IBM Security Directory Server
Version 6.3.1.5

Guide d'installation et de configuration

SC11-6792-02

IBM Security Directory Server
Version 6.3.1.5

Guide d'installation et de configuration

SC11-6792-02

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 269.

Notice d'édition

Remarque : Cette édition concerne la version version 6.3.1.5 de *IBM Security Directory Server* **(référence 5724-J39) et toutes les versions et modifications suivantes sauf indication contraire dans les nouvelles éditions.**

Réf. US : SC27-2747-02

Compagnie IBM France
Direction Qualité
17, avenue de l'Europe
92275 Bois-Colombes Cedex

Table des matières

Avis aux lecteurs canadiens

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

Illustrations

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

Terminologie

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

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

Claviers

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

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

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

Nomenclature

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

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

Brevets

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

Assistance téléphonique

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

A propos de cette publication

IBM® Security Directory Server, précédemment IBM Tivoli Directory Server, est une implémentation IBM de Lightweight Directory Access Protocol pour les systèmes d'exploitation suivants :

- Microsoft Windows
- AIX
- Linux (System x, System z, System p et System i)
- Solaris
- Hewlett-Packard UNIX (HP-UX) (Itanium)

Le manuel IBM Security Directory ServerGuide d'installation et de configuration contient des informations sur l'installation, la configuration et la désinstallation d'IBM Security Directory Server. Il inclut aussi des informations sur la mise à niveau à partir d'une version précédente.

Accès aux publications et à la terminologie

La présente section contient :

- Une liste des publications contenues dans la «Bibliothèque IBM Security Directory Server».
- Des liens vers «Publications en ligne», à la page x.
- Un lien vers «Site Web de terminologie IBM», à la page xi.

Bibliothèque IBM Security Directory Server

Les documents suivants sont disponibles dans la bibliothèque IBM Security Directory Server :

- *IBM Security Directory Server version 6.3.1.5 - Présentation du produit*, GC27-6212-01

  Fournit des informations sur le produit IBM Security Directory Server, les nouvelles fonctions de l'édition actuelle et la configuration système requise.
- *IBM Security Directory Server version 6.3.1.5 - Guide de démarrage rapide*, GI11-9351-02

  Vous aide à commencer à utiliser IBM Security Directory Server. Inclut une courte description du produit, un diagramme d'architecture, ainsi qu'un lien vers le site Web de documentation du produit et des instructions d'installation.
- *IBM Security Directory Server version 6.3.1.5 - Guide d'installation et de configuration*, SC27-2747-02

  Contient des informations complètes sur l'installation, la configuration et la désinstallation d'IBM Security Directory Server. Inclut des informations sur la mise à niveau à partir d'une version antérieure d'IBM Security Directory Server.
- *IBM Security Directory Server version 6.3.1.5 - Guide d'administration*, SC27-2749-02

  Contient des instructions pour effectuer des tâches d'administration à l'aide de l'outil d'administration Web et de la ligne de commande.
- *IBM Security Directory Server version 6.3.1.5 - Guide de génération de rapports*, SC27-6531-00

  Contient des informations sur les outils et logiciels de création de rapports IBM Security Directory Server.

- *IBM Security Directory Server version 6.3.1.5 - Guide de référence des commandes*, SC27-2753-02

  Décrit la syntaxe et l'utilisation des utilitaires de ligne de commande fournis avec IBM Security Directory Server.
- *IBM Security Directory Server version 6.3.1.5 - Guide de référence des plug-ins de serveur*, SC27-2750-02

  Contient des informations sur l'écriture de modules d'extension du serveur.
- *IBM Security Directory Server version 6.3.1.5 - Guide de référence de programmation*, SC27-2754-02

  Contient des informations sur l'écriture d'applications client LDAP (Lightweight Directory Access Protocol) en langages C et Java™.
- *IBM Security Directory Server version 6.3.1.5 - Guide d'optimisation des performances et de planification de la capacité*, SC27-2748-02

  Contient des informations sur l'optimisation des performances du serveur d'annuaire. Décrit les exigences liées au disque et autres besoins matériels pour les répertoires de différentes tailles et différents débits de lecture/écriture. Présente plusieurs scénarios d'exécution pour chacun des niveaux de répertoire ainsi que le disque et la mémoire utilisés. Indique également plusieurs règles empiriques.
- *IBM Security Directory Server version 6.3.1.5 - Guide de dépannage*, GC27-2752-02

  Contient des informations sur les incidents potentiels et sur les actions correctives à effectuer avant de contacter le service de support logiciel IBM.
- *IBM Security Directory Server version 6.3.1.5 - Guide de référence des messages d'erreur*, GC27-2751-02

  Contient la liste de tous les messages d'avertissement et d'erreur associés à IBM Security Directory Server.

Publications en ligne

IBM présente ses publications lors du lancement du produit et lorsque ces documents sont mis à jour aux emplacements suivants :

Site Web de documentation IBM Security Directory Server
Le site http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/welcome.htm affiche la page d'accueil de la documentation de ce produit.

IBM Security Systems Documentation Central et page d'accueil
IBM Security Systems Documentation Central fournit une liste alphabétique de toutes les documentations produit des systèmes de sécurité IBM. Vous pouvez également trouver des liens vers la documentation produit pour des versions spécifiques de chaque produit.

La page Welcome to IBM Security Systems documentation propose une introduction, des liens ainsi que des informations générales sur la documentation des systèmes de sécurité IBM.

IBM Publications Center
Le site http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.wss comporte des fonctions de recherche personnalisée vous permettant de trouver toutes les publications IBM dont vous avez besoin.

Site Web de terminologie IBM

Le site Web de terminologie IBM regroupe la terminologie des bibliothèques de logiciels en un seul emplacement. Vous pouvez y accéder à l'adresse http://www.ibm.com/software/globalization/terminology.

Accessibilité

Les fonctions d'accessibilité permettent aux utilisateurs souffrant d'un handicap physique, comme une mobilité réduite ou une déficience visuelle, de pouvoir utiliser correctement les produits logiciels. Sur ce produit, vous pouvez utiliser les technologies d'assistance pour entendre des sons et naviguer dans l'interface. Vous pouvez également utiliser le clavier au lieu de la souris pour accéder à toutes les fonctions de l'interface graphique utilisateur.

Pour plus d'informations, consultez la section relative à l'accessibilité dans la *Présentation d'IBM Security Directory Server*.

Formation technique

Pour plus d'informations sur la formation technique, accédez au site Web IBM Education à l'adresse http://www.ibm.com/software/tivoli/education.

Informations relatives au support

Le support IBM vous offre une assistance dans la résolution de vos problèmes de codes, de routine, d'installation de courte durée et de vos questions liées à l'utilisation. Vous pouvez accéder directement au site de support logiciel IBM à l'adresse http://www.ibm.com/software/support/probsub.html.

Le document *IBM Security Directory Server Troubleshooting Guide* contient les détails suivants :

- Les informations à collecter avant de contacter le service de support IBM.
- Les diverses méthodes permettant de contacter le support IBM.
- Le mode d'utilisation d'IBM Support Assistant.
- Les instructions et ressources d'identification de problème permettant d'isoler et résoudre le problème vous-même.

Remarque : L'onglet **Community and Support** dans le centre de documentation du produit peut fournir des ressources de support supplémentaires.

Déclaration des bonnes pratiques de sécurité

La sécurité des systèmes informatiques implique la protection des systèmes et des informations via la prévention, la détection et la réponse aux accès incorrects depuis l'intérieur et l'extérieur de votre entreprise. Un accès non autorisé peut se traduire par la modification, la destruction ou une utilisation inadéquate ou malveillante de vos systèmes, y compris l'utilisation de ces derniers pour attaquer d'autres systèmes. Aucun système ou produit informatique ne doit être considéré comme étant complètement sécurisé et aucun produit, service ou mesure de sécurité ne peut être entièrement efficace contre une utilisation ou un accès non autorisé. Les systèmes, les produits et les services IBM sont conçus pour s'intégrer à une approche de sécurité complète, qui implique nécessairement des procédures opérationnelles supplémentaires, et peuvent avoir besoin d'autres systèmes, produit ou services pour optimiser leur efficacité. IBM NE GARANTIT PAS QUE TOUS

LES SYSTEMES, PRODUITS OU SERVICES SONT A L'ABRI DES CONDUITES MALVEILLANTES OU ILLICITES DE TIERS OU QU'ILS PROTEGERONT VOTRE ENTREPRISE CONTRE CELLES-CI.

Chapitre 1. Planification de l'installation

Avant d'installer IBM Security Directory Server, vous devez choisir notamment les composants matériels et logiciels, les rôles utilisateur et la sécurité de l'environnement du serveur d'annuaire.

Feuille de route de la planification

Aidez-vous de la liste de contrôle figurant dans cette section pour installer un serveur.

Si vous effectuez une mise à niveau à partir d'une version précédente, n'utilisez pas cette liste de contrôle. Pour obtenir les instructions correspondantes, voir Chapitre 14, «Mise à niveau d'une instance d'une version précédente», à la page 91.

Pour installer le serveur :

1. Lisez la présentation succincte pour comprendre les composants IBM Security Directory Server que vous allez installer :
2. Vérifiez que vous possédez la configuration matérielle et logicielle minimale requise. Pour plus d'informations sur les conditions requises, voir «Espace disque requis», à la page 3.
3. Installez IBM Security Directory Server à l'aide d'IBM Installation Manager.
4. Sur les systèmes Windows, si le système redémarre, connectez-vous avec l'ID utilisateur que vous avez utilisé pour vous connecter lors de l'installation.
5. Utilisez l'outil d'administration d'instance pour gérer les instances de serveur d'annuaire.
6. Si nécessaire, vérifiez l'installation et la configuration en chargeant l'exemple de fichier LDIF dans la base de données. Pour plus d'informations, voir Annexe B, «Chargement d'une base de données exemple et démarrage du serveur», à la page 255.
7. Démarrez l'instance de serveur d'annuaire et, si vous avez installé l'outil d'administration Web, démarrez-le.
8. Voir la section Administration de la documentation IBM Security Directory Server, pour plus d'informations sur la configuration et l'utilisation du serveur et de l'outil d'administration Web.

Si vous avez installé un serveur d'annuaire complet et que vous souhaitez planifier l'organisation de la base de données, pour plus d'informations, voir «Planification de la configuration», à la page 129.

Chapitre 2. Présentation de l'installation

Vous devez préparer votre ordinateur et choisir le mode d'installation d'IBM Security Directory Server qui s'applique à votre environnement.

Le programme d'installation basé sur IBM Installation Manager est fourni pour Windows, Linux64 et AIX. Des installateurs d'encapsuleur sont disponibles pour IBM Security Directory Server sur les systèmes UNIX, sauf Linux 64 et AIX. Avec le programme d'installation basé sur Installation Manager, l'installation par l'interface graphique et l'installation silencieuse sont prises en charge pour IBM Security Directory Server V6.3.1.

Espace disque requis

Pour que l'installation d'IBM Security Directory Server et des logiciels corequis réussisse, l'ordinateur doit contenir l'espace disque nécessaire. Cet espace varie en fonction du système d'exploitation, des fonctions IBM Security Directory Server et des corequis dont vous sélectionnez l'installation.

Espace disque requis sous Windows

Remarque : Si vous sélectionnez la fonction serveur proxy ou serveur d'annuaire complet, ajoutez une fois la taille du SDK client, du kit JDK (IBM Java Development Kit) et du clientJava.

Tableau 1. Espace disque requis pour les fonctions IBM Security Directory Server et les logiciels corequis sous Windows

Fonction installable	**Espace disque requis pour l'installation (en Mo)**
SDK client	25 Mo
IBM Java Development Kit	200 Mo
Client Java	124 Mo
Outil d'administration Web déployé (comprend Embedded WebSphere Application Server et l'outil d'administration Web déployé dans Embedded WebSphere Application Server)	440 Mo
Déploiement de l'outil d'administration Web dans une instance existante d'Embedded WebSphere Application Server ou de WebSphere Application Server	260 Mo
Serveur de base	23 Mo
Serveur proxy (n'oubliez pas d'ajouter la taille du client SDK, du client Java et du serveur de base.)	40 Mo
Serveur d'annuaire complet (n'oubliez pas d'ajouter la taille du client SDK, du client Java et du serveur de base.)	8 Mo
IBM DB2	763 Mo
IBM Global Security Kit	11 Mo

Espace disque requis sous AIX

Remarque : Si vous sélectionnez la fonction serveur proxy ou serveur d'annuaire complet, ajoutez une fois la taille du SDK client, du kit JDK (IBM Java Development Kit) et du clientJava.

Tableau 2. Espace disque requis pour les fonctions IBM Security Directory Server et les logiciels corequis sous AIX

Fonction installable	Espace disque requis pour l'installation (en Mo)
SDK client	8 Mo
IBM Java Development Kit	200 Mo
Client Java	91 Mo
Outil d'administration Web déployé (comprend Embedded WebSphere Application Server et l'outil d'administration Web déployé dans Embedded WebSphere Application Server)	443 Mo
Déploiement de l'outil d'administration Web dans une instance existante d'Embedded WebSphere Application Server ou de WebSphere Application Server	500 Mo
Outil d'administration Web SSL	51 Mo
Serveur de base	39 Mo
Serveur proxy (n'oubliez pas d'ajouter la taille du client SDK, du client Java et du serveur de base.)	4 Mo
Serveur d'annuaire complet (n'oubliez pas d'ajouter la taille du client SDK, du client Java et du serveur de base.)	12 Mo
IBM DB2	1250 Mo
IBM Global Security Kit	16 Mo

Espace disque requis sous Linux

Remarque : Si vous sélectionnez la fonction serveur proxy ou serveur d'annuaire complet, ajoutez une fois la taille du SDK client, du kit JDK (IBM Java Development Kit) et du clientJava.

Tableau 3. Espace disque requis pour les fonctions IBM Security Directory Server et les logiciels corequis sous Linux

Fonction installable	Espace disque requis pour l'installation (en Mo)
SDK client	9 Mo
IBM Java Development Kit	200 Mo
Client Java	166 Mo
Outil d'administration Web déployé (comprend Embedded WebSphere Application Server et l'outil d'administration Web déployé dans Embedded WebSphere Application Server)	443 Mo

Tableau 3. Espace disque requis pour les fonctions IBM Security Directory Server et les logiciels corequis sous Linux (suite)

Fonction installable	Espace disque requis pour l'installation (en Mo)
Déploiement de l'outil d'administration Web dans une instance existante d'Embedded WebSphere Application Server ou de WebSphere Application Server	375 Mo
Serveur de base	32 Mo
Serveur proxy (n'oubliez pas d'ajouter la taille du client SDK, du client Java et du serveur de base.)	40 Mo
Serveur d'annuaire complet (n'oubliez pas d'ajouter la taille du client SDK, du client Java et du serveur de base.)	8 Mo
IBM DB2 (System x Linux)	460 Mo
IBM DB2 (System zLinux)	670 Mo
IBM DB2 (System i et System p Linux)	520 Mo
IBM DB2 (AMD64/EM64T Linux)	1300 Mo
IBM Global Security Kit	40 Mo

Remarque : (Applicable aux programmes d'installation basée sur Installation Manager) Dans le répertoire des ressources partagées, 200 Mo d'espace disque sont nécessaires. Dans le répertoire d'installation d'IBM Security Directory Server, 200 Mo supplémentaires sont requis.

Espace disque requis pour le répertoire temporaire par défaut du système : Si l'installation de DB2 est sélectionnée, 2048 Mo + 500 Mo d'espace disponible dans le répertoire temporaire sont nécessaire. Sans DB2, 500 Mo d'espace disponible sont nécessaires dans le répertoire temporaire.

Espace disque requis sous Solaris

Remarque : Si vous sélectionnez la fonction serveur ou serveur proxy, ajoutez une fois la taille du client C, du kit JDK (IBM Java Development Kit) et du clientJava.

Tableau 4. Espace disque requis pour les fonctions IBM Security Directory Server et les logiciels corequis sous Solaris

Fonction installable	Espace disque requis pour l'installation (en Mo)	Remarques
Client C	11 Mo	
IBM Java Development Kit		
Client Java	145 Mo	
Serveur	47 Mo	Ajoutez la taille du client C et du client Java
Serveur proxy	40 Mo	Ajoutez la taille du client C et du client Java

Tableau 4. Espace disque requis pour les fonctions IBM Security Directory Server et les logiciels corequis sous Solaris (suite)

Fonction installable	Espace disque requis pour l'installation (en Mo)	Remarques
Outil d'administration Web	470 Mo	Comprend Embedded WebSphere Application Server et l'outil d'administration Web déployé dans Embedded WebSphere Application Server
IBM DB2	1155 Mo	
IBM Global Security Kit	34 Mo	

Espace disque requis sous HP-UX

Tableau 5. Espace disque requis pour les fonctions IBM Security Directory Server et les logiciels corequis sous HP-UX

Fonction installable	Espace disque requis pour l'installation (en Mo)
Client C	26 Mo
IBM Java Development Kit	
Client Java	172 Mo
IBM Global Security Kit	41 Mo

Préparation du support d'installation

Le module du produit IBM Security Directory Server contient IBM Security Directory Server, les logiciels corequis et le programme d'installation. Le support d'installation est disponible sur les DVD d'installation ou sur le site Web Passport Advantage.

IBM Security Directory Server est disponible sous trois types de fichiers : `.zip`, `.tar` et `.iso`. Un fichier `.iso` contient plusieurs fichiers qui correspondent à plusieurs fichiers `.zip` ou `.tar`.

