispositif permettant de limiter l'utilisation des ressources à une sélection d'utilisateurs autorisés.

liste des certificats délivrés (LCD) : Liste exhaustive des certificats délivrés avec mention de leur état courant (actif, révoqué, etc.). Les certificats sont indexés selon leur numéro de série et leur état. Cette liste est administrée par l'autorité de certification d'origine et stockée dans sa base de données.

liste des révocations de certificat (LRC) : Liste, signée et datée par une autorité de certification, répertoriant les certificats révoqués par cette autorité. Les certificats figurant dans cette liste ne doivent plus être acceptés. Voir aussicertificat numérique.

LRC : Liste des révocations de certificat.

M

MIME (Multipurpose Internet Mail Extensions) : Jeu de spécifications librement accessible qui permet l'échange de textes rédigés dans des langues utilisant des jeux de caractères différents. Le système MIME permet aussi l'échange de courriers électroniques incorporant des éléments multimédia entre différents systèmes informatiques utilisant les normes de

messagerie d'Internet. Les courriers électroniques peuvent, par exemple, contenir des jeux de caractères non ASCII, du texte avec mise en forme, des images, des sons, etc.

modèle de sécurisation : Convention d'organisation qui détermine la manière dont les autorités de certification s'homologuent réciproquement.

N

National Language Support (NLS) : Support de langue nationale. Permet de gérer les différences d'environnement local telles que les langues, les monnaies, les formats de date et d'heure et les formats de présentation des nombres.

National Security Agency (NSA) : Agence de la sécurité nationale. Administration américaine en charge de la sécurité nationale.

navigateur : Voirnavigateur Web

navigateur Web : Programme client, exécuté à partir d'un PC, qui permet à l'utilisateur de naviguer dans le World Wide Web ou de visualiser des pages HTML locales ou distantes. Le navigateur est un outil d'extraction qui permet un accès géographiquement illimité à l'ensemble des ressources multimédia disponibles sur le Web et sur l'Internet. Certains navigateurs peuvent afficher les textes comme les images tandis que d'autres se limitent à l'affichage des textes. La plupart des navigateurs gèrent les principales formes de communication utilisées sur l'Internet, telles que les transactions FTP.

NLS : National language support (support de langue nationale).

non-contestation : Utilisation d'une clé privée numérique visant à empêcher le signataire d'un document de contester indûment sa signature.

O

objet : Dans le contexte de la conception ou de la programmation orientée objet, un objet est la représentation abstraite de données et d'opérations associées à ces données. Voir aussiclasse.

P

paire de clés : Clés associées utilisées pour la cryptographie asymétrique. Une clé est utilisée pour coder les données (la clé publique), l'autre pour les décoder (la clé privée).

paire de clés publique/privée : La paire de clés publique/privée est un élément du concept de cryptographie par paire de clés introduit en 1976 par Diffie et Hellman pour résoudre la problématique de la gestion des clés. Selon ce concept, chaque utilisateur doit obtenir une paire de clés, une appelée la clé publique et l'autre la clé privée. La clé publique peut être communiquée aux tiers tandis que la clé privée doit rester secrète. L'émetteur et le destinataire des données n'ont pas besoin de partager des informations secrètes ; toutes les communications se font au moyen de la clé publique et la clé privée n'a besoin d'être ni transmise, ni divulguée. Dès lors, il n'est plus nécessaire de sécuriser un canal de communication pour éviter l'interception illicite ou le détournement des données. La seule règle imposée est que la clé publique doit être associée à son propriétaire d'une manière sûre (authentifiée), par exemple, dans un répertoire sécurisé. Chacun peut envoyer un message confidentiel au moyen d'une clé publique. En revanche, ce message ne peut être décodé qu'avec une clé privée que seul le destinataire prévu doit posséder. En outre, la cryptographie par paire de clés peut être utilisée pour sauvegarder la confidentialité des données (par le chiffrement) mais aussi pour l'authentification (par la signature numérique).

pare-feu : Passerelle permettant de relier des réseaux tout en limitant le flux des informations circulant entre eux. Habituellement, la finalité d'un pare-feu est de protéger les réseaux internes contre les accès et utilisations non autorisés en provenance de l'extérieur.

passerelle : Unité fonctionnelle permettant à des réseaux ou applications incompatibles de communiquer ensemble.