Tableau 6. Le produit IBM Security Directory Server est disponible au format suivant sur différents systèmes d'exploitation

AIX, Linux, Solaris et Windows	AIX, Linux, Solaris et HP-UX	Windows
Image ISO (fichier `.iso`)	Fichiers d'archivage sur bande (fichiers `.tar`)	Fichiers d'archive (fichiers `.zip`)

Pour utiliser un DVD comme support d'installation, effectuez l'une des tâches ci-après.

- Créez une image du DVD à partir de l'image du produit IBM Security Directory Server correspondant à votre système d'exploitation.
- Stockez l'image du produit IBM Security Directory Server sur le disque dur de l'ordinateur, et montez-celui-ci si nécessaire.

Lorsque vous téléchargez les fichiers d'archive du produit, vous devez vérifier que les conditions ci-après sont remplies.

1. Téléchargez tous les fichiers d'archive requis dans le même répertoire. Evitez de télécharger les fichiers d'archive dans un chemin de répertoire qui contient des espaces.
2. Décompressez tous les fichiers dans le même répertoire, dont le chemin ne contient pas d'espaces. Le chemin du répertoire du fichier installable ne doit pas contenir d'espaces.

Pour télécharger le produit IBM Security Directory Server à partir du site Passport Advantage, voir «Téléchargement du logiciel à partir de Passport Advantage».

Lorsque le support d'installation est prêt, vérifiez que la configuration logicielle requise correspondant au système d'exploitation est prête. Voir «Configuration requise pour l'installation», à la page 15.

Téléchargement du logiciel à partir de Passport Advantage

Avant d'installer IBM Security Directory Server, vous devez télécharger le logiciel depuis IBM Passport Advantage.

Avant de commencer

Vous devez vous enregistrer auprès d'IBM Passport Advantage, et obtenir un numéro de compte client et un mot de passe pour y accéder.

Procédure

1. Accédez au site Web IBM Passport Advantage à l'adresse http://www.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm.
2. Cliquez sur **Customer sign in**.
3. Dans la zone **IBM ID**, entrez votre ID IBM.
4. Dans la zone **Password**, entrez votre mot de passe.
5. Cliquez sur **Sign in**.
6. Suivez les instructions pour télécharger le logiciel IBM Security Directory Server.

Arborescence des fichiers téléchargés

Après avoir téléchargé les fichiers d'installation d'IBM Security Directory Server, vous devez vérifier l'arborescence des fichiers téléchargés.

Arborescence des modules Windows

Les noms de fichier des modules de Security Directory Server 6.3.1 destinés à Windows sont les suivants :

Image de DVD : sds631-win.iso
Fichiers .zip :
– sds631-win-base.zip (Security Directory Server 6.3.1 client et serveur)
– sds631-win-db2.zip (DB2 V9.7)
– sds631-win-ewas.zip (Embedded WebSphere Application Server 7.0.0.29)
– sds631-win-gskit.zip (GSKit 8.0)
– sds631-win-jdk.zip (IBM Java Development Kit)
– sds631-win-IM.zip (IBM Installation Manager)

Une fois le DVD créé ou les fichiers .zip décompressés, l'arborescence est celle ci-après.

\sdsV6.3.1 (répertoire principal des fichiers décompressés)
– ibm_gskit\ (GSKit)
– license\ (licences de Security Directory Server et des autres produits fournis)
– quickstart\ (Guide de démarrage rapide dans différentes langues,
y compris l'anglais)
– entitlement\ (fichiers de droits d'utilisation du serveur proxy)
– entitlement.txt
– tools\ (outils, y compris migbkup)
– migbkup.bat
– ibm_db2_32bit\ (DB2)
– ibm_db2_64bit\ (DB2)
– ibm_ewas_32bit\ (Embedded WebSphere Application Server)
– ibm_ewas_64bit\ (Embedded WebSphere Application Server)
– ibm_im_32bit\ (IBM Installation Manager)
– ibm_im_64bit\ (IBM Installation Manager)
– ibm_jdk\ (IBM Java Development Kit)
– ibm_sds\ (fichiers du programme d'installation)
– atoc
– files
– native
– Offerings
– plugins
– ShareableEntities
– build.properties
– repository.config
– repository.xml
– launchpad\
– SilentInstallScripts\ (fichiers de réponses destinés à l'installation silencieuse)
– autorun.inf
– imLauncherWindows.bat
– launchpad.exe
– launchpad.ini
– launchpad64.exe
– launchpad64.ini
– sds_install.xml
– write_sds_path.bat

Module client seul pour Windows

Fichier .zip :
– sds631-win-client.zip (Security Directory Server 6.3.1 client)

Une fois le fichier .zip décompressé, l'arborescence est celle ci-après.

\sdsV6.3.1 (répertoire principal des fichiers décompressés)
– ibm_gskit\ (GSKit 8)
– jdk\ (IBM Java Development Kit)
– ibm_im_32bit (IBM Installation Manager)
– ibm_im_64bit (IBM Installation Manager)
– ibm_sds\ (fichiers du programme d'installation)
– launchpad\
– SilentInstallScripts\
– autorun.inf

– license\ (licences de Security Directory Server et des autres produits fournis)
– quickstart\ (Guide de démarrage rapide dans différentes langues,
y compris l'anglais)
– ibm_im_32bit\ (IBM Installation Manager)
– ibm_im_64bit\ (IBM Installation Manager)
– imLauncherWindows.bat
– launchpad.exe
– launchpad.ini
– launchpad64.exe
– launchpad64.ini
– sds_install.xml
– write_sds_path.bat

Arborescence des modules serveur pour AIX

Les noms de fichier des modules de Security Directory Server 6.3.1 destinés à AIX sont les suivants :

Image de DVD : sds631-aix-ppc64.iso
Fichiers .tar :
– tds63-aix-ppc64-base.tar (Security Directory Server 6.3.1 client et serveur)
– sds631-aix-ppc64-db2.tar (DB2 V9.7)
– sds631-aix-ppc64-ewas.tar (Embedded WebSphere Application Server 7.0.0.29)
– sds631-aix-ppc64-gskit.tar (GSKit 8.0)
– sds631-aix-ppc64-jdk.tar (IBM Java Development Kit)
– sds631-aix-ppc64-IM.tar (IBM Installation Manager)

Une fois le DVD créé ou les fichiers .tar décompressés, l'arborescence est celle ci-après.

/sdsV6.3.1 (répertoire principal des fichiers tar décompressés)
– license/ (licences de Security Directory Server et des autres produits fournis)
– quickstart/ (Guide de démarrage rapide dans différentes langues,
y compris l'anglais)
– ibm_im (IBM Installation Manager)
– ibm_db2/ (DB2)
– ibm_ewas/ (Embedded WebSphere Application Server)
– ibm_gskit/ (GSKit 8)
– ibm_jdk/ (IBM Java Development Kit)
– ibm_sds/ (fichiers du programme d'installation)
– atoc/
– files/
– native/
– Offerings/
– plugins/
– ShareableEntities
– build.properties
– repository.config
– repository.xml

– tools/ (outils, y compris migbkup)
– launchpad/
– SilentInstallScripts/
– launchpad.sh
– sds_install.xml

– write_sds_path.sh
– entitlement/ (fichiers de droits d'utilisation du serveur proxy)
– native / (modules natifs)

Module client seul pour AIX

Fichier .zip :
– sds631-aix-ppc64-client.tar (Security Directory Server 6.3.1 client)

Une fois le fichier .zip décompressé, l'arborescence est celle ci-après.

\sdsV6.3.1 (répertoire principal des fichiers décompressés)
– ibm_gskit\ (GSKit 8)
– ibm_jdk\ (IBM Java Development Kit)
– ibm_im\ (IBM Installation Manager)
– ibm_sds\ (fichiers du programme d'installation)
– launchpad\
– SilentInstallScripts\
– autorun.inf
– license\ (licences de Security Directory Server et des autres produits fournis)
– quickstart\ (Guide de démarrage rapide dans différentes langues,
y compris l'anglais)
– ibm_im\ (IBM Installation Manager)
– imLauncherWindows.bat
– launchpad.exe
– launchpad.ini
– sds_install.xml
– write_sds_path.bat

Arborescence des modules serveur pour Linux x86_64

Les noms de fichier des modules de Security Directory Server 6.3.1 destinés à Linux x86_64 sont les suivants :

Image de DVD : sds631-linux-x86-64.iso
Fichiers .tar :
– sds631-linux-x86-64-base.tar (IBM Security Directory Server 6.3.1 client et serveur)
– sds631-linux-x86-64-IM.tar (IBM Installation Manager)
– sds631-linux-x86-64-gskit.tar (GSKit 8)
– sds631-linux-x86-64-db2.tar (DB2 vV9.7)
– sds631-linux-x86-64-ewas.tar (Embedded WebSphere Application Server 7.0.0.29)
– sds631-linux-x86-64-jdk.tar (IBM Java Development Kit)

Une fois le DVD créé ou les fichiers .tar décompressés, l'arborescence est celle ci-après.

/sdsV6.3.1 (répertoire principal des fichiers tar décompressés)
– license/ (licences de Security Directory Server et des autres produits fournis)
– quickstart/ (Guide de démarrage rapide dans différentes langues,
y compris l'anglais)
– ibm_im (IBM Installation Manager)
– ibm_db2/ (DB2)
– ibm_ewas/ (Embedded WebSphere Application Server)
– ibm_gskit/ (GSKit 8)
– ibm_jdk/ (IBM Java Development Kit)
– ibm_sds/ (fichiers du programme d'installation)

– atoc/
– files/
– native/
– Offerings/
– plugins/
– ShareableEntities
– build.properties
– repository.config
– repository.xml

– tools/ (outils, y compris migbkup)
– launchpad/
– SilentInstallScripts/
– launchpad.sh
– sds_install.xml
– write_sds_path.sh
– entitlement/ (fichiers de droits d'utilisation du serveur proxy)
– native/ (module natif)

Module client seul pour Linux x86_64

Fichier .zip :
– sds631-linux-x86-64-client.tar (Security Directory Server 6.3.1 client)

Une fois le fichier .zip décompressé, l'arborescence est celle ci-après.

\sdsV6.3.1 (répertoire principal des fichiers décompressés)
– ibm_jdk\ (IBM Java Development Kit)
– ibm_im (IBM Installation Manager)
– ibm_sds\ (fichiers du programme d'installation)
– launchpad\
– SilentInstallScripts\
– autorun.inf
– license\ (licences de Security Directory Server et des autres produits fournis)
– quickstart\ (Guide de démarrage rapide dans différentes langues,
y compris l'anglais)
– ibm_im\ (IBM Installation Manager)
– imLauncherWindows.bat
– launchpad.exe
– launchpad.ini
– sds_install.xml
– write_sds_path.bat

Arborescence des modules serveur pour Linux x86

Les noms de fichier des modules de Security Directory Server 6.3.1 destinés à Linux x86 sont les suivants :

Image de DVD : sds631-linux-x86.iso
Fichiers .tar :
– sds631-linux-x86-base.tar (IBM Security Directory Server 6.3.1 client et serveur)
– sds631-linux-x86-gskit.tar (GSKit 8)
– sds631-linux-x86-db2.tar (DB2 v9.7)
– sds631-linux-x86-ewas.tar (Embedded WebSphere Application Server 7.0.0.29)
– sds631-linux-x86-jdk.tar (IBM Java Development Kit)

Une fois le DVD créé ou les fichiers .tar décompressés, l'arborescence est celle ci-après.

/sdsV6.3.1 (répertoire principal des fichiers tar décompressés)
– appsrv/ (embedded WebSphere Application Server)
– db2 (DB2)
– gskit/ (GSKit 8)
– jdk/ (IBM Java Development Kit)
– ids_detectGskitVersion
– idsinstall_i
– idsNativeInstall.sh
– images/ (images natives)
– license (licences de Security Directory Server et des autres produits fournis)
– responseFile.txt (fichier de réponses)

Module client seul pour Linux x86

Fichier .zip :
– sds631-linux-x86-client.tar (Security Directory Server 6.3.1 client)

Une fois le fichier .zip décompressé, l'arborescence est celle ci-après.

\sdsV6.3.1 (répertoire principal des fichiers décompressés)
– gskit/ (GSKit 8)
– image/
– license/ (licences de Security Directory Server et des autres produits fournis)
– jdk (IBM Java Development Kit)

Arborescence des modules serveur pour Linux ppc

Les noms de fichier des modules de Security Directory Server 6.3.1 destinés à Linux ppc sont les suivants :

Image de DVD : sds631-linux-ppc64.iso
Fichiers .tar :
– sds631-linux-ppc64-base.tar (IBM Security Directory Server 6.3.1 client et serveur)
– sds631-linux-ppc64-gskit.tar (GSKit 8)
– sds631-linux-ppc64-db2.tar (DB2 V9.7)
– sds631-linux-ppc64-ewas.tar (Embedded WebSphere Application Server 7.0.0.29)
– sds631-linux-ppc64-jdk.tar (IBM Java Development Kit)

Une fois le DVD créé ou les fichiers .tar décompressés, l'arborescence est celle ci-après.

/sdsV6.3.1 (répertoire principal des fichiers tar décompressés)
– appsrv/ (embedded WebSphere Application Server)
– db2 (DB2)
– gskit/ (GSKit 8)
– jdk/ (IBM Java Development Kit)
– ids_detectGskitVersion
– idsinstall_i
– idsNativeInstall.sh
– images/ (images natives)
– license (licences de Security Directory Server et des autres produits fournis)
– responseFile.txt (fichier de réponses)

Module client seul pour Linux ppc

Fichier .zip :
– sds631-linux-ppc64-client.tar (Security Directory Server 6.3.1 client)

Une fois le fichier .zip décompressé, l'arborescence est celle ci-après.

\sdsV6.3.1 (répertoire principal des fichiers décompressés)
– gskit/ (GSKit 8)
– image/
– license/ (licences de Security Directory Server et des autres produits fournis)
– jdk (IBM Java Development Kit)

Arborescence des modules serveur pour Linux s390

Les noms de fichier des modules de Security Directory Server 6.3.1 destinés à Linux s390 sont les suivants :

Image de DVD : sds631-linux-s390x.iso
Fichiers .tar :
– sds631-linux-s390x-base.tar (IBM Security Directory Server 6.3.1 client et serveur)
– sds631-linux-s390x-gskit.tar (GSKit 8)
– sds631-linux-s390x-db2.tar (DB2 V9.7)
– sds631-linux-s390x-ewas.tar (Embedded WebSphere Application Server 7.0.0.29)
– sds631-linux-s390x-jdk.tar (IBM Java Development Kit)

Une fois le DVD créé ou les fichiers .tar décompressés, l'arborescence est celle ci-après.

/sdsV6.3.1 (répertoire principal des fichiers tar décompressés)
– appsrv/ (embedded WebSphere Application Server)
– db2 (DB2)
– gskit/ (GSKit 8)
– jdk/ (IBM Java Development Kit)
– ids_detectGskitVersion
– idsinstall_i
– idsNativeInstall.sh
– images/ (images natives)
– license (licences de Security Directory Server et des autres produits fournis)
– responseFile.txt (fichier de réponses)

Module client seul pour Linux s390

Fichier .zip :
– sds631-linux-s390x-client.tar (Security Directory Server 6.3.1 client)

Une fois le fichier .zip décompressé, l'arborescence est celle ci-après.

\sdsV6.3.1 (répertoire principal des fichiers décompressés)
– gskit/ (GSKit 8)
– image/
– license/ (licences de Security Directory Server et des autres produits fournis)
– jdk (IBM Java Development Kit)

Arborescence des modules serveur pour Solaris x86_64

Les noms de fichier des modules de Security Directory Server 6.3.1 destinés à Solaris x86_64 sont les suivants :

Image de DVD : sds631-solaris-x86-64.iso
Fichiers .tar :
– sds631-solaris-x86-64-base.tar (IBM Security Directory Server 6.3.1 client et serveur)
– sds631-solaris-x86-64-gskit.tar (GSKit 8)
– sds631-solaris-x86-64-db2.tar(DB2 v9.7)
– sds631-solaris-x86-64-ewas.tar (Embedded WebSphere Application Server 7.0.0.29)
– sds631-solaris-x86-64-jdk.tar (IBM Java Development Kit)

Une fois le DVD créé ou les fichiers .tar décompressés, l'arborescence est celle ci-après.

/sdsV6.3.1 (répertoire principal des fichiers tar décompressés)
– appsrv/ (embedded WebSphere Application Server)
– db2 (DB2)
– gskit/ (GSKit 8)
– jdk/ (IBM Java Development Kit)
– ids_detectGskitVersion
– idsinstall_i
– idsNativeInstall.sh
– images/ (images natives)
– license (licences de Security Directory Server et des autres produits fournis)
– responseFile.txt (fichier de réponses)

Module client seul pour Solaris x86_64

Fichier .zip :
– sds631-solaris-x86-64-client.tar (Security Directory Server 6.3.1 client)

Une fois le fichier .zip décompressé, l'arborescence est celle ci-après.

\sdsV6.3.1 (répertoire principal des fichiers décompressés)
– gskit/ (GSKit 8)
– image/
– license/ (licences de Security Directory Server et des autres produits fournis)
– jdk (IBM Java Development Kit)

Arborescence des modules serveur Solaris sparc

Les noms de fichier des modules de Security Directory Server 6.3.1 destinés à Solaris sparc sont les suivants :

Image de DVD :
Fichiers .tar :
– sds631-solaris-sparc.iso
– sds631-solaris-sparc-base.tar (IBM Security Directory Server 6.3.1 client et serveur)
– sds631-solaris-sparc-gskit.tar (GSKit 8)
– sds631-solaris-sparc-db2.tar (DB2 v9.7)
– sds631-solaris-sparc-ewas.tar (Embedded WebSphere Application Server 7.0.0.29)
– sds631-solaris-sparc-jdk.tar (IBM Java Development Kit)

Une fois le DVD créé ou les fichiers .tar décompressés, l'arborescence est celle ci-après.

/sdsV6.3.1 (répertoire principal des fichiers tar décompressés)
– appsrv/ (embedded WebSphere Application Server)
– db2 (DB2)
– gskit/ (GSKit 8)
– jdk/ (IBM Java Development Kit)
– ids_detectGskitVersion
– idsinstall_i
– idsNativeInstall.sh
– images/ (images natives)
– license (licences de Security Directory Server et des autres produits fournis)
– responseFile.txt (fichier de réponses)

Module client seul pour Solaris Sparc

Fichier .zip :
– sds631-solaris-sparc-client.tar (Security Directory Server 6.3.1 client)

Une fois le fichier .zip décompressé, l'arborescence est celle ci-après.

\sdsV6.3.1 (répertoire principal des fichiers décompressés)
– gskit/ (GSKit 8)
– image/
– license/ (licences de Security Directory Server et des autres produits fournis)
– jdk (IBM Java Development Kit)

Configuration requise pour l'installation

L'installation d'IBM Security Directory Server et des logiciels corequis peut nécessiter l'installation préalable d'autres logiciels sur l'ordinateur. Ces logiciels doivent être installés avant IBM Security Directory Server et les logiciels corequis.

Modules prérequis pour différents systèmes d'exploitation

Vous devez mettre à jour votre ordinateur à l'aide des modules qui sont requis pour l'installation d'IBM Security Directory Server et des produits corequis.

Le shell Korn est requis sur les systèmes d'exploitation AIX, Linux, Solaris et HP-UX (Itanium). Sur SuSE Linux Enterprise Server, `PDKSH` est requis.

Les modules suivants sont prérequis pour l'installation d'IBM Security Directory Server sur les systèmes d'exploitation suivants :

AIX Pour l'installation des modules rpm sous AIX, téléchargez le gestionnaire de module `rpm` pour les systèmes AIX à partir du sire Web ftp://public.dhe.ibm.com/aix/freeSoftware/aixtoolbox/INSTALLP/ppc/rpm.rte.

Tableau 7. Modules prérequis pour les systèmes d'exploitation AIX

Module	Raison	Adresse de téléchargement
Navigateur Web Mozilla Firefox pour AIX	Pour ouvrir le tableau de bord sous AIX, vous devez disposer d'une version compatible du navigateur.	Pour plus d'informations sur les navigateurs Web pour AIX, voir le site Web http://www.ibm.com/systems/power/software/aix/browsers/.
`gtk+ RPM (gtk2-2.10.6-4.aix5.2.ppc.rpm)`	Le nouveau système de fenêtrage d'Eclipse n'est plus basé sur `motif` mais sur `gtk` sur les systèmes d'exploitation UNIX. Pour AIX, la modification du système de fenêtrage Eclipse nécessite l'installation des bibliothèques `gtk` pour la prise en charge de l'interface. Pour IBM Installation Manager, l'interface est le mode assistant du fonctionnement.	Pour plus d'informations sur l'installation des bibliothèques `gtk`, voir la note technique Required gtk libraries for Installation Manager on AIX sur le site Web http://www.ibm.com/support/docview.wss?uid=swg21631478.
GNU `tar`	Pour décompresser les fichiers d'archive fournis avec IBM Security Directory Server sur les systèmes AIX, le programme d'archivage de fichiers GNU est requis. Vous devez définir le chemin du programme GNU `tar` avant le programme `tar` fourni avec le système d'exploitation. Le programme GNU `tar` est installé dans le répertoire `/opt/freeware/bin`, et le programme `tar` qui est fourni avec le système d'exploitation, dans le répertoire `/usr/bin`. Pour définir le chemin `/opt/freeware/bin`, exécutez la commande ci-après. `export PATH=/opt/freeware/bin:$PATH`.	Pour télécharger le fichier archive `tar` des GNU (`tar`), consultez le site web http://www.ibm.com/systems/power/software/aix/linux/toolbox/alpha.html .
Ensemble de fichiers `X11.adt.lib`	L'ensemble de fichiers `X11.adt.lib` est un prérequis pour l'installation des modules `idsldap.cltjava631` et `idsldap.webadmin631` sur les systèmes AIX.	
`xlC.rte 8.0.0.6` et `xlC.aix50.rte 8.0.0.6` ou niveaux ultérieurs	Les composants de l'environnement d'exécution IBM C++ pour AIX nécessitent les niveaux d'exécution `xlC.rte 8.0.0.6` et `xlC.aix50.rte 8.0.0.6` ou ultérieurs.	

Tableau 7. Modules prérequis pour les systèmes d'exploitation AIX (suite)

Module	Raison	Adresse de téléchargement
`bos.loc.iso.en_US 5.3.0.0`	IBM Security Directory Server version 6.3.1 nécessite le niveau `bos.loc.iso.en_US 5.3.0.0` de l'ensemble de fichiers de l'environnement local du système de base.	

Prérequis pour le client LDAP sur PowerPC LE

Pour exécuter le client IBM Security Directory Server sur PowerPC LE (Little Endian), vous devez installer IBM Advance Toolchain version 7.1 sur le système PowerPC LE.

Vous devez installer IBM Advance Toolchain version 7.1 si vous envisagez d'exécuter le client LDAP ou d'écrire vos propres clients en les liant aux bibliothèques fournies.

Pour télécharger et installer IBM Advanced Toolchain version 7.1 pour votre système d'exploitation, voir IBM Advance Toolchain documentation.

Utilisateur et groupe `idsldap`

Si vous sélectionnez l'installation de la fonction serveur ou serveur proxy, le programme d'installation peut créer l 'utilisateur et le groupe `idsldap`.

Le programme d'installation crée l'utilisateur et le groupe `idsldap` s'ils n'existent pas.

Remarque : Sous AIX, Linux et Solaris, l'installation à l'aide des utilitaires du système d'exploitation crée l'utilisateur `idsldap` si celui-ci n'existe pas. Cependant, si le répertoire `/home/idsldap` sous Linux et AIX, ou le répertoire `/export/home/idsldap` sous Solaris, existe déjà, la création de l'utilisateur `idsldap` peut s'avérer impossible. Vous devez donc vérifier que le répertoire de base de `idsldap` n'existe pas si l'utilisateur `idsldap` lui-même n'existe pas.

Si votre environnement nécessite que vous contrôliez l'utilisateur et le groupe `idsldap`, vous pouvez les créer avant l'installation. L'utilisateur et le groupe `idsldap` doivent répondre aux conditions ci-après.

- L'utilisateur `idsldap` doit être membre du groupe `idsldap`.
- Sous AIX, Linux et Solaris, l'utilisateur root doit être membre du groupe `idsldap`. Sous Windows, l'administrateur doit être membre du groupe `idsldap`.
- L'utilisateur `idsldap` doit posséder un répertoire de base.
- Sous AIX, Linux et Solaris, le shell par défaut de l'utilisateur `idsldap` doit être le shell Korn.
- L'utilisateur `idsldap` peut posséder un mot de passe, mais cela n'est pas obligatoire.
- L'utilisateur `idsldap` peut être le propriétaire de l'instance de serveur d'annuaire.

Vous devez vérifier que toutes ces conditions sont respectées avant de commencer l'installation d'IBM Security Directory Server. L'installation du serveur proxy peut échouer si l'utilisateur `idsldap` existe mais ne respecte pas ces conditions.

Remarque : Pour plus d'informations sur les conditions relatives aux ID utilisateur pour une instance, une instance d'annuaire ou le propriétaire d'une base de données, voir «Utilisateurs et groupes associés à une instance de serveur d'annuaire», à la page 125.

Vous pouvez utiliser l'outil d'administration d'instance pour créer des utilisateurs et des groupes lors de la création d'une instance de serveur d'annuaire. Vous pouvez également utiliser les utilitaires du système d'exploitation pour créer l'utilisateur et le groupe `idsldap` et les configurer correctement.

Exemples

Exécutez les utilitaires suivants du système d'exploitation pour créer le groupe `idsldap`, l'utilisateur `idsldap`, le mot de passe, et pour ajouter l'utilisateur root en tant que membre du groupe `idsldap`.

Sur les systèmes AIX :

Pour créer le groupe `idsldap`, entrez la commande ci-après.

```
mkgroup idsldap
```

Pour créer l'ID utilisateur `idsldap` en tant que membre du groupe `idsldap` et définir le shell Korn comme shell par défaut, entrez la commande ci-après.

```
mkuser pgrp=idsldap home=/home/idsldap shell=/bin/ksh idsldap
```

Pour définir le mot de passe de l'utilisateur `idsldap`, entrez la commande ci-après.

```
passwd idsldap
```

Pour ajouter l'ID utilisateur root en tant que membre du groupe `idsldap`, entrez la commande ci-après.

```
/usr/bin/chgrpmem -m + root idsldap
```

Sur les systèmes Linux :

Pour créer le groupe `idsldap`, entrez la commande ci-après.

```
groupadd idsldap
```

Pour créer l'ID utilisateur `idsldap` en tant que membre du groupe `idsldap` et définir le shell Korn comme shell par défaut, entrez la commande ci-après.

```
useradd -g idsldap -d /home/idsldap -m -s /bin/ksh  idsldap
```

Pour définir le mot de passe de l'utilisateur `idsldap`, entrez la commande ci-après.

```
passwd idsldap
```

Pour ajouter l'ID utilisateur root en tant que membre du groupe `idsldap`, entrez la commande ci-après.

```
usermod -G idsldap,groupes_root root
```

La commande `groups root` vous permet d'extraire les valeurs de *rootgroups* de l'ordinateur.

Sur les systèmes Solaris :

Pour créer le groupe `idsldap`, entrez la commande ci-après.

```
groupadd idsldap
```

Pour créer l'ID utilisateur idsldap en tant que membre du groupe idsldap et définir le shell Korn comme shell par défaut, entrez la commande ci-après.

```
useradd -g idsldap -d /export/home/idsldap -m -s /bin/ksh idsldap
```

Pour définir le mot de passe de l'utilisateur idsldap, entrez la commande ci-après.

```
passwd idsldap
```

Pour ajouter l'ID utilisateur root en tant que membre du groupe idsldap, entrez la commande ci-après.

```
usermod -G idsldap,root idsldap
```

Pour modifier l'ID utilisateur root afin que root soit membre du groupe idsldap, utilisez un outil approprié.

Pour plus d'informations sur les commandes d'ajout d'utilisateurs et de groupes, consultez la documentation du système d'exploitation.

Méthodes d'installation

Pour l'installation d'IBM Security Directory Server et des logiciels corequis, vous devez choisir la méthode la plus adaptée à votre environnement.

Vous pouvez utiliser les méthodes suivantes pour l'installation d'IBM Security Directory Server et des logiciels corequis :

- Installation avec IBM Installation Manager
- Installation avec les utilitaires de ligne de commande du système d'exploitation

ATTENTION :

- **Les installations sur un ordinateur donné doivent toujours être exécutées avec la même méthode. Vous devez réaliser l'installation d'IBM Security Directory Server avec IBM Installation Manager ou avec les utilitaires de ligne de commande du système d'exploitation, mais pas avec les deux. Si vous mélangez les deux modes d'installation, certains modules de fonction peuvent ne pas s'installer.**
- **Vous devez éviter d'installer manuellement DB2 et Embedded WebSphere Application Server dans le chemin d'installation par défaut utilisé par IBM Installation Manager. Cela pourrait faire échouer les opérations d'installation, de modification ou de désinstallation exécutées avec IBM Installation Manager. Pour plus d'informations sur le chemin d'installation par défaut, voir «Emplacements d'installation par défaut», à la page 27.**

Chapitre 3. Installation à l'aide d'IBM Installation Manager

IBM Installation Manager est un outil permettant d'effectuer l'installation et la maintenance d'IBM Security Directory Server et des logiciels corequis.

Présentation d'IBM Installation Manager

IBM Installation Manager est un assistant d'installation qui vous guide dans les procédures d'installation, de modification, de mise à jour, d'annulation ou de désinstallation des produits IBM. Il est capable d'utiliser des référentiels de produits distants ou locaux.

IBM Installation Manager permet aussi de gérer les applications et les modules IBM qu'il installe sur vos postes :

- Il conserve la trace des éléments installés
- Il identifie et vous montre les modules disponibles pour une installation
- Il vérifie les prérequis et les interdépendances

IBM Installation Manager comprend six assistants qui facilitent la gestion des modules :

- L'assistant **Installer** vous guide tout au long de la procédure d'installation. Vous pouvez installer plusieurs modules en même temps. Vous pouvez accepter les paramètres par défaut, ou créer une installation personnalisée lorsque c'est possible. Avant de procéder réellement à l'installation, vous pouvez consulter un récapitulatif complet des sélections que vous avez effectuées dans l'assistant.
- L'assistant **Mettre à jour** recherche les mises à jour disponibles pour les modules installés sur votre système. Les détails du contenu de la mise à jour sont fournis dans l'assistant. Vous pouvez choisir d'appliquer ou non une mise à jour.
- L'assistant **Modifier** vous aide à modifier certains éléments d'un module déjà installé. Au cours de la première installation du module, vous êtes amené à sélectionner les fonctions que vous souhaitez installer. Par la suite, si vous avez besoin d'autres fonctions, vous pourrez utiliser l'assistant de modification des modules pour les ajouter à votre module. Vous pouvez aussi supprimer des fonctions.
- L'assistant **Gérer les licences** vous aide à configurer les licences de vos modules. Utilisez-le pour changer votre licence d'évaluation en licence complète, pour mettre en place vos serveurs de licences flottantes et pour sélectionner le type de licence à utiliser pour chaque module.
- L'assistant **Rétrograder les modules** permet de revenir à une version précédente d'un module.
- L'assistant **Désinstaller** supprime un module de votre ordinateur. Vous pouvez désinstaller plusieurs modules à la fois.

Systèmes d'exploitation supportés

Vous pouvez utiliser IBM Installation Manager pour l'installation d'IBM Security Directory Server sous AIX (ppc64), Linux (AMD64/EM64T architecture) et Microsoft Windows.

La liste qui suit répertorie les versions des systèmes d'exploitation qui sont pris en charge pour l'installation d'IBM Security Directory Server à l'aide d'IBM Installation Manager.

Pour installer IBM Security Directory Server sur un système d'exploitation qui ne figure pas dans les sections suivantes :

1. Vérifiez si la version du système d'exploitation est compatible avec IBM Security Directory Server. Consultez la liste de tous les système d'exploitation pris en charge dans le manuel *Présentation d'IBM Security Directory Server*.
2. Si elle est prise en charge, vous pouvez installer IBM Security Directory Server à l'aide des utilitaires de ligne de commande du système d'exploitation.

AIX (ppc64)

- AIX version 6.1
- AIX version 7.1

Linux (AMD64/EM64T)

- Red Hat Enterprise Linux 5, Advanced Platform
- Red Hat Enterprise Linux 6
- SUSE Linux Enterprise Server 10
- SUSE Linux Enterprise Server 11

Microsoft Windows (x64)

- Microsoft Windows Server 2008 R2, Enterprise Edition
- Microsoft Windows Server 2008 R2, Standard Edition
- Microsoft Windows Server 2008, Enterprise Edition
- Microsoft Windows Server 2008, Standard Edition
- Microsoft Windows Server 2012, Standard Edition

Types des modules d'installation d'IBM Security Directory Server

Pour pouvoir choisir le module adéquant pour l'installation d'IBM Security Directory Server vous devez connaître les différents types disponibles.

Les types de module suivants sont disponibles pour l'installation d'IBM Security Directory Server avec IBM Installation Manager :

Tableau 8. Types des modules d'installation d'IBM Security Directory Server et fonctions installables

Toutes les fonctions	Fonctions dans le programme d'installation du produit complet	Fonctions dans le programme d'installation du client seul
IBM DB2	Oui	Non
IBM Global Security Kit	Oui	Oui
Client C	Oui	Oui
IBM Java Development Kit	Oui	Oui
Client Java	Oui	Oui
Serveur	Oui	Non
Serveur proxy	Oui	Non
outil d'administration Web	Oui	Non

Remarque : Si vous choisissez d'installer l'outil d'administration Web, IBM Installation Manager propose une option permettant d'installer Embedded WebSphere Application Server.

Instructions d'installation

Vous devez prendre en compte certaines restrictions avant de commencer l'installation d'IBM Security Directory Server à l'aide d'IBM Installation Manager.

Méthode d'installation

Lorsque vous installez IBM Security Directory Server, vous pouvez choisir de l'installer à l'aide d'IBM Installation Manager ou des utilitaires de ligne de commande du système d'exploitation. Toutes les installations et désinstallations à venir des modules, des fonctions et des groupes de correctifs d'IBM Security Directory Server sur le même système devront être effectuées par la même méthode. Par exemple, si vous installez IBM Security Directory Server à l'aide d'IBM Installation Manager, vous ne devez pas utiliser les utilitaires de ligne de commande pour installer des fonctions ou désinstaller le produit. Si vous le faites, la configuration d'IBM Security Directory Server peut être endommagée ou devenir inutilisable.