PEM : Privacy Enhanced Mail (courrier avec confidentialité renforcée). Norme de messagerie.

PKCS : Public Key Cryptography Standards (normes de cryptographie par clé publique). Norme de chiffrement de données.

PKCS#12 : VoirPublic Key Cryptography Standards.

PKCS#10 : VoirPublic Key Cryptography Standards.

PKI : Public Key Infrastructure (infrastructure de clé publique). Norme de clé de chiffrement.

PKIX : Norme PKI avec usage des certificats X.509 v3.

PKIX CMP (Certificate Management Protocol) : Protocole de gestion des certificats PKIX. Protocole permettant l'établissement de connexions entre des applications compatibles PKIX. PKIX CMP utilise TCP/IP comme premier vecteur de transmission et une couche abstraite en plus des sockets. Cette conception permet d'effectuer des interrogations supplémentaires.

pré-enregistrement : Dans le contexte du produit IBM SecureWay Trust Authority, processus permettant d'enregistrer un premier utilisateur, habituellement l'administrateur, qui pourra ensuite en enregistrer d'autres. Si la requête est approuvée, l'autorité

d'enregistrement (AR) délivre les informations qui permettront ensuite à cet utilisateur d'obtenir un certificat à l'aide du client Trust Authority.

Privacy Enhanced Mail (PEM) : (Courrier avec confidentialité renforcée). Norme de messagerie Internet avec confidentialité renforcée. Adoptée par le IAB (Internet Architect Board) pour garantir la sécurité des courriers électroniques sur l'Internet. Les protocoles PEM permettent le chiffrement des messages, l'authentification, le contrôle d'intégrité et la gestion des clés.

profil de certificat : Ensemble des caractéristiques qui définissent le type de certificat désiré (certificat SSL, ou IPSec par exemple). Le profil facilite la spécification et l'enregistrement des certificats. L'émetteur peut modifier le nom des profils et spécifier les caractéristiques du certificat désiré, par exemple, son délai de validité, la syntaxe des clés, les contraintes de définition du nom distinctif (DN), etc.

protocole : Convention de procédures de communication entre ordinateurs.

Public Key Cryptography Standards (PKCS) : Normes non officielles développées en 1991 par RSA Laboratories avec le concours de différents fabricants d'ordinateurs. Ces normes couvrent le chiffrement RSA, la convention Diffie-Hellman, le chiffrement par mot de passe, la syntaxe des certificats avancés, la syntaxe des messages cryptographiques, la syntaxe des clés privées et la syntaxe des procédures de certification.

- La norme PKCS#10 définit une syntaxe standard pour les requêtes de certification.
- La norme PKCS#12 définit un format portable pour le stockage ou la transmission des clés privées, des certificats, des données secrètes, etc.

Public Key Infrastructure (PKI) : Infrastructure de clé publique. Norme de sécurité logicielle basée sur la cryptographie par clé publique. PKI est un système de sécurité reposant sur les certificats numériques, les autorités de certification, les autorités d'enregistrement, les services de gestion des certificats et les services de répertoire partagé. Ce système permet de vérifier l'identité et l'autorité de chaque partie impliquée dans une transaction par Internet. Ces transactions peuvent impliquer des opérations rendant obligatoire la vérification des identités. Il peut s'agir, par exemple, de confirmer l'origine d'une offre commerciale, d'un courrier électronique ou de transactions financières.

Le système PKI réalise cet objectif en permettant à une personne ou une organisation habilitée d'authentifier les clés de chiffrement publiques et les certificats des utilisateurs. Il fournit des répertoires en ligne qui contiennent les clés de chiffrement publiques et les certificats utilisés pour la vérification des certificats numériques, des droits d'accès et des signatures numériques.

Il constitue un moyen efficace et rapide pour obtenir des réponses aux requêtes de vérification et aux requêtes de clés de chiffrement publiques. Il permet également d'identifier les dangers potentiels pour le système et de gérer les ressources en conséquence. Enfin, le PKI fournit un service d'horodate pour les transactions commerciales importantes.