Version d'IBM Installation Manager

IBM Installation Manager version 1.7.0 et versions ultérieures est pris en charge pour l'installation d'IBM Security Directory Server. Un message d'erreur s'affiche sur la page d'installation des modules d'IBM Installation Manager et les scénarios d'installation suivants ne sont plus possibles :

- Vous tentez de démarrer l'installation d'IBM Security Directory Server avec une version précédente d'IBM Installation Manager.
- Une version précédente d'IBM Installation Manager est détectée au démarrage de l'installation d'IBM Security Directory Server à partir du tableau de bord.

Installations multiples

Il n'est pas possible d'installer plusieurs copies de la même version d'IBM Security Directory Server sur le même système. Si vous resélectionnez le module d'installation de la même version, IBM Installation Manager génère un message d'avertissement et vous ne pouvez pas réaliser l'installation. Cependant, différentes versions d'IBM Security Directory Server peuvent coexister sur le même système.

Emplacements d'installation sur les systèmes AIX et Linux :

IBM Security Directory Server n'est installable qu'à un emplacement prédéfini sur les systèmes AIX et Linux. Le chemin est défini par défaut dans la zone **Répertoire d'installation** d'IBM Installation Manager. Bien que cette zone soit éditable dans IBM Installation Manager, si vous modifiez le chemin par défaut, il devient impossible de cliquer sur **Suivant** pour continuer l'installation. Vous devez revenir au chemin d'installation par défaut d'IBM Security Directory Server.

Cette restrictions ne s'applique pas aux systèmes d'exploitation Microsoft Windows. Sous Microsoft Windows, IBM Security Directory Server peut être installé dans le chemin personnalisé de votre choix. Même si vous sélectionnez un emplacement d'installation personnalisé pour IBM Security Directory Server, le répertoire `idsinstinfo` et le fichier `idsinstances.ldif` qu'il contient sont toujours créés sur la partition définie par `%SystemDrive%`.

Si IBM Security Directory Server est installé sur l'unité `E:` et si le système d'exploitation est sur l'unité `C:`, vous observerez peut-être les modifications suivantes :

- Le répertoire `idsinstinfo` est créé sur l'unité `C:`, (`C:\idsinstinfo`), et non dans le répertoire `E:\Program Files\IBM\ldap`.

Pour plus d'informations sur les emplacements d'installation par défaut, voir «Emplacements d'installation par défaut», à la page 27.

Composants d'IBM Security Directory Server

Lorsque vous installez IBM Security Directory Server à l'aide d'IBM Installation Manager, vous pouvez sélectionner les composants à installer. IBM Installation Manager affiche les dépendances de chaque composant sélectionné.

Les composants suivants d'IBM Security Directory Server peuvent être installés :

IBM DB2

Vous pouvez installer IBM DB2 en tant que fonction. Si une version compatible d'IBM DB2 est installée, il n'est pas nécessaire d'installer la version de DB2 qui est livrée dans le module IBM Security Directory Server. Pour plus d'informations sur les versions de DB2 prises en charge pour les différents systèmes d'exploitation, consultez le manuel *Présentation d'IBM Security Directory Server*.

IBM DB2 est requis pour le serveur d'annuaire complet car les données d'annuaire sont stockées dans une base de données DB2. IBM DB2 n'est pas requis pour le serveur proxy.

IBM Global Security Kit

Vous pouvez installer IBM Global Security Kit (GSKit) avec d'autres fonctions d'IBM Security Directory Server. GSKit est une fonction facultative qui n'est requise que si vous souhaitez utiliser le protocole de communication SSL (Secure Sockets Layer) ou TLS (Transport Layer Security). Pour établir et utiliser des connections sécurisées, vous devez installer GSKit sur les systèmes serveur et client.

Client C

Le client C peut être installé comme une fonction autonome, ou avec d'autres fonctions d'IBM Security Directory Server. La fonction client C n'a pas de dépendances vis-à-vis des autres fonctions. Cependant, les fonctions serveur et serveur proxy sont dépendantes du client C. Si vous installez la fonction serveur ou serveur proxy, l'installation de la fonction client C est sélectionnée automatiquement.

Le client C est un kit SDK (Software Development Kit) qui fournit les outils permettant de développer des applications LDAP en langage C. Le module du client C contient les fichiers et les applications ci-après.

- Bibliothèques client comprenant un ensemble d'API en langage C
- Fichiers d'en-tête C utilisés pour la création et la compilation d'applications LDAP
- Utilitaire serveur et client C
- Exemples de programmes sources

IBM Java Development Kit

IBM Java Development Kit peut être installé comme une fonction autonome, ou avec d'autres fonctions d'IBM Security Directory Server. Si vous choisissez d'installer IBM Java Development Kit, IBM Installation

Manager décompresse les fichiers dans le sous-répertoire `java` du répertoire d'installation d'IBM Security Directory Server. IBM Java Development Kit comprend IBM Java SDK et Java 1.6 SR 14. IBM Java Development Kit est requis pour la compilation des exemples de programme Java, et pour l'exécution des programmes Java, par exemple l'outil d'administration d'instance (**idsxinst**) et l'outil de configuration (**idsxcfg**).

Client Java
Le client Java peut être installé comme une fonction autonome, ou avec d'autres fonctions d'IBM Security Directory Server. La fonction client Java n'a pas de dépendances vis-à-vis des autres fonctions. Cependant, les fonctions serveur et serveur proxy sont dépendantes du client Java. Si vous installez la fonction serveur ou serveur proxy, l'installation de la fonction client Java est sélectionnée automatiquement.

Le client Java comprend le kit d'outils JDNI d'IBM Security Directory Server et les utilitaires client Java.

Serveur
Vous pouvez installer le serveur avec d'autres fonctions d'IBM Security Directory Server. La fonction serveur est dépendante des fonctions client C et client Java. Si vous sélectionnez l'installation de la fonction serveur, l'installation des fonctions client C et client Java est également sélectionnée.

La fonction serveur est requise pour créer un serveur d'annuaire complet ou un serveur LDAP. Vous devez configurer un serveur d'annuaire complet avec une instance de base de données. Il traite les requêtes des clients qui nécessitent un accès aux entrées stockées dans la base de données. DB2 est requis pour les serveurs d'annuaire complets.

Serveur proxy
Vous pouvez installer le serveur proxy avec d'autres fonctions d'IBM Security Directory Server. La fonction serveur proxy est dépendante des fonctions client C et client Java. Si vous sélectionnez l'installation de la fonction serveur proxy , l'installation des fonctions client C et client Java est également sélectionnée.

Le serveur proxy est un serveur LDAP qui joue le rôle d'interface pour l'annuaire. Il authentifie les demandes des clients pour l'ensemble de l'annuaire, et achemine les requêtes vers les serveurs d'annuaire complets. Le serveur proxy peut également être utilisé comme interface d'un cluster de serveurs ou d'un annuaire distribué à des fins de reprise et d'équilibrage de charge.

Outil d'administration Web
L'outil d'administration Web peut être installé comme une fonction autonome, ou avec d'autres fonctions d'IBM Security Directory Server. L'outil d'administration Web est une fonction facultative requise si vous souhaitez gérer votre serveur d'annuaire à distance. Pour utiliser l'outil d'administration Web, vous devez le déployer sur une version prise en charge d'Embedded WebSphere Application Server ou de WebSphere Application Server.

Lorsque vous installez l'outil d'administration Web, les fichiers DSML (Directory Services Markup Language) sont aussi copiés sur l'ordinateur. Pour plus d'informations sur DSML, voir Annexe A, «Directory Services Markup Language», à la page 253.

Vous pouvez utiliser l'outil d'administration Web comme une console pour gérer les serveurs d'annuaire, qui peuvent être de type :

- IBM Security Directory Server, version 6.3.1
- IBM Security Directory Server, version 6.3
- IBM Security Directory Server version 6.2
- IBM Security Directory Server, version 6.1
- IBM Security Directory Server, version 6.0
- i5/OS V5 R4
- z/OS V1 R6 Integrated Security Services
- z/OS V1 R8 Integrated Security Services
- z/OS V1 R8 IBM Tivoli Directory Server
- z/OS V1 R9 IBM Tivoli Directory Server
- z/OS V1 R10 IBM Tivoli Directory Server

Important : Sous z/OS, la gestion des données d'annuaire est prise en charge, mais pas l'administration du serveur.

Embedded WebSphere Application Server
Vous pouvez installer Embedded WebSphere Application Server si vous installez l'outil d'administration Web. Embedded WebSphere Application Server est une fonction facultative qui n'est requise que si vous souhaitez déployer et exécuter l'outil d'administration Web. Si une version prise en charge de WebSphere Application Server est installée sur votre système, il n'est pas nécessaire d'installer cette fonction. Vous pouvez déployer l'outil d'administration Web sur une instance existante de WebSphere Application Server ou d'Embedded WebSphere Application Server installée sur le système.

Personnalisation de l'installation d'IBM Security Directory Server

Vous pouvez personnaliser l'installation d'IBM Security Directory Server en fonction de votre utilisation du produit.

Différents objectifs peuvent soutendre l'installation d'IBM Security Directory Server :

- Produit complet
- Serveur d'annuaire complet
- Serveur proxy
- Client
- Gestion à distance des serveurs à l'aide de l'outil d'administration Web

Tableau 9. Fonctions d'IBM Security Directory Server à installer en fonction de l'utilisation du produit

Toutes les fonctions	**Serveur d'annuaire complet**	**Serveur proxy**	**Client**	**Gestion à distance des serveurs à l'aide de l'outil d'administration Web**
IBM DB2	Oui	Non	Non	Non
IBM Global Security Kit	Oui	Oui	Oui	Non

Tableau 9. Fonctions d'IBM Security Directory Server à installer en fonction de l'utilisation du produit (suite)

Toutes les fonctions	Serveur d'annuaire complet	Serveur proxy	Client	Gestion à distance des serveurs à l'aide de l'outil d'administration Web
Client C	Oui	Oui	Oui	Non
IBM Java Development Kit	Oui	Oui	Oui	Non
Client Java	Oui	Oui	Oui	Non
Serveur	Oui	Non	Non	Non
Serveur proxy	Non	Oui	Non	Non
Outil d'administration Web	Facultatif	Facultatif	Non	Oui

Remarque : Si vous choisissez d'installer l'outil d'administration Web, IBM Installation Manager propose une option permettant d'installer Embedded WebSphere Application Server.

Avec l'installation du serveur d'annuaire complet et du serveur proxy, vous pouvez, si vous le souhaitez, sélectionner Embedded WebSphere Application Server et l'outil d'administration Web.

Emplacements d'installation par défaut

Si vous effectuez l'installation à l'aide d'IBM Installation Manager, IBM Security Directory Server et les logiciels corequis sont installés dans le répertoire d'installation prédéfini.

Tableau 10. Emplacements d'installation par défaut d'IBM Security Directory Server, d'IBM DB2, d'Embedded WebSphere Application Server et d'IBM Java Development Kit.

Système d'exploita--tion	IBM Security Directory Server	IBM DB2	Embedded WebSphere Application Server	IBM Java Development Kit
Linux	`/opt/ibm/ldap/V6.3.1`	`/opt/ibm/sdsV6.3.1db2`	`/opt/ibm/ldap/V6.3.1/appsrv`	`/opt/ibm/ldap/V6.3.1/java`
AIX	`/opt/IBM/ldap/V6.3.1`	`/opt/IBM/sdsV6.3.1db2`	`/opt/IBM/ldap/V6.3.1/appsrv`	`/opt/IBM/ldap/V6.3.1/java`
Microsoft Windows	`C:\Program Files\IBM\ldap\V6.3.1`	`C:\Program Files\IBM\sdsV6.3.1db2`	`C:\Program Files\IBM\ldap\V6.3.1\appsrv`	`C:\Program Files\IBM\ldap\V6.3.1\java`

IBM Security Directory Server n'est installable qu'à un emplacement prédéfini sur les systèmes AIX et Linux. Le chemin est défini par défaut dans la zone **Répertoire d'installation** d'IBM Installation Manager. Bien que cette zone soit éditable dans IBM Installation Manager, si vous modifiez le chemin par défaut, il devient impossible de cliquer sur **Suivant** pour continuer l'installation. Vous devez revenir au chemin d'installation par défaut d'IBM Security Directory Server.

Cette restrictions ne s'applique pas aux systèmes d'exploitation Microsoft Windows. Sous Microsoft Windows, IBM Security Directory Server peut être installé dans le chemin personnalisé de votre choix. Même si vous sélectionnez un emplacement d'installation personnalisé pour IBM Security Directory Server, le répertoire `idsinstinfo` et le fichier `idsinstances.ldif` qu'il contient sont toujours créés sur la partition définie par `%SystemDrive%`. Si IBM Security Directory Server est installé sur l'unité `E:` et si le système d'exploitation est sur l'unité `C:`, vous observerez peut-être les modifications suivantes :

- Le répertoire `idsinstinfo` est créé sur l'unité `C:`, (`C:\idsinstinfo`), et non dans le répertoire `E:\Program Files\IBM\ldap`.

Référentiels d'installation

Le référentiel d'installation est un emplacement dans lequel les modules d'IBM Security Directory Server son disponible pour les installations.

Vous pouvez installer IBM Security Directory Server à partir de l'un des emplacements suivants :

- Disques d'installation du produit
- Unité partagée distante ou répertoire local contenant une image électronique du module d'installation

Vous pouvez commencer l'installation à partir du référentiel par l'une des méthodes suivantes :

- Utilisez le tableau de bord pour lancer l'installation depuis :
  - Un disque d'installation du produit
  - Une image électronique du module d'installation sur une unité locale partagée ou un répertoire local

  Lorsque vous utilisez le tableau de bord, la procédure d'installation est déjà configurée avec l'emplacement du référentiel qui contient le module d'installation.
- Démarrez IBM Installation Manager directement et définissez manuellement les préférences du référentiel. Par exemple :
  - L'URL du référentiel sur un serveur Web
  - Le chemin d'une unité partagée distante qui contient le module du produit

Démarrage de l'installation

Vous pouvez démarrer l'installation d'IBM Security Directory Server soit par le tableau de bord, soit à l'aide d'IBM Installation Manager, dans lequel vous aurez défini les préférences pour le référentiel.

Démarrage de l'installation silencieuse à l'aide du tableau de bord :

Le tableau de bord fournit un emplacement unique pour démarrer l'installation.

Pourquoi et quand exécuter cette tâche

Le tableau de bord vous permet de démarrer une installation dans les scénarios suivants :

- Installation à partir d'un disque d'installation du produit.

- Installation à partir d'un répertoire local ou d'une unité partagée distante contenant une image électronique du module du produit.

Lorsque vous utilisez le tableau de bord pour démarrer l'installation, IBM Installation Manager est installé automatiquement si une version prise en charge ne se trouve pas sur votre système.

Procédure

1. Accédez au répertoire racine du module d'installation.
   - Si vous utilisez le disque d'installation du produit IBM Security Directory Server, insérez-le dans l'unité.
   - Si vous effectuez l'installation à partir de l'image électronique du module d'installation du produit, à l'invite, accédez au répertoire contenant l'image.
2. Démarrez le tableau de bord.

   Remarque : Pour les systèmes d'exploitation Windows, cliquez avec le bouton droit de la souris sur le fichier `.exe` du tableau de bord, puis sélectionnez **`Exécuter en tant qu'administrateur`**.

Système d'exploitation	Commande à exécuter :
Windows 32 bits	`launchpad.exe`
Windows 64 bits	`launchpad64.exe`
AIX et Linux	`./launchpad.sh`

   Le tableau de bord d'IBM Security Directory Server démarre et la page de Bienvenue s'affiche.
3. Dans la page de **Bienvenue**, sélectionnez la langue dans la liste de **sélection de langue**, puis cliquez sur **OK**.
4. Dans la zone de navigation de gauche, cliquez sur **Installation d'IBM Security Directory Server**.
5. Dans la page **Installation**, cliquez su le lien de **lancement du programme d'installation d'IBM Security Directory Server**0 IBM Installation Manager démarre.
6. Vérifiez que les modules suivants sont sélectionnés et vont être installés :
   - IBM Installation Manager (il est listé uniquement si une version prise en charge n'est pas déjà installée sur votre système).
   - IBM Security Directory Server
7. Continuez la procédure d'installation d' IBM Security Directory Server. Voir «Installation à l'aide d'IBM Installation Manager», à la page 31.
8. Lorsque vous avez terminé l'installation, cliquez sur **Quitter**.

Résultats

Lorsque vous utilisez le tableau de bord pour démarrer l'installation d'IBM Security Directory Server, le tableau de bord crée un fichier temporaire, `sds631.temp`, qu contient le nom de chemin du média. Le fichier `sds631.temp` est crée dans l'emplacement suivant sur le système d'exploitation :

AIX et Linux

```
/tmp
```

Microsoft Windows
Le répertoire temporaire par défaut du système défini dans la variable *TEMP*.

Il n'est pas possible d'installer plusieurs copies de la même version d'IBM Security Directory Server sur le même système. Si vous resélectionnez le module d'installation de la même version, IBM Installation Manager génère un message d'avertissement et vous ne pouvez pas réaliser l'installation. Cependant, différentes versions d'IBM Security Directory Server peuvent coexister sur le même système.

Que faire ensuite

Continuez la procédure d'installation d'IBM Security Directory Server. Voir «Installation à l'aide d'IBM Installation Manager», à la page 31.

Démarrage de l'installation par la définition des préférences liées au référentiel

Si la version prise en charge d'IBM Installation Manager est installée sur le système, vous pouvez la démarrer directement et définir vos préférences pour le référentiel.

Avant de commencer

IBM Installation Manager version 1.7.0 et versions ultérieures est pris en charge pour l'installation d'IBM Security Directory Server. Un message d'erreur s'affiche sur la page d'installation des modules d'IBM Installation Manager et les scénarios d'installation suivants ne sont plus possibles :

- Vous tentez de démarrer l'installation d'IBM Security Directory Server avec une version précédente d'IBM Installation Manager.
- Une version précédente d'IBM Installation Manager est détectée au démarrage de l'installation d'IBM Security Directory Server à partir du tableau de bord.

Si le système contient une version d'IBM Installation Manager antérieure à la version 1.7.0, vous devez effectuer la mise à niveau vers la 1.7.0 au minimum. Vous disposez de plusieurs possibilités pour installer la version requise d'IBM Installation Manager.

- Lancez l'installation d'IBM Installation Manager à partir du tableau de bord. Pour plus d'informations, voir «Démarrage de l'installation silencieuse à l'aide du tableau de bord :», à la page 28.
- Téléchargez IBM Installation Manager, version 1.7.0 ou supérieure correspondant à votre système d'exploitation. Pour plus d'informations sur l'installation en mode silencieux d'IBM Installation Manager, voir la documentation IBM Installation Manager à l'adresse http://www-01.ibm.com/support/knowledgecenter/SSDV2W/welcome.

Pourquoi et quand exécuter cette tâche

Vous pouvez commencer l'installation par la définition des préférences liées au référentiel, selon les scénarios suivants :

- Installation à partir d'un répertoire local ou d'une unité partagée distante contenant le module du produit téléchargé depuis le site IBM Passport Advantage.
- Installation à partir de l'URL du référentiel sur un serveur Web

Procédure

1. Démarrez IBM Installation Manager.

   Windows
   Dans le menu **Démarrer**, cliquez sur **Tous les programmes** > **IBM Installation Manager** > **IBM Installation Manager**.

   AIX et Linux
   Entrez la commande suivante à l'invite de commande. Modifiez le chemin par défaut suivant si IBM Installation Manager est installé à un emplacement différent.

   ```
   /opt/IBM/InstallationManager/eclipse/IBMIM
   ```

2. Dans la page d'accueil d'IBM Installation Manager, cliquez sur **Fichier** > **Préférences**.
3. Dans la page Référentiels, cliquez sur **Ajouter un référentiel**.
4. Dans la page d'ajout du référentiel, entrez l'URL du référentiel, ou naviguez jusqu'à lui.
5. Cliquez sur **OK**. Si vous définissez une adresse HTTPS ou si l'accès au référentiel est restreint, vous êtes invités à saisir un ID utilisateur et un mot de passe. Le nouvel emplacement ou l'emplacement modifié du référentiel apparaît alors dans la liste.
6. Pour vérifier l'accès au référentiel, cliquez sur **Tester les connexions**.
7. Cliquez sur **OK** pour quitter la page Référentiels.

Résultats

Il n'est pas possible d'installer plusieurs copies de la même version d'IBM Security Directory Server sur le même système. Si vous resélectionnez le module d'installation de la même version, IBM Installation Manager génère un message d'avertissement et vous ne pouvez pas réaliser l'installation. Cependant, différentes versions d'IBM Security Directory Server peuvent coexister sur le même système.

Que faire ensuite

Continuez la procédure d'installation d'IBM Security Directory Server. Voir «Installation à l'aide d'IBM Installation Manager».

Installation à l'aide d'IBM Installation Manager

Procédez de la manière suivante pour installer IBM Security Directory Server à l'aide d'IBM Installation Manager.

Avant de commencer

Démarrez l'installation.

Procédure

1. Dans la page d'accueil d'IBM Installation Manager, cliquez sur **Installer**.
2. Dans la page d'installation des modules, sélectionnez le module IBM Security Directory Server.
3. Cliquez sur **Suivant**. IBM Installation Manager vérifie la présence des modules prérequis sur le système.
4. Les modules manquants sont identifiés dans la page des résultats de la validation.

a. Lorsque vous avez installé les modules manquants, vous pouvez revérifier la présence des prérequis en cliquant sur **Revérifier l'état**. Pour plus d'informations sur les prérequis, voir «Modules prérequis pour différents systèmes d'exploitation», à la page 15.

b. Si toutes les conditions requises sont remplies, cliquez sur **Suivant**.

5. Cliquez sur **J'accepte les dispositions du contrat de licence**, puis cliquez sur **Suivant**. L'emplacement du répertoire des ressources partagées s'affiche.
6. Facultatif : Utilisez le chemin par défaut, ou entrez un chemin dans la zone du répertoire de ressources partagées. Le répertoire de ressources partagées est celui dans lequel les artefacts d'installation sont mis à la disposition d'un ou de plusieurs groupes de modules de produit. Vous pouvez spécifier le répertoire des ressources partagées uniquement lorsque vous installez un package pour la première fois.
7. Cliquez sur **Suivant**. Le nom du groupe de modules et le répertoire d'installation par défaut s'affichent. Si elle est prise en charge pour l'installation d'IBM Security Directory Server, l'option de création d'un nouveau groupe de modules est sélectionnée par défaut. Un groupe de modules représente un répertoire dans lequel les modules partagent des ressources avec les autres modules du même groupe. L'attribution d'un nom au groupe de modules est automatique.

   Restriction :

   IBM Security Directory Server n'est installable qu'à un emplacement prédéfini sur les systèmes AIX et Linux. Le chemin est défini par défaut dans la zone **Répertoire d'installation** d'IBM Installation Manager. Bien que cette zone soit éditable dans IBM Installation Manager, si vous modifiez le chemin par défaut, il devient impossible de cliquer sur **Suivant** pour continuer l'installation. Vous devez revenir au chemin d'installation par défaut d'IBM Security Directory Server.

   Pour connaître la liste des emplacements d'installation par défaut sous différentes systèmes d'exploitation, voir «Emplacements d'installation par défaut», à la page 27.

   Cette restrictions ne s'applique pas aux systèmes d'exploitation Microsoft Windows. Sous Microsoft Windows, IBM Security Directory Server peut être installé dans le chemin personnalisé de votre choix. Même si vous sélectionnez un emplacement d'installation personnalisé pour IBM Security Directory Server, le répertoire `idsinstinfo` et le fichier `idsinstances.ldif` qu'il contient sont toujours créés sur la partition définie par `%SystemDrive%`. Si IBM Security Directory Server est installé sur l'unité `E:` et si le système d'exploitation est sur l'unité `C:`, vous observerez peut-être les modifications suivantes :

   - Le répertoire `idsinstinfo` est créé sur l'unité `C:`, (`C:\idsinstinfo`), et non dans le répertoire `E:\Program Files\IBM\ldap`.

8. Cliquez sur **Suivant**.
9. Dans la page d'installation des modules, sélectionnez la fonction de votre choix. Pour afficher les fonctions qui dépendent d'une fonction sélectionnée, ou la dépendance de celle-ci vis-à-vis d'autres fonctions, cochez la case **Afficher les dépendances**.

Tableau 11. Fonctions d'IBM Security Directory Server installables dans les modules du produit complet et les modules client seul

Toutes les fonctions	Dépendances d'installation	Fonctions dans le module du produit complet	Fonctions dans le module client seul
IBM DB2	Aucune	Oui	Non
IBM Global Security Kit	Aucune	Oui	Oui
Client C	Aucune	Oui	Oui
IBM Java Development Kit	Aucune	Oui	Oui
Client Java	Aucune	Oui	Oui
Serveur	Client C Client Java	Oui	Non
Serveur proxy	Client C Client Java	Oui	Non
Outil d'administration Web	Aucune	Oui	Non

10. Cliquez sur **Suivant**.
11. Si vous avez sélectionné l'installation de la fonction IBM DB2, cliquez sur **IBM DB2**, puis effectuez l'une des opérations ci-après.
    - Pour installer IBM DB2, effectuez l'une des opérations ci-après.
      a. Cliquez sur **Installer DB2**.
      b. Dans la zone **Chemin installable DB2**, entrez le chemin de l'élément installable DB2. Vous pouvez cliquer sur **Parcourir** pour rechercher cet emplacement.
      c. Sous Windows, l'ID utilisateur système de votre choix pour les groupes `DB2ADMNS` ou `DB2USERS` dans la zone **Nom d'utilisateur**. Vous pouvez utiliser cet ID utilisateur pour exécuter des applications et des outils DB2 en local sur l'ordinateur. Si l'ID utilisateur n'existe pas, le programme d'installation crée le compte utilisateur.
      d. Sous Windows, entrez le mot de passe correspondant à l'ID utilisateur dans la zone **Mot de passe**. Si le mot de passe ne respecte pas les règles sur les mots de passe définies sur l'ordinateur, l'installation risque d'échouer.
      e. Sous Windows, entrez le mot de passe correspondant à l'ID utilisateur dans la zone **Confirmer le mot de passe**.
      f. Cliquez sur **Suivant**.
    - Si une version compatible d'IBM DB2 est installée sur l'ordinateur, effectuez l'une des opérations suivantes.
      a. Pour utiliser une version existante d'IBM DB2, cliquez sur **Continuer avec l'élément DB2 existant**.

         Important : Si vous choisissez d'utiliser une version existante de DB2 pendant l'installation, IBM Installation Manager met à jour l'entrée de la fonction DB2 dans son registre.
      b. Dans la liste, sélectionnez une version compatible de DB2 à utiliser avec IBM Security Directory Server.
      c. Cliquez sur **Suivant**.

12. Si vous avez sélectionné l'installation de la fonction IBM Global Security Kit, cliquez sur **IBM Global Security Kit**, puis effectuez l'une des opérations ci-après.
    - Si GSKit version 8.0 ou une version ultérieure n'est pas installé sur l'ordinateur, effectuez les opérations ci-après.
        a. Cliquez sur **Installer GSKit**.
        b. Dans la zone **Chemin de l'élément installable GSKit**, entrez le chemin de l'élément installable GSKit. Vous pouvez cliquer sur **Parcourir** pour rechercher cet emplacement.

           Remarque : Le chemin saisi doit contenir les versions 32 bits et 64 bits du fichier installable de GSKit.
        c. Cliquez sur **Suivant**.
    - Si GSKit version 8.0 ou une version ultérieure est installé sur l'ordinateur, effectuez l'une des opérations ci-après.
        a. Pour utiliser une version existante de GSKit, cliquez sur **Poursuivre avec l'élément GSKit existant**.

           Important : Si vous choisissez d'utiliser une version existante de GSKit pendant l'installation, IBM Installation Manager met à jour l'entrée de la fonction GSKit dans son registre.
        b. Cliquez sur **Suivant**.
13. Si vous sélectionnez l'installation de la fonction IBM Java Development Kit, cliquez sur **IBM Java Development Kit**, puis effectuez les opérations ci-après.
    a. Dans la zone **IBM Java Development Kit**, entrez le nom et le chemin du fichier compressé du JDK. Vous pouvez cliquer sur **Parcourir** pour rechercher cet emplacement.
    b. Cliquez sur **Suivant**.
14. Si vous sélectionnez l'installation de la fonction outil d'administration Web, cliquez sur **Outil d'administration Web**, puis effectuez les opérations ci-après.
    a. Pour installer Embedded WebSphere Application Server, effectuez l'une des opérations ci-après.
        1) Sélectionnez **Installer Embedded WebSphere Application Server**.
        2) Dans la zone **Chemin de l'élément installable Embedded WebSphere Application Server**, entrez le chemin de l'élément installable d'Embedded WebSphere Application Server. Vous pouvez cliquer sur **Parcourir** pour rechercher cet emplacement.
    b. Pour déployer l'outil d'administration Web, effectuez l'une des opérations ci-après.
        - Pour effectuer le déploiement dans un instance d'Embedded WebSphere Application Server qui se trouve dans le chemin d'installation par défaut, cliquez sur **Déployer dans Embedded WebSphere Application Server**.

          Remarque : S'il existe une version précédente de l'outil d'administration Web, le programme d'installation la migre vers la version en cours si les conditions ci-après sont remplies.
            1) Les versions précédentes de l'outil d'administration Web et d'Embedded WebSphere Application Server sont installées dans le chemin d'installation par défaut.

2) La version précédente de l'outil d'administration Web est déployées dans l'instance d'Embedded WebSphere Application Server qui se trouve dans le chemin d'installation par défaut.
3) L'outil d'administration Web qui est fourni avec IBM Security Directory Server version 6.1, 6.2 ou 6.3 est pris en charge par la migration.

- Pour effectuer le déploiement dans une instance de WebSphere Application Server ou d'Embedded WebSphere Application Server qui se trouve dans un chemin d'installation personnalisé, cliquez sur **Déployer dans un serveur WebSphere Application Server existant**.
  1) Dans la zone **Chemin d'installation WebSphere Application Server ou Embedded WebSphere Application Server**, entrez le chemin d'installation d'un serveur d'applications Web existant.
- Si vous voulez remettre à plus tard le déploiement de l'outil d'administration Web sur un serveur d'applications Web pris en charge, cliquez sur **Déployer manuellement ultérieurement**.

15. Cliquez sur **Suivant**. Les informations de préinstallation s'affichent : elles comprennent le répertoire d'installation, la liste des modules et les informations sur le référentiel.
16. Vérifiez le récapitulatif, et cliquez sur **Installer**. L'installation commence, et une barre de progression s'affiche. Après l'installation, le récapitulatif post-installation s'affiche.
17. Cliquez sur le lien d'affichage des journaux pour vérifier la réussite de l'installation. Pour plus d'informations, voir Chapitre 5, «Fichiers journaux d'IBM Installation Manager», à la page 45.
18. Pour lancer l'un des programmes suivants, effectuez l'opération correspondante :
    - Pour démarrer l'outil d'administration d'instance, cliquez sur **Outils d'administration d'instance (idsxinst)**.
    - Si vous ne souhaitez lancer aucun programme, cliquez sur **Aucun**.
19. Cliquez sur **Terminer**.
20. Cliquez sur **Fichier** > **Quitter**.

Résultats

Si l'installation aboutit, IBM Security Directory Server est installé dans le répertoire d'installation. Pour plus d'informations sur le répertoire d'installation par défaut, voir «Emplacements d'installation par défaut», à la page 27. Si l'installation de l'une des fonctions sélectionnées échoue, l'installation des modules d'IBM Security Directory Server est annulée.

Que faire ensuite

Après l'installation d'IBM Security Directory Server, vous devez réaliser les opérations ci-après.

- Pour utiliser IBM Security Directory Server en tant que serveur d'annuaire complet, créez une instance de serveur d'annuaire. Pour plus d'informations, voir «Création de l'instance de serveur d'annuaire par défaut», à la page 138.
- Pour utiliser IBM Security Directory Server en tant que serveur proxy, créez une instance de serveur proxy. Pour plus d'informations, voir «Création d'une instance de serveur proxy avec des paramètres personnalisés», à la page 148.

Installation en mode silencieux

L'installation en mode silencieux permet d'installer IBM Security Directory Server sur plusieurs systèmes sans aucune intervention manuelle.

Pour une installation silencieuse, vous devez effectuer les opérations ci-après.

1. Installez IBM Installation Manager si cela n'est pas déjà fait.
2. Utilisez le fichier de réponses par défaut ou enregistrez un fichier de réponses personnalisé.
3. Installez les modules.

Fichier de réponses pour une installation silencieuse

Dans le mode d'installation silencieux, l'interface utilisateur n'est pas disponible. Le fichier de réponses fournit les entrées à l'installation. Un fichier de réponses est un fichier XML qui contient les données requises pour l'installation silencieuse.

Enregistrement d'un fichier de réponses personnalisé

Vous pouvez enregistrer un fichier de réponses pour les tâches ci-après.

- Installation des modules
- Modification des modules
- Désinstallation des modules

Pour enregistrer un fichier de réponses, vous devez enregistrer les préférences et les actions d'installation à l'aide d'IBM Installation Manager en mode d'interface utilisateur. Lors du premier enregistrement d'un fichier de réponses destiné à une installation silencieuse, vous pouvez choisir de ne pas installer les modules avec le paramètre **-skipInstall** *emplacement_données_agent*.

L'emplacement *emplacement_données_agent* stocke les données d'installation du produit. Pour enregistrer un fichier de réponses pour une modification ou une désinstallation silencieuse du produit, vous devez utiliser le même emplacement *emplacement_données_agent* avec le paramètre **-skipInstall** .

Pour un scénario à plusieurs installations, vous devez enregistrer plusieurs fichiers de réponses avec un emplacement *emplacement_données_agent* différent pour chaque installation.

Pour plus d'informations sur l'enregistrement d'un fichier de réponses pour une installation en mode silencieux, voir la documentation IBM Installation Manager à l'adresse http://www-01.ibm.com/support/knowledgecenter/SSDV2W/welcome.

Vérification de l'installation silencieuse

Lorsque l'installation silencieuse est terminée, vous devez la vérifier. Vous pouvez vérifier l'installation de l'une des manières suivantes :

- Vérification du code retour
- Vérification du fichier journal
- Vérification des modules

Installation en mode silencieux avec un fichier de réponses

Utilisez l'installation en mode silencieux de IBM Security Directory Server pour installer les modules obligatoires sans aucune intervention manuelle.

Avant de commencer

IBM Installation Manager, version 1.7.0 ou supérieure est requise pour l'installation en mode silencieux des modules IBM Security Directory Server.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser le fichier de réponses ou enregistrer un fichier de réponses personnalisé et l'utiliser comme fichier en entrée de l'installation en mode silencieux.