R

RC4 : Code de bloc avec taille de clé variable, développé par Ron Rivest pour RSA Data Security. RC signifie Ron's Code (code de Ron) ou encore Rivest's Cipher (code de Rivest). Système similaire à RC2 mais utilisant une taille de bloc de 128 bits.

RC2 : Code de bloc avec taille de clé variable, développé par Ron Rivest pour RSA Data Security. RC signifie Ron's Code (code de Ron) ou encore Rivest's Cipher (code de Rivest). Ce système est plus rapide que le DES et est présenté comme une alternative à celui-ci. Il peut protéger des recherches de clés exhaustives, mieux ou moins bien que DES, selon la taille définie pour les clés. RC2 utilise des blocs de 64 bits et est deux à trois fois plus rapide que DES sur le plan logiciel. RC2 peut être utilisé dans les mêmes modes que DES.

Une convention passée entre la Software Publishers Association (SPA) et le gouvernement des Etats-Unis accorde à RC2 un statut spécial. RC2 permet un processus d'approbation des exportations plus rapide et plus simple que le processus d'exportation cryptographique conventionnel. Cependant, pour bénéficier d'une procédure d'approbation d'exportation rapide, un produit doit limiter la taille de clé RC2 à 40 bits, avec quelques exceptions. Une chaîne supplémentaire doit être utilisée pour déjouer les tentatives de fraude (notamment par l'utilisation d'une grande table de recherche de codes).

règles de certificat : Jeu de règles nommé qui détermine l'application ou non d'un certificat à une catégorie d'applications ayant les mêmes exigences de sécurité. Par exemple, des règles de certificat peuvent indiquer si un type de certification donné permet à un utilisateur d'accomplir des transactions sur des biens dans la limite d'une fourchette de prix déterminée.

répertoire : Dans le contexte des services de répertoire, il s'agit d'une structure hiérarchique, également appelée annuaire, conçue comme un référentiel mondial d'informations en rapport avec les communications (notamment pour les échanges de messagerie électronique et les usages cryptographiques). Le répertoire contient des éléments fondamentaux de la structure du PKI, notamment des clés publiques, des certificats et des listes de révocation des certificats.

Les données y sont organisées sur un principe hiérarchique, sous la forme d'une arborescence dont la

racine est le sommet. Les organisations représentées dans les niveaux supérieurs de cette arborescence sont souvent des gouvernements, des administrations ou des sociétés. Les utilisateurs et les périphériques sont habituellement représentés sous la forme de subdivisions (feuilles) de chaque sous-arborescence (branche). Ces utilisateurs, organisations, administrations, états et périphériques possèdent chacun une entrée qui les définit. Chaque entrée contient des attributs spécifiquement définis. Ces attributs fournissent des informations sur l'objet que l'entrée représente.

Chaque entrée de l'annuaire est associée à un nom distinctif, ou DN (pour distinguished name). Ce DN est unique dès lors que l'entrée qui le définit contient un attribut réputé unique dans le monde réel. A titre d'exemple, voici un DN dans lequel le code de pays (C pour ″country″) est US, l'organisation (O) est IBM, la division (OU pour ″organizational unit″) est Trust et le nom commun (CN pour ″common name″) est CA1.

```
C=US/O=vnet/OU=Trust/CN=CA1
```

Réseau privé virtuel (RPV) : Réseau de données privé utilisant l'Internet au lieu des lignes téléphoniques pour établir des connexions avec des systèmes distants. Dans la mesure où les utilisateurs accèdent aux ressources du réseau de l'entreprise par l'intermédiaire d'un fournisseur de service Internet au lieu d'un opérateur de téléphonie, le coût de l'accès à distance s'en trouve notablement diminué. Un réseau privé virtuel accroît également la sécurité des échanges de données. Dans le contexte d'un pare-feu standard, le contenu d'un message peut être codé mais les adresses de sa source et de sa destination ne peuvent pas l'être. Dans le cadre d'un RPV, l'utilisateur peut établir une connexion par tunnel qui permettra d'imbriquer et de coder l'ensemble des données (contenu et en-tête).