Procédure

1. Connectez-vous au système en tant qu'administrateur.
2. Accédez à la commande **IBMIM** depuis l'emplacement d'installation d'IBM Installation Manager.

Système d'exploitation	Emplacement par défaut de la commande IBMIM :
Microsoft Windows	`C:\Program Files\IBM\InstallationManager\eclipse`
AIX et Linux	`/opt/IBM/InstallationManager/eclipse`

3. Facultatif : Exécutez la commande **IBMIM** pour enregistrer un fichier de réponses pour l'installation.

   Conseil : Vous pouvez utiliser le fichier de réponses exemple pour l'installation. Voir l'emplacement par défaut du fichier de réponses exemple, «Installation en mode silencieux», à la page 36.

   a. Pour enregistrer les étapes d'installation sans installer le produit, exécutez les commandes suivantes sur les différents systèmes d'exploitation :

      Microsoft Windows

      ```
      IBMIM.exe -record path_name\responseFile.xml -skipInstall
      agentDataLocation
      ```

      AIX et Linux

      ```
      ./IBMIM -record path_name/responseFile.xml -skipInstall
      agentDataLocation
      ```

      la commande ouvre IBM Installation Manager.

   b. Définissez le référentiel IBM Security Directory Server. Pour plus d'informations, voir 2, à la page 31

   c. Terminez l'enregistrement de l'installation d'IBM Security Directory Server. Pour plus d'informations, voir «Installation à l'aide d'IBM Installation Manager», à la page 31

4. Exécutez la commande **imcl** pour démarrer l'installation en mode silencieux avec le fichier de réponses comme entrée. La commande **imcl** doit se trouver dans <*IBM_Installation_Manager_install_dir*>/eclipse/tools.

Système d'exploitation	Commande à exécuter :
Microsoft Windows	`imcl.exe input path_name\responseFile.xml -acceptLicense -showProgess`

Système d'exploitation	Commande à exécuter :
AIX et Linux	`./imcl input path_name/responseFile.xml -acceptLicense -showProgess`

Remarque : Ce nombreux autres paramètres peuvent être utilisés avec la commande **imcl**. Pour plus de détails, voir l'aide de la commande **imcl**.

5. Vérifiez le récapitulatif d'installation et les fichiers journaux.

Système d'exploitation	Chemin d'accès au journal par défaut :
Microsoft Windows	`C:\ProgramData\IBM\InstallationManager\logs`
AIX et Linux	`/var/ibm/InstallationManager/logs/`

6. Vérifiez que les modules IBM Security Directory Server sont au niveau requis :

Système d'exploitation	Vérification des modules :
Microsoft Windows	Voir «Vérification des fonctions IBM Security Directory Server à l'aide d'IBM Installation Manager», à la page 85.
AIX et Linux	Voir «Vérification des fonctions IBM Security Directory Server à l'aide d'IBM Installation Manager», à la page 85.

Résultats

Si l'installation réussit, IBM Security Directory Server est installé dans l'emplacement d'installation d'IBM Security Directory Server0 Pour plus d'informations sur le répertoire d'installation par défaut, voir «Emplacements d'installation par défaut», à la page 27. Si l'installation de l'une des fonctions sélectionnées échoue, l'installation des modules IBM Security Directory Server est annulée.

Que faire ensuite

Remarque : Si vous choisissez d'ouvrir l'Outil d'administration d'instance lorsque vous enregistrez votre fichier de réponses d'installation, cet outil ne s'ouvre pas après l'installation en mode silencieux d'IBM Security Directory Server.

Si vous avez choisi la fonction Serveur ou Serveur proxy pour l'installation, ouvrez l'Outil d'administration d'instance pour créer une instance de serveur d'annuaire ou une instance de serveur proxy. Voir «Démarrage de l'outil d'administration d'instance», à la page 135.

Chapitre 4. Modification avec IBM Installation Manager

IBM Installation Manager vous permet d'installer des fonctions d'IBM Security Directory Server que vous n'aviez pas encore installées et de désinstaller des fonctions installées.

vous ne pouvez pas désinstaller une fonction qui est requise pour d'autres fonctions installées. Vous ne pouvez supprimer une dépendance que si toutes les autres fonctions dépendantes sont sélectionnées pour la suppression, ou si elles ont déjà été supprimées.

Important : Si vous choisissez d'utiliser une version existante de DB2 ou de GSKit pendant l'installation, IBM Installation Manager met à jour l'entrée de la fonction dans son registre. Si vous supprimez une fonction qui a été installée avec l'option **Continuer avec l'élément existant**, Installation Manager :

- Supprime l'entrée de son propre registre.
- Ne désinstalle pas la fonction sur l'ordinateur.

Modification des fonctions à l'aide d'IBM Installation Manager

Procédez de la manière suivante pour modifier les fonctions d'IBM Security Directory Server à l'aide d'IBM Installation Manager.

Avant de commencer

Vous devez arrêter tous les processus IBM Security Directory Server client et serveur.

- Serveur d'annuaire
- Serveur d'administration
- Traces LDAP
- Applications LDAP personnalisées

Si des processus sont en cours d'utilisation, les programmes et les bibliothèques ne peuvent pas être supprimés.

Procédure

1. Démarrez IBM Installation Manager.
   - AIX et Linux :
     a. Ouvrez une fenêtre de commande et accédez au répertoire qui contient IBM Installation Manager. Voici le répertoire d'installation par défaut d'IBM Installation Manager :
        `opt/IBM/InstallationManager/eclipse`
     b. Exécutez la commande ci-après.
        `./IBMIM`
   - Microsoft Windows :
     a. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Installation Manager** > **IBM Installation Manager**.
2. Cliquez sur **Modifier**.
3. Sélectionnez **IBM Security Directory Server**, puis cliquez sur **Suivant**.

4. Dans la page de modification des modules, vous devez effectuer les opérations ci-après.
   a. Sélectionnez les fonctions à installer.
   b. Désélectionnez les fonctions à désinstaller.

Tableau 12. Fonctions IBM Security Directory Server modifiables dans les module du produit complet et du client seul

Toutes les fonctions	Dépendances d'installation	Fonctions dans le module du produit complet	Fonctions dans le module client seul
IBM DB2	Aucune	Oui	Non
IBM Global Security Kit	Aucune	Oui	Oui
Client C	Aucune	Oui	Oui
IBM Java Development Kit	Aucune	Oui	Oui
Client Java	Aucune	Oui	Oui
Serveur	Client C Client Java	Oui	Non
Serveur proxy	Client C Client Java	Oui	Non
Outil d'administration Web	Aucune	Oui	Non

Important : Si vous choisissez d'utiliser une version existante de DB2 ou de GSKit pendant l'installation, IBM Installation Manager met à jour l'entrée de la fonction dans son registre. Si vous supprimez une fonction qui a été installée avec l'option **Continuer avec l'élément existant**, Installation Manager :

- Supprime l'entrée de son propre registre.
- Ne désinstalle pas la fonction sur l'ordinateur.

s'il existe des instances DB2 que vous avez créées avec la copie de DB2 installée à l'aide d'IBM Installation Manager, IBM DB2 ne peut pas être supprimé. Dans ce cas, retirez manuellement les instances DB2 et réessayez. Il est recommandé de sauvegarder la base de données avant de supprimer les instances DB2.

   c. Cliquez sur **Suivant**.
5. Si vous avez sélectionné l'installation de la fonction IBM DB2, cliquez sur **IBM DB2**, puis effectuez l'une des opérations ci-après.
   - Pour installer IBM DB2, effectuez l'une des opérations ci-après.
     a. Cliquez sur **Installer DB2**.
     b. Dans la zone **Chemin installable DB2**, entrez le chemin de l'élément installable DB2. Vous pouvez cliquer sur **Parcourir** pour rechercher cet emplacement.
     c. Sous Windows, l'ID utilisateur système de votre choix pour les groupes `DB2ADMNS` ou `DB2USERS` dans la zone **Nom d'utilisateur**. Vous pouvez utiliser cet ID utilisateur pour exécuter des applications et des outils DB2 en local sur l'ordinateur. Si l'ID utilisateur n'existe pas, le programme d'installation crée le compte utilisateur.

d. Sous Windows, entrez le mot de passe correspondant à l'ID utilisateur dans la zone **Mot de passe**. Si le mot de passe ne respecte pas les règles sur les mots de passe définies sur l'ordinateur, l'installation risque d'échouer.

e. Sous Windows, entrez le mot de passe correspondant à l'ID utilisateur dans la zone **Confirmer le mot de passe**.

f. Cliquez sur **Suivant**.

- Si une version compatible d'IBM DB2 est installée sur l'ordinateur, effectuez les opérations ci-après.

  a. Pour utiliser une version existante d'IBM DB2, cliquez sur **Continuer avec l'élément DB2 existant**.

     Important : Si vous choisissez d'utiliser une version existante de DB2 pendant l'installation, IBM Installation Manager met à jour l'entrée de la fonction DB2 dans son registre.

  b. Dans la liste, sélectionnez une version compatible de DB2 à utiliser avec IBM Security Directory Server.

  c. Cliquez sur **Suivant**.

6. Si vous avez sélectionné l'installation de la fonction IBM Global Security Kit, cliquez sur **IBM Global Security Kit**, puis effectuez l'une des opérations ci-après.

   - Si GSKit version 8.0 ou une version ultérieure n'est pas installé sur l'ordinateur, effectuez les opérations ci-après.

     a. Cliquez sur **Installer GSKit**.

     b. Dans la zone **Chemin de l'élément installable GSKit**, entrez le chemin de l'élément installable GSKit. Vous pouvez cliquer sur **Parcourir** pour rechercher cet emplacement.

        Remarque : Le chemin saisi doit contenir les versions 32 bits et 64 bits du fichier installable de GSKit.

     c. Cliquez sur **Suivant**.

   - Si GSKit version 8.0 ou une version ultérieure est installé sur l'ordinateur, effectuez les opérations ci-après.

     a. Pour utiliser une version existante de GSKit, cliquez sur **Poursuivre avec l'élément GSKit existant**.

        Important : Si vous choisissez d'utiliser une version existante de GSKit pendant l'installation, IBM Installation Manager met à jour l'entrée de la fonction GSKit dans son registre.

     b. Cliquez sur **Suivant**.

7. Si vous sélectionnez l'installation de la fonction IBM Java Development Kit, cliquez sur **IBM Java Development Kit**, puis effectuez les opérations ci-après.

   a. Dans la zone **IBM Java Development Kit**, entrez le nom et le chemin du fichier compressé du JDK. Vous pouvez cliquer sur **Parcourir** pour rechercher cet emplacement.

   b. Cliquez sur **Suivant**.

8. Si vous sélectionnez l'installation de la fonction outil d'administration Web, cliquez sur **Outil d'administration Web**, puis effectuez les opérations ci-après.

   a. Pour installer Embedded WebSphere Application Server, effectuez l'une des opérations ci-après.

      1) Sélectionnez **Installer Embedded WebSphere Application Server**.

2) Dans la zone **Chemin de l'élément installable Embedded WebSphere Application Server**, entrez le chemin de l'élément installable d'Embedded WebSphere Application Server. Vous pouvez cliquer sur **Parcourir** pour rechercher cet emplacement.

b. Pour déployer l'outil d'administration Web, effectuez l'une des opérations ci-après.

- Pour effectuer le déploiement dans un instance d'Embedded WebSphere Application Server qui se trouve dans le chemin d'installation par défaut, cliquez sur **Déployer dans Embedded WebSphere Application Server**.

  Remarque : S'il existe une version précédente de l'outil d'administration Web, le programme d'installation la migre vers la version en cours si les conditions ci-après sont remplies.

  1) Les versions précédentes de l'outil d'administration Web et d'Embedded WebSphere Application Server sont installées dans le chemin d'installation par défaut.
  2) La version précédente de l'outil d'administration Web est déployées dans l'instance d'Embedded WebSphere Application Server qui se trouve dans le chemin d'installation par défaut.
  3) L'outil d'administration Web qui est fourni avec IBM Security Directory Server version 6.1, 6.2 ou 6.3 est pris en charge par la migration.

- Pour effectuer le déploiement dans une instance de WebSphere Application Server ou d'Embedded WebSphere Application Server qui se trouve dans un chemin d'installation personnalisé, cliquez sur **Déployer dans un serveur WebSphere Application Server existant**.

  1) Dans la zone **Chemin d'installation WebSphere Application Server ou Embedded WebSphere Application Server**, entrez le chemin d'installation d'un serveur d'applications Web existant.

- Si vous voulez remettre à plus tard le déploiement de l'outil d'administration Web sur un serveur d'applications Web pris en charge, cliquez sur **Déployer manuellement ultérieurement**.

9. Cliquez sur **Suivant**.

   Important : Si vous choisissez d'utiliser une version existante de DB2 ou de GSKit pendant l'installation, IBM Installation Manager met à jour l'entrée de la fonction dans son registre. Si vous supprimez une fonction qui a été installée avec l'option **Continuer avec l'élément existant**, Installation Manager :

   - Supprime l'entrée de son propre registre.
   - Ne désinstalle pas la fonction sur l'ordinateur.

10. Vérifiez le récapitulatif, et cliquez sur **Modifier**.
11. Facultatif : En cas d'erreur lors de la désinstallation, cliquez sur **Afficher le fichier journal** pour en lire les détails. Pour plus d'informations, voir Chapitre 5, «Fichiers journaux d'IBM Installation Manager», à la page 45.
12. Cliquez sur **Terminer**.
13. Cliquez sur **Fichier** > **Quitter**.

Résultats

Si les modifications aboutissent, vous pouvez constater ce qui suit.

- Les fonctions d'IBM Security Directory Server dont vous aviez demandé l'ajout sont installées dans le répertoire d'installation. Pour plus d'informations sur le répertoire d'installation par défaut, voir «Emplacements d'installation par défaut», à la page 27.
- Les fonctions d'IBM Security Directory Server dont vous aviez demandé le retrait ont été désinstallées.

Chapitre 5. Fichiers journaux d'IBM Installation Manager

Vous pouvez vérifier l'installation, la modification ou la désinstallation d'IBM Security Directory Server et de ses composants en consultant les fichiers journaux créés par IBM Installation Manager.

Si une erreur se produit au cours de l'installation, la modification ou la désinstallation d'IBM Security Directory Server et de ses composants, vous pouvez consulter les fichiers journaux. IBM Installation Manager crée les fichiers journaux à l'emplacement par défaut.

Tableau 13. Emplacement par défaut des fichiers journaux d'IBM Installation Manager sur différents systèmes d'exploitation

Système d'exploitation	**Emplacement par défaut d'IBM Installation Manager**
AIX et Linux	`/var/ibm/InstallationManager/logs`
Microsoft Windows	`C:\ProgramData\IBM\InstallationManager\logs`

Les emplacements par défaut s'appliquent à toutes les versions prises en charge d'AIX, de Linux et de Microsoft Windows.

Chapitre 6. Interrogation des modules d'IBM Security Directory Server

Vérifiez les modules d'IBM Security Directory Server en interrogeant les modules IBM Security Directory Server sur les plateformes prises en charge.

Pourquoi et quand exécuter cette tâche

Après l'installation des modules d'IBM Security Directory Server, vous devez vérifier que les modules sont au niveau requis : Cette tâche vous aide à interroger les numéros de version des modules IBM Security Directory Server installés.

Procédure

Connectez-vous au système sur lequel vous avez installé les modules d'IBM Security Directory Server et exécutez les commandes avec les privilège de superutilisateur.

- Sur les systèmes AIX : exécutez la commande **lslpp**. Par exemple :

  ```
  lslpp -l 'idsldap*'
  ```

- Sur les systèmes Linux : exécutez la commande **rpm**. Par exemple :

  ```
  rpm -qa | grep idsldap
  ```

- Sur les systèmes Solaris :
  1. Pour lister les modules installés, exécutez la commande **pkginfo**0 Par exemple :

     ```
     pkginfo | grep IDSl
     ```

  2. Pour interroger la version d'un module IBM Security Directory Server particulier, exécutez la commande **pkgparam**. Par exemple :

     ```
     pkgparam IDSlbc63 VERSION
     ```

- Sous les systèmes HP-UX (Itanium) : excéutez la commande **swlist**. Par exemple :

  ```
  swlist | grep idsldap
  ```

Chapitre 7. Installation en mode natif et configuration à l'aide de scripts

Vous pouvez installer et configurer IBM Security Directory Server à l'aide de scripts.

Feuille de route de l'installation

Utilisez la feuille de route pour installer IBM Security Directory Server sur les systèmes Linux x86, Linux i/pSeries, Linux s390, Solaris et HP-UX.

1. Vérifiez que le système possède la configuration matérielle et logicielle minimale requise. Pour plus d'informations, voir *Configuration système requise* dans la section Présentation du produit de la documentation IBM Security Directory Server documentation.
2. Installez les logiciels prérequis, par exemple DB2. S'il n'était pas déjà installé, vérifiez que le chemin de l'installable DB2 est accessible et qu'il dispose des droits nécessaires.
3. Si vous prévoyez d'utiliser les fonctions suivantes, les logiciels facultatifs suivants deviennent des logiciels prérequis et doivent être installés. S'ils n'étaient pas déjà installés, vérifiez que leur chemin est accessible et qu'ils disposent des droits nécessaires.
   - Pour utiliser l'outil d'administration Web, vous devez disposer d'une version compatible d'Embedded WebSphere Application Server ou de WebSphere Application Server. Une version compatible d'un navigateur est également nécessaire.
   - Le chiffrement SSL (Secure Socket Layer) ou TLS (Transport Layer Security) nécessite une version compatible d'IBM Global Security Kit (GSKit).
4. Su les systèmes Linux x86, Linux i/pSeries, Linux s390, Solaris et HP-UX, utilisez le programme d'installation **idsNativeInstall** pour installer les packages IBM Security Directory Server et les autres logiciels requis.
5. Après avoir installé IBM Security Directory Server, utilisez la commande **idsdefinst** pour créer et configurer une instance de serveur d'annuaire.
6. Démarrez l'instance du serveur d'annuaire.
7. Chargez l'exemple de fichier LDIF dans la base de données. Voir la section Administration de la documentation IBM Security Directory Server, pour plus d'informations sur l'utilisation de l'instance de serveur d'annuaire.

Remarque : Le script d'installation natif, **idsNativeInstall**, n'est pas fourni pour les systèmes d'exploitation Windows, AIX et Linux x86_64 (64 bits). Vous pouvez utiliser IBM Installation Manager ou les utilitaires de ligne de commande du système d'exploitation pour effectuer une installation manuelle sur ces systèmes d'exploitation.

Installation des modules IBM Security Directory Server sur des plateformes Linux, Solaris et HP-UX

Utilisez la procédure d'installation ou de mise à niveau des modules IBM Security Directory Server sur les systèmes Linux x86, Linux i/pSeries, Linux s390, Solaris et HP-UX.

Avant de commencer

Avant de commencer à installer les modules IBM Security Directory Server, vous devez effectuer les opérations ci-après.

1. Connectez-vous au système avec les droits d'administrateur.
2. Extrayez le fichier archive IBM Security Directory Server version 6.3.1 dans un répertoire, par exemple `/sdsV6.3.1`, possédant l'espace disque suffisant.
3. Arrêtez tous les processus serveur et client IBM Security Directory Server, y compris le serveur d'annuaire, le serveur d'administration, et les applications LDAP personnalisées. Les programmes et les bibliothèques ne peuvent pas être remplacés lorsqu'ils sont en cours d'utilisation. Si le traçage est défini, exécutez `ldtrc off` pour arrêter le processus de trace. Consultez les sections "Tâches d'administration de base du serveur" et "Serveur d'administration d'annuaire" dans la section *Administration* de la documentation IBM Security Directory Server pour savoir comment arrêter les instances du serveur d'annuaire et les serveurs d'administration.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la commande **idsNativeInstall** pour installer ou mettre à niveau les modules IBM Security Directory Server sur les systèmes Linux x86, Linux i/pSeries, Linux s390, Solaris et HP-UX. Vous pouvez aussi utiliser la commande **idsNativeInstall** pour installer en option DB2, GSKit, et la version intégrée de WebSphere Application Server, si ce n'est déjà fait.

Remarque :

- Le script d'installation natif, **idsNativeInstall**, n'est pas fourni pour les systèmes d'exploitation Windows, AIX et Linux x86_64 (64 bits). Vous pouvez utiliser IBM Installation Manager ou les utilitaires de ligne de commande du système d'exploitation pour effectuer une installation manuelle sur ces systèmes d'exploitation.
- Sur les systèmes HP-UX, les modules IBM Security Directory Server client seulement peuvent être installés ou mis à niveau.

Procédure

1. Accédez au répertoire contenant le programme d'installation **idsNativeInstall** et le fichier `responseFile.txt`. Les fichiers `idsNativeInstall` et `responseFile.txt` doivent être présents dans le même répertoire.
2. Mettez à jour les entrées suivantes du fichier `responseFile.txt`. Par défaut, les valeurs des variables d'installation de fonction sont définies sur `false` et les variables de chemin correspondantes ne sont pas définies.
   - Pour installer DB2, définissez la variable *db2FeatureInstall* sur `true` et mettez à jour la variable *db2InstallimagePath* avec le chemin d'accès absolu de l'élément installable DB2. Par exemple :

     ```
     db2FeatureInstall=true
     db2InstallimagePath=/sdsV6.3.1/db2
     ```

     Important : Pour une installation complète du serveur d'annuaire, DB2 doit être installé sur le système. Si vous définissez les variables DB2, *db2FeatureInstall* et *db2InstallimagePath*, DB2 est installé dans le répertoire `/opt/ibm/sdsV6.3.1db2` sous Linux ou dans le répertoire `/opt/IBM/sdsV6.3.1db2` sous Solaris. Si une version de DB2 est déjà installée dans l'emplacement indiqué, l'installation écrase alors les fichiers existants.

- Pour installer GSKit, définissez la variable *gskitFeatureInstall* sur `true`, puis mettez à jour la variable *gskitInstallimagePath* avec le chemin d'accès absolu de l'élément installable GSKit. Par exemple :

  ```
  gskitFeatureInstall=true
  gskitInstallimagePath=/sdsV6.3.1/gskit
  ```

  Important : Pour configurer une instance de serveur d'annuaire afin qu'elle communique via SSL ou TLS, une version obligatoire de GSKit doit être installée sur le système.
- Pour installer IBM Java Development Kit, définissez la variable *JDKFeatureInstall* sur `true` et mettez à jour la variable *JDKInstallimagePath* avec le chemin absolu de l'élément installable IBM Java Development Kit. Par exemple :

  ```
  JDKFeatureInstall=true
  JDKInstallimagePath=/sdsV6.3.1/java/ibm-java-16sr14-linux-i386.tar
  ```

  IBM Java Development est est installé dans le répertoire `/opt/ibm/ldap/V6.3.1/java` sur les systèmes Linux et Solaris.
- Pour installer la version intégrée de WebSphere Application Server, définissez la variable*eWasFeatureInstall* sur `true` et mettez à jour la variable *eWasInstallimagePath* avec le chemin d'accès absolu de la version intégrée de l'élément installable WebSphere Application Server. Par exemple :

  ```
  eWasFeatureInstall=true
  eWasInstallimagePath=/sdsV6.3.1/appsrv
  ```

  La version intégrée de WebSphere Application Server est installée dans le répertoire `/opt/ibm/ldap/V6.3/appsrv` sur les systèmes Linux et Solaris.
- Pour installer la disponibilité générale de IBM Security Directory Server version 6.3.1 (GA), mettez à jour la variable *tdsInstallimagePath* avec le chemin d'accès absolu de l'élément installableIBM Security Directory Server version 6.3.1 GA. Par exemple :

  ```
  tdsInstallimagePath=/sdsV6.3.1
  ```

  Si vous indiquez `/sdsV6.3.1` comme emplacement installable de IBM Security Directory Server version 6.3.1, vérifiez que les fichiers suivants sont présents dans le répertoire `/sdsV6.3.1`.

  ```
  idsinstall
  idsinstall_i
  ids_detectGskitVersion
  ```

  Les modules IBM Security Directory Server version 6.3.1 doivent être présents dans le répertoire `/sdsV6.3.1/tdsfiles`.

3. Exécutez la commande **idsNativeInstall** à l'invite de commande.

Résultats

Lorsque vous avez exécuté la commande **idsNativeInstall**, elle installe les modules IBM Security Directory Server 6.3.1. La commande **idsNativeInstall** installe également DB2, GSKit, IBM Java Development Kit, ou la version intégrée de WebSphere Application Server en fonction des valeurs contenues dans le fichier de réponses.

Remarque : Si IBM Security Directory Server version 6.3.1 n'est pas installé sur le système, tous les composants de IBM Security Directory Server version 6.3.1 sont

installés. IBM Security Directory Server version 6.3.1 est installé dans le répertoire /opt/ibm/ldap/V6.3.1/ sur les systèmes Linux, Solaris et HP-UX.

Que faire ensuite

Après avoir installé IBM Security Directory Server, vous devez vérifier que les modules IBM Security Directory Server sont installés. Pour plus d'informations sur la vérifications des journaux, voir «Vérification des journaux d'installation».

Vérification des journaux d'installation

Déterminez le fichier journal dans lequel vous devez vérifier le statut d'installation sur les systèmes Linux x86, Linux i/pSeries, Linux s390, Solaris et HP-UX.

Lorsque l'installation est terminée, la commande **idsNativeInstall** affiche des messages qui indiquent si l'installation a abouti. Pour vérifier si les packages IBM Security Directory Server sont installés, consultez le fichier journal des journaux d'installation.

Le fichier journal est /var/idsldap/V6.3/idsNativeInstall_*horodatage*.log.

Après avoir passé en revue le journal d'installation, vérifiez que tous les modules se sont bien installés et qu'ils sont au niveau attendu. Pour savoir comment connaître le numéro de version des modules installés, consultez la rubrique Chapitre 6, «Interrogation des modules d'IBM Security Directory Server», à la page 47.

Chapitre 8. Installation d'IBM DB2

Vous ne pouvez créer une instance d'IBM Security Directory Server en configurant et en lui associant une base de données DB2, que si une version compatible d'IBM DB2 est installée sur votre ordinateur.

Le support d'installation d'IBM Security Directory Server contient une version compatible d'IBM DB2. Si vous utilisez les utilitaires du système d'exploitation pour l'installation d'IBM Security Directory Server, vous devez installer IBM DB2. Lors de l'installation d'IBM Security Directory Server, des informations détaillées sur la version compatible d'IBM DB2 sont insérées dans les fichiers de propriété. Si une version compatible d'IBM DB2 est installée sur votre poste, vous pouvez l'utiliser et la configurer avec l'instance du serveur d'annuaire. Pour plus d'informations sur la mise à jour du fichier `ldapdb.properties`, voir Annexe C, «Mise à jour manuelle du fichier `ldapdb.properties`», à la page 257.

Pour installer IBM DB2, accédez au support d'installation d'IBM Security Directory Server et accédez au répertoire qui contient le fichier installable d'IBM DB2.

Avant d'installer IBM DB2, vérifiez que l'environnement remplit les conditions requises pour ce produit. La commande **db2prereqcheck** permet de vérifier que la configuration requise pour DB2 est bien respectée. Si des modules sont manquants sur l'ordinateur, vous devez les y installer.

Sous AIX, Linux et Solaris, vous pouvez installer IBM DB2 à l'aide de la commande **db2_install**. Sous Windows, installez IBM DB2 à l'aide de la commande **setup.exe**.

Sous System x Linux dans une architecture 32 bits, vous devez sélectionner Workspace Server Edition en entrant WSE. Pour les autres systèmes d'exploitation pris en charge, sélectionnez Enterprise Server Edition en entrant ESE.

Après avoir installé IBM DB2, vérifiez dans le fichier `/tmp/db2_install_log.`*XXXXX* que l'installation a abouti. La chaîne *XXXXX* correspond à un chiffre aléatoire associé à l'installation.

Pour plus d'informations sur les prérequis DB2 et l'installation IBM DB2, voir la documentation du produit IBM DB2 à l'adresse http://www-01.ibm.com/support/knowledgecenter/SSEPGG/welcome.

Paramètres du noyau sur les systèmes Solaris

Sur les systèmes Solaris, vous devrez peut-être mettre à jour les paramètres du noyau dans le fichier `/etc/system` avant d'installer IBM DB2. La commande **db2osconf** permet de connaître les valeurs requises pour les paramètres du noyau sur l'ordinateur. Sous Solaris, vous pouvez utiliser la commande **projmod** pour configurer les valeurs des paramètres du noyau Solaris avant d'installer DB2.

Sur un système Solaris avec des zones configurées, la commande **db2osconf** n'est exécutable qu'à partir de la zone globale.

Pour plus d'informations sur la commande **db2osconf**, recherchez `db2osconf` dans la documentation du produit IBM DB2 à l'adresse http://www-01.ibm.com/

support/knowledgecenter/SSEPGG/welcome.

Chapitre 9. IBM Java Development Kit pour IBM Security Directory Server

Pour compiler des exemples de programme Java, et pour exécuter des programmes Java, par exemple l'outil d'administration d'instance et l'outil de configuration, vous devez décompresser IBM Java Development Kit dans l'emplacement d'installation d'IBM Security Directory Server.

Le support d'installation d'IBM Security Directory Server contient une version compatible d'IBM Java Development Kit, IBM Java 1.6 SR 14. Si vous utilisez les utilitaires du système d'exploitation pour l'installation d'IBM Security Directory Server, vous devez installer IBM Java Development Kit.

Pour installer IBM Java Development Kit, accédez au support d'installation d'IBM Security Directory Server et accédez au répertoire qui contient le fichier compressé d'IBM Java Development Kit.

Vous devez décompresser le fichier d'archive d'IBM Java Development Kit dans l'emplacement d'installation d'IBM Security Directory Server. Le fichier d'archive d'IBM Java Development Kit est décompressé dans le répertoire `java`. Pour plus d'informations sur l'emplacement d'installation d'IBM Security Directory Server, voir «Emplacements d'installation par défaut», à la page 27.

Sous AIX, vous pouvez utiliser GNU `tar` pour décompresser le fichier d'archive d'IBM Java Development Kit dans l'emplacement d'installation d'IBM Security Directory Server. Sinon, vous pourrez être obligé de déplacer le répertoire `java` que vous avez décompressé dans l'emplacement d'installation d'IBM Security Directory Server. Pour plus d'informations sur les modules prérequis, voir «Modules prérequis pour différents systèmes d'exploitation», à la page 15.

Tableau 14. Modules IBM Java Development Kit disponibles pour différents systèmes d'exploitation

Système d'exploitation	Nom du module
AIX	`ibm-java-16sr14-aix-ppc-64.tar`
System x Linux (Intel 32 bits)	`ibm-java-16sr14-linux-i386.tar`
Linux System i et System p	`ibm-java-16sr14-linux-ppc-64.tar`
System z Linux	`ibm-java-16sr14-linux-s390-64.tar`
Linux on AMD64/EM64T	`ibm-java-16sr14-linux-64.tar`
HP-UX (Itanium)	`ibm-java-16sr14-hp-itanium-64.tar`
Solaris on AMD64/EM64T	`ibm-java-16sr14-solaris-amd-64.tar`
Solaris SPARC	`ibm-java-16sr14-solaris-sparc-64.tar`
Windows 32 bits	`ibm-java-16sr14-win-i386.zip`
Windows on AMD64/EM64T	`ibm-java-16sr14-win-x86_64.zip`

Exemples

Exemple 1 :

Pour décompresser le fichier d'archive d'IBM Java Development Kit dans

l'emplacement d'installation d'IBM Security Directory Server sur un système Linux, entrez la commande ci-après.

```
tar -xf ibm-java-16sr14-linux-64.tar -C /opt/ibm/ldap/V6.3.1/
```

Chapitre 10. Installation d'IBM Global Security Kit

Si vous voulez utiliser SSL (Secure Sockets Layer) ou TLS (Transaction Layer Security) avec IBM Security Directory Server, une version prise en charge d'IBM Global Security Kit doit exister sur l'ordinateur.

Si votre système d'exploitation ne prend pas en charge l'installation avec IBM Installation Manager, vous pouvez installer IBM Global Security Kit avec les utilitaires du système d'exploitation. Pour établir et utiliser des connections sécurisées, vous devez installer GSKit sur les systèmes serveur et client.

Le module GSKit crypt est requis pour la prise en charge du chiffrement de bas niveau. Le module SSL de GSKit est requis pour l'établissement de liaisons de communication sécurisées. Le module GSKit crypt est un prérequis pour le module GSKit SSL.

Le support d'installation d'IBM Security Directory Server contient les modules GSKit suivants pour les différents systèmes d'exploitation :

Remarque : Pour les architectures Solaris x64 et SPARC, les noms des modules GSKit sont les mêmes.

AIX

Nom des modules GSKit (64 bits)

```
GSKit8.gskcrypt64.ppc.rte

GSKit8.gskssl64.ppc.rte
```

Nom des modules GSKit (32 bits)

```
GSKit8.gskcrypt32.ppc.rte

GSKit8.gskssl32.ppc.rte
```

Linux System x

Nom des modules GSKit (32 bits)

```
gskcrypt32-8.0.14.26.linux.x86.rpm

gskssl32-8.0.14.26.linux.x86.rpm
```

Linux System z

Nom des modules GSKit (64 bits)

```
gskcrypt64-8.0.14.26.linux.s390x.rpm

gskssl64-8.0.14.26.linux.s390x.rpm
```

Nom des modules GSKit (32 bits)

```
gskcrypt31-8.0.14.26.linux.s390.rpm

gskssl31-8.0.14.26.linux.s390.rpm
```

Linux System i et System p

Nom des modules GSKit (64 bits)

```
gskcrypt64-8.0.14.26.linux.ppc.rpm

gskssl64-8.0.14.26.linux.ppc.rpm
```

Nom des modules GSKit (32 bits)

```
gskcrypt32-8.0.14.26.linux.ppc.rpm
```

gskssl32-8.0.14.26.linux.ppc.rpm

Linux IA64 (Itanium) et AMD64/EM64T Linux

Nom des modules GSKit (64 bits)

gskcrypt64-8.0.14.26.linux.x86_64.rpm

gskssl64-8.0.14.26.linux.x86_64.rpm

Nom des modules GSKit (32 bits)

gskcrypt32-8.0.14.26.linux.x86.rpm

gskssl32-8.0.14.26.linux.x86.rpm

Solaris

Nom des modules GSKit (64 bits)

gsk8cry64.pkg

gsk8ssl64.pkg

Nom des modules GSKit (32 bits)

gsk8cry32.pkg

gsk8ssl32.pkg

HP-UX (Itanium)

Nom des modules GSKit (64 bits)

gskcrypt64

gskssl64

Nom des modules GSKit (32 bits)

gskcrypt32

gskssl32

Microsoft Windows

Nom des modules GSKit (64 bits)

gsk8crypt64.exe

gsk8ssl64.exe

Nom des modules GSKit (32 bits)

gsk8crypt32.exe

gsk8ssl32.exe

Installation d'IBM Global Security Kit avec la commande `installp`

Vous pouvez utiliser la commande **installp** pour exécuter l'installation d'IBM Global Security Kit sur un système AIX.