RPV : Réseau privé virtuel.

S

SAD : Service d'acquisition de droits d'accès.

schéma : Dans le contexte d'IBM SecureWay Directory, il s'agit de la structure interne qui définit les relations entre différents types d'objet.

Secure Sockets Layer (SSL) : Couche de sockets sécurisée. Protocole de communication standard d'IETF intégrant des services de sécurité aussi transparents que possible vis-à-vis de l'utilisateur final. Le protocole SSL établit un canal de communication sécurisé numériquement.

Un serveur compatible SSL accepte généralement les requêtes de connexion par SSL sur un autre port que celui utilisé pour les requêtes de connexion HTTP standard. Le protocole SSL ouvre une session pendant laquelle l'échange des signaux permettant d'établir les communications entre deux modems n'intervient qu'une seule fois. Cela fait, les communications sont codées. Le contrôle de l'intégrité des messages est continu jusqu'à la fin de la session SSL.

serveur : (1) Dans le contexte d'un réseau, station de travail fournissant des données et des fonctions à d'autres stations de travail (par exemple, un serveur de fichiers). (2) Dans le contexte de TCP/IP, système membre d'un réseau qui gère les requêtes d'un système installé dans un autre site, dans le cadre d'une architecture client-serveur.

serveur d'audit : Serveur chargé de réceptionner les événements contrôlés de la part des clients d'audit et de les enregistrer dans un journal d'audit.

serveur HTTP : Serveur chargé de gérer les communications Web avec les navigateurs et les autres programmes d'un réseau.

serveur relais : Dispositif intermédiaire situé entre l'ordinateur à l'origine de la demande d'accès (ordinateur A) et l'ordinateur auquel l'accès est demandé (ordinateur B). Si un utilisateur final soumet une requête d'utilisation d'une ressource dépendante de l'ordinateur A, cette requête est adressée à un serveur relais. Le serveur relais transmet la requête à l'ordinateur B, réceptionne sa réponse, puis la restitue à l'utilisateur final (A). Les serveurs relais permettent notamment d'accéder à des ressources du World Wide Web à partir d'un domaine protégé par un pare-feu.

serveur SAD : Serveur dédié au composant Service d'acquisition de droits d'accès (SAD) de Policy Director.

serveur Web : Programme de serveur qui répond aux requêtes d'accès aux informations adressées par les programmes de navigation. Voir aussiserveur.

service d'acquisition de droits d'accès (SAD) : Composant Service d'acquisition de droits d'accès (SAD) de Policy Director.

servlet : Programme, exécuté côté serveur, qui procure aux serveurs compatibles Java des fonctionnalités supplémentaires.

SGML : Standard Generalized Markup Language.

signature : Utilisation d'une clé privée pour créer une signature numérique. La signature est un moyen de prouver que vous acceptez la responsabilité du message que vous signez et que vous l'approuvez.

signature de code : Technique de signature des programmes exécutables utilisant des signatures numériques. La signature de code a pour objet de renforcer la fiabilité des logiciels distribués sur l'Internet.

signature et vérification : Signer signifie utiliser une clé numérique privée pour créer une signature. Vérifier signifie utiliser la clé publique associée pour contrôler cette signature.

signature numérique : Message codé accompagnant un document ou des données, qui garantit l'identité de son émetteur.

Une signature numérique peut procurer un niveau de sécurité supérieur à celui d'une signature manuscrite. En effet, une signature numérique n'est pas un nom codé ou une série de simples codes d'identification. Il s'agit plutôt d'une synthèse codée du message signé. L'ajout d'une signature numérique à un message permet donc une identification sûre de son émetteur (seule la clé de l'émetteur peut créer la signature). Il fige également le contenu du message signé (la synthèse codée du message doit refléter son contenu complet, sans quoi la signature n'est pas reconnue comme authentique). Ainsi, une signature numérique ne peut pas être reproduite d'un message sur un autre puisque la synthèse ne correspondrait pas. Toute modification postérieure du message signé aura pour effet d'invalider sa signature.

Simple Mail Transfer Protocol (SMTP) : Protocole de transfert de courrier électronique par l'Internet.

S/MIME : Norme acceptant la signature et le chiffrement des courriers électroniques transmis par l'Internet. VoirMIME.

SMTP : Simple Mail Transfer Protocol.

SSL : Secure Sockets Layer.

Standard Generalized Markup Language (SGML) : Normes de description des langages de marquage. Le langage HTML est dérivé du langage SGML.

structure interne : Voirschéma.

T

TCP/IP : Transmission Control Protocol/Internet Protocol.

texte nu : Données non codées. Synonyme de texte seul

texte seul : Données non codées (texte brut). Synonyme de texte nu.

Transmission Control Protocol/Internet Protocol (TCP/IP) : Protocole de contrôle de transmission/Protocole Internet. Série de protocoles de communication permettant des fonctions de connectivité bilatérale pour les réseaux longue distance (WAN) et les réseaux locaux.

Triple DES : Algorithme symétrique qui code le texte nu trois fois. Bien qu'il existe plusieurs moyens équivalents, la forme de chiffrement multiple la plus sûre est la méthode Triple DES dans la mesure où elle utilise trois clés distinctes.

Trust Authority : (Autorité de sécurisation). Solution de sécurité, intégrée au produit IBM SecureWay, qui permet la délivrance, le renouvellement et la révocation des certificats numériques. Ces certificats peuvent être utilisés avec un large éventail d'applications Internet afin d'authentifier les utilisateurs et de sécuriser les communications.

tunnel : Dans le contexte des réseaux privés virtuels (RPV), connexion bilatérale établie à l'initiative d'une des parties par le biais de l'Internet. Une fois connectés, les utilisateurs distants peuvent utiliser le tunnel pour échanger des informations sécurisées, codées et imbriquées avec les serveurs du réseau privé de l'entreprise.

type : Voirtype d'objet.

type d'objet : Catégorie d'objet pouvant être stocké dans le répertoire d'IBM SecureWay Directory. Par exemple, ces objets peuvent représenter une organisation, un événement tel qu'une réunion, un lieu, un équipement, une personne, un programme ou un processus.

U

Unicode : Jeu de caractères 16 bits défini par la norme ISO 10646. La norme de chiffrement de caractères Unicode est un code international utilisé pour le traitement des informations. Elle s'applique aux principaux scripts utilisés dans le monde et constitue la base de l'internationalisation et de la localisation (traduction) des logiciels. Tous les codes source utilisés en programmation sous Java sont élaborés avec Unicode.

Uniform Resource Indicator (URI) : Indicateur de ressource standard. Une adresse URL absolue indique la position URI par rapport à la fois à un nom d'hôte, ou une adresse IP, et à un port de réseau.

Uniform Resource Locator (URL) : Localisateur de ressource standard. Dispositif d'adressage des ressources sur l'Internet. L'adresse URL spécifie le protocole utilisé et le nom du système hôte ou son adresse IP. Elle comprend également le numéro de port, le chemin et d'autres données permettant d'accéder à une ressource à partir d'une machine déterminée.

URI : Uniform Resource Indicator.

URL : Uniform Resource Locator.

UTF-8 : Format de transformation. Permet aux ordinateurs ne gérant que les jeux de caractères 8 bits de convertir les données Unicode 16 bits en données 8

bits équivalentes puis de les reconvertir dans leur format d'origine sans perte d'informations.

V

validation de chaîne : Validation des signatures de toutes les autorités de certification représentées dans la hiérarchie de sécurisation ayant contribué à la délivrance d'un certificat. Par exemple, si une autorité de certification a reçu un certificat de droit de signature de la part d'une autre AC, les deux signatures sont validées au cours de la validation du certificat soumis par l'utilisateur.

W

World Wide Web (WWW) : Egalement appelé la Toile. Division de l'Internet dans laquelle existe un réseau de connexions entre des ordinateurs contenant des équipements et ressources multimédia. Ces équipements fournissent des informations et permettent d'établir des liaisons avec d'autres ordinateurs sur le WWW et sur l'Internet. Les ressources du WWW sont accessibles au moyen d'un navigateur Web.