Avant de commencer

Accédez au support d'installation d'IBM Security Directory Server pour obtenir le fichier installable d'IBM Global Security Kit. Voir «Préparation du support d'installation», à la page 6.

Pourquoi et quand exécuter cette tâche

Le programme d'installation **installp** installe IBM Global Security Kit (GSKit) sur un système AIX.

Procédure

1. Connectez-vous en tant qu'utilisateur root.
2. Accédez à l'invite de commande.
3. Le répertoire de travail en cours doit être le répertoire `gskit` dans lequel l'installable d'IBM Global Security Kit est stocké.
4. Lancez la commande **installp** pour installer les modules IBM Global Security Kit.
   a. Pour installer les modules GSKit 64 bits, exécutez les commandes suivantes :
      ```
      installp -acgXd . GSKit8.gskcrypt64.ppc.rte
      installp -acgXd . GSKit8.gskssl64.ppc.rte
      ```
   b. Pour installer les modules GSKit 32 bits, exécutez les commandes suivantes :
      ```
      installp -acgXd . GSKit8.gskcrypt32.ppc.rte
      installp -acgXd . GSKit8.gskssl32.ppc.rte
      ```
5. Lancez la commande ci-après pour vérifier si l'installation d'IBM Global Security Kit a réussi.
   ```
   lslpp -aL GSKit8*
   ```

Résultats

Le programme d'installation installe IBM Global Security Kit aux emplacements suivants sur un système AIX :

GSKit 64 bits
`/usr/opt/ibm/gsk8_64/`

GSKit 32 bits
`/usr/opt/ibm/gsk8/`

Installation d'IBM Global Security Kit à l'aide des utilitaires Linux

Utilisez la commande **rpm** pour installer IBM Global Security Kit sur un système Linux.

Avant de commencer

Accédez au support d'installation d'IBM Security Directory Server pour obtenir le fichier installable d'IBM Global Security Kit. Voir «Préparation du support d'installation», à la page 6.

Pourquoi et quand exécuter cette tâche

La commande **rpm** installe IBM Global Security Kit (GSKit) sur un système Linux. L'exemple montre l'installation d'IBM Global Security Kit sous AMD64 Opteron/EM64T Linux. Pour System z, System i ou System p ou System x Linux, remplacez les noms des modules par les noms appropriés.

Procédure

1. Connectez-vous en tant qu'utilisateur root.
2. Accédez à l'invite de commande.
3. Le répertoire de travail en cours doit être le répertoire `gskit` dans lequel l'installable d'IBM Global Security Kit est stocké.
4. Lancez la commande **rpm** pour installer les modules IBM Global Security Kit.

a. Pour installer les modules GSKit 64 bits, exécutez les commandes suivantes :

```
rpm -ivh gskcrypt64-8.0.14.26.linux.x86_64.rpm
rpm -ivh gskssl64-8.0.14.26.linux.x86_64.rpm
```

b. Pour installer les modules GSKit 32 bits, exécutez les commandes suivantes :

```
rpm -ivh gskcrypt32-8.0.14.26.linux.x86.rpm
rpm -ivh gskssl32-8.0.14.26.linux.x86.rpm
```

5. Lancez la commande ci-après pour vérifier si l'installation d'IBM Global Security Kit a réussi.

```
rpm -qa | grep -i gsk
```

Résultats

Le programme d'installation installe IBM Global Security Kit aux emplacements suivants sur un système Linux :

GSKit 64 bits
`/usr/local/ibm/gsk8_64/`

GSKit 32 bits
`/usr/local/ibm/gsk8/`

Installation d'IBM Global Security Kit à l'aide des utilitaires Solaris

Utilisez la commande **pkgadd** pour installer IBM Global Security Kit sur un système Solaris.

Avant de commencer

Accédez au support d'installation d'IBM Security Directory Server. Voir «Préparation du support d'installation», à la page 6.

Pourquoi et quand exécuter cette tâche

La commande **pkgadd** installe IBM Global Security Kit (GSKit) sur un système Solaris. Les noms des modules et des fichiers sont identiques pour les systèmes d'exploitation Solaris SPARC et Solaris X64.

Procédure

1. Connectez-vous en tant qu'utilisateur root.
2. Accédez à l'invite de commande.
3. Le répertoire de travail en cours doit être le répertoire `gskit` dans lequel l'installable d'IBM Global Security Kit est stocké.
4. Lancez la commande **pkgadd** pour installer les modules IBM Global Security Kit.
   a. Pour installer les modules GSKit 64 bits, exécutez les commandes suivantes :

```
pkgadd -d gsk8cry64.pkg
pkgadd -d gsk8ssl64.pkg
```

   b. Pour installer les modules GSKit 32 bits, exécutez les commandes suivantes :

```
pkgadd -d gsk8cry32.pkg
pkgadd -d gsk8ssl32.pkg
```

5. Lancez la commande ci-après pour vérifier si l'installation d'IBM Global Security Kit a réussi.

   ```
   pkginfo | grep -i gsk
   pkgparam nom_module VERSION
   ```

   Remplacez la valeur `nom_module` par le nom du module GSKit pour vérifier la version.

Installation d'IBM Global Security Kit à l'aide des utilitaires HP-UX

Utilisez la commande **swinstall** pour installer IBM Global Security Kit sur un système HP-UX.

Avant de commencer

Accédez au support d'installation d'IBM Security Directory Server pour obtenir le fichier installable d'IBM Global Security Kit. Voir «Préparation du support d'installation», à la page 6.

Procédure

1. Connectez-vous en tant qu'utilisateur root.
2. Accédez à l'invite de commande.
3. Le répertoire de travail en cours doit être le répertoire `gskit` dans lequel l'installable d'IBM Global Security Kit est stocké.
4. Lancez la commande **swinstall** pour installer les modules IBM Global Security Kit.
   a. Pour installer les modules GSKit 64 bits, exécutez les commandes suivantes :

      ```
      swinstall -s path_to_gskit_installable/gskcrypt64 gskcrypt64
      swinstall -s path_to_gskit_installable/gskssl64 gskssl64
      ```

      Vous devez fournir le nom de chemin absolu de l'élément installable de GSKit avec le paramètre **-s**.
   b. Pour installer les modules GSKit 32 bits, exécutez les commandes suivantes :

      ```
      swinstall -s path_to_gskit_installable/gskcrypt32 gskcrypt32
      swinstall -s path_to_gskit_installable/gskssl32 gskssl32
      ```
5. Lancez la commande ci-après pour vérifier si l'installation d'IBM Global Security Kit a réussi.

   ```
   swlist | grep -i gsk
   ```

Installation d'IBM Global Security Kit sous Windows

Lancez le programme d'installation d'IBM Global Security Kit à partir de l'invite de commande pour installer IBM Global Security Kit sur un système Windows.

Avant de commencer

Accédez au support d'installation d'IBM Security Directory Server pour obtenir le fichier installable d'IBM Global Security Kit. Voir «Préparation du support d'installation», à la page 6.

Pourquoi et quand exécuter cette tâche

L'exemple montre l'installation de GSKit crypt 64 bits et de GSKit SSL 64 bits. Pour installer GSKit 32 bits, utilisez les modules correspondants. Sur les systèmes d'exploitation Windows 64 bits, vous pouvez installer des modules GSKit 64 bits et 32 bits.

Procédure

1. Connectez-vous en tant que membre du groupe des administrateurs.
2. Le répertoire de travail en cours doit être le répertoire `gskit` dans lequel l'installable d'IBM Global Security Kit est stocké.
3. Pour installer les modules GSKit 64 bits, exécutez le programme d'installation de GSKit.
   a. Exécutez le module d'installation GSKit8 crypt, `gsk8crypt64.exe`.
   b. Dans la fenêtre d'installation de GSKit8 crypt, procédez comme suit.
      1) Indiquez le chemin d'installation de GSKit8 crypt.
      2) Cliquez sur **Suivant**.
      3) Cliquez sur **Installer**.
      4) Cliquez sur **Terminer**.
   c. Exécutez le module d'installation GSKit8 SSL, `gsk8ssl64.exe`.
   d. Dans la fenêtre d'installation de GSKit8 SSL, procédez comme suit.
      1) Indiquez le chemin d'installation de GSKit8 SSL.
      2) Cliquez sur **Suivant**.
      3) Cliquez sur **Installer**.
      4) Cliquez sur **Terminer**.
4. Pour exécuter les commandes GSKit à partir de la ligne de commande, définissez les répertoires `bin` et `lib64` dans la variable *PATH* sur les systèmes Windows x86_64.

   Remarque : Sous Windows 32 bits, définissez les répertoires `bin` et `lib` dans la variable *PATH*.
   Si l'emplacement d'installation de GSKit est `C:\Program Files\IBM\gsk8`, entrez les valeurs ci-après dans la variable *PATH*.

   ```
   set PATH="C:\Program Files\IBM\gsk8\bin";%PATH%
   set PATH="C:\Program Files\IBM\gsk8\lib64";%PATH%
   ```

Installation silencieuse d'IBM Global Security Kit sous Windows

Lancez le programme d'installation d'IBM Global Security Kit à partir de l'invite de commande pour installer IBM Global Security Kit en mode silencieux sur un système Windows.

Avant de commencer

Accédez au support d'installation d'IBM Security Directory Server pour obtenir le fichier installable d'IBM Global Security Kit. Voir «Préparation du support d'installation», à la page 6.

Pourquoi et quand exécuter cette tâche

L'exemple montre l'installation de GSKit crypt 64 bits et de GSKit SSL 64 bits. Pour installer GSKit 32 bits, utilisez les modules correspondants. Sur les systèmes

d'exploitation Windows 64 bits, vous pouvez installer des modules GSKit 64 bits et 32 bits.

Procédure

1. Connectez-vous en tant que membre du groupe des administrateurs.
2. Accédez à l'invite de commande.
3. Le répertoire de travail en cours doit être le répertoire `gskit` dans lequel l'installable d'IBM Global Security Kit est stocké.
4. Pour installer les modules GSKit 64 bits en mode silencieux, exécutez les commandes suivantes :

   ```
   gsk8crypt64.exe /s /v"/quiet"
   gsk8ssl64.exe /s /v"/quiet"
   ```

5. Pour exécuter les commandes GSKit à partir de la ligne de commande, définissez les répertoires `bin` et `lib64` dans la variable *PATH* sur les systèmes Windows x86_64.

   Remarque : Sous Windows 32 bits, définissez les répertoires `bin` et `lib` dans la variable *PATH*.
   Si l'emplacement d'installation de GSKit est `C:\Program Files\IBM\gsk8`, entrez les valeurs ci-après dans la variable *PATH*.

   ```
   set PATH="C:\Program Files\IBM\gsk8\bin";%PATH%
   set PATH="C:\Program Files\IBM\gsk8\lib64";%PATH%
   ```

Chapitre 11. Installation des modules de langue

Si vous souhaitez afficher les messages du serveur d'annuaire dans des langues autres que l'anglais, vous devez installer les modules de langue correspondants.

IBM Installation Manager peut installer tous les modules de langue disponibles pour le système d'exploitation si vous sélectionnez l'installation d'une fonction dans le programme d'installation. Les modules de langue sont installés dans le sous-répertoire `nls` du répertoire d'installation d'IBM Security Directory Server.

Remarque : Il n'est pas indispensable d'installer les modules de langue pour le client. Installez-les uniquement si vous voulez que les messages des commandes **idslink** et **idsrmlink** s'affichent dans une autre langue que l'anglais. Pour plus d'informations sur les commandes **idslink** et **idsrmlink**, voir le manuel *Command Reference*.

Vous pouvez installer les modules de langue à l'aide d'IBM Installation Manager ou des utilitaires du système d'exploitation sur les systèmes AIX et Linux. L'installation des modules de langue par IBM Installation Manager est fournie avec le programme d'installation complet du produit IBM Security Directory Server.

A faire : L'installation des modules de langue avec IBM Installation Manager n'est prise en charge que sur les système AIX, Linux sur l'architecture AMD64/EM64T, et Microsoft Windows. Sur les ordinateurs qui prennent en charge l'installation d'IBM Security Directory Server par IBM Installation Manager, vous ne devez pas installer les modules de langue manuellement à l'aide des utilitaires du systèmes d'exploitation. Si l'installation des modules de langue avec IBM Installation Manager n'est pas prise en charge par le système d'exploitation, utilisez les utilitaires du système d'exploitation.

Tableau 15. Liste des langues prises en charge sur les systèmes d'exploitation AIX, Linux, Solaris et Windows

Langues	AIX	Linux	Solaris	Microsoft Windows
Tchèque	✓			
Français	✓	✓	✓	✓
Allemand	✓	✓	✓	✓
Hongrois	✓			
Italien	✓	✓	✓	✓
Japonais	✓	✓	✓	✓
Coréen	✓	✓	✓	✓
Polonais	✓			
Portugais (Brésil)	✓	✓	✓	✓
Russe	✓			
Slovaque	✓			
Espagnol	✓	✓	✓	✓
Chinois simplifié	✓	✓	✓	✓
Chinois traditionnel	✓	✓	✓	✓

Module de langue pour l'installation

Avant d'installer un module de langue, vous devez identifier le nom des modules à chaque langue et correspondant à un système d'exploitation.

Langue et nom des modules de langue

A faire : Les modules de langue pour Linux sont pris en charge pour les architectures suivantes :

- System x Linux
- System z Linux
- AMD64 Opteron / Intel EM64T Linux
- Linux System i et System p

A faire : Les modules de langue pour Solaris sont pris en charge pour les architectures suivantes :

- Solaris SPARC
- Solaris X64

Tableau 16. Liste des langues prises en charge et nom des modules de langue pour les systèmes d'exploitation AIX, Linux et Solaris

Langues	AIX	Linux	Solaris
Tchèque	idsldap.msg631.cs_CZ		
Français	idsldap.msg631.fr_FR	idsldap-msg631-fr-6.3.1-0.noarch.rpm	idsldap.msg631.fr.pkg
Allemand	idsldap.msg631.de_DE	idsldap-msg631-de-6.3.1-0.noarch.rpm	idsldap.msg631.de.pkg
Hongrois	idsldap.msg631.hu_HU		
Italien	idsldap.msg631.it_IT	idsldap-msg631-it-6.3.1-0.noarch.rpm	idsldap.msg631.it.pkg
Japonais	idsldap.msg631.ja_JP	idsldap-msg631-ja-6.3.1-0.noarch.rpm	idsldap.msg631.ja.pkg
Coréen	idsldap.msg631.ko_KO	idsldap-msg631-ko-6.3.1-0.noarch.rpm	idsldap.msg631.ko.pkg
Polonais	idsldap.msg631.pl_PL		
Portugais (Brésil)	idsldap.msg631.pt_BR	idsldap-msg631-pt_BR-6.3.1-0.noarch.rpm	idsldap.msg631.pt_BR.pkg
Russe	idsldap.msg631.ru_RU		
Slovaque	idsldap.msg631.sk_SK		
Espagnol	idsldap.msg631.es_ES	idsldap-msg631-es-6.3.1-0.noarch.rpm	idsldap.msg631.es.pkg
Chinois simplifié	idsldap.msg631.zh_CN	idsldap-msg631-zh_CN-6.3.1-0.noarch.rpm	idsldap.msg631.zh_CN.pkg
Chinois traditionnel	idsldap.msg631.zh_TW	idsldap-msg631-zh_TW-6.3.1-0.noarch.rpm	idsldap.msg631.zh_TW.pkg

Installation des modules de langue à l'aide des utilitaires du système d'exploitation

Utilisez les utilitaires du système d'exploitation pour installer les modules de langue si le système d'exploitation ne prend pas en charge leur installation par IBM Installation Manager.

Avant de commencer

Vous devez préparer le support d'installation d'IBM Security Directory Server. Voir «Préparation du support d'installation», à la page 6.

Pourquoi et quand exécuter cette tâche

Si vous souhaitez afficher les messages du serveur d'annuaire dans des langues autres que l'anglais, vous devez installer les modules de langue correspondants.

Procédure

1. Connectez-vous en tant qu'utilisateur root.
2. Accédez à l'invite de commande.
3. Le répertoire de travail en cours doit être celui qui contient l'installable d'IBM Security Directory Server.
4. Accédez au sous-répertoire `tdsLangpack`.
5. Pour installer un module de langue, lancez les commandes d'installation du module. L'exemple suivant montre l'installation du module de langue français. Pour installer les autres modules de langue, remplacez le nom du module par le nom de votre choix correspondant au système d'exploitation.

Système d'exploitation	**Commande à exécuter :**
AIX	`installp -acgXd . idsldap.msg631.fr_FR`
Linux	`rpm -ivh idsldap-msg631-fr-6.3.1-0.noarch.rpm`
Solaris	`pkgadd -d idsldap.msg631.fr.pkg`

6. Vérifiez la bonne installation du module de langue. Pour plus d'informations, voir «Vérification des modules d'IBM Security Directory Server», à la page 87.

Résultats

Le programme d'installation installe les modules de langue dans les répertoires suivants :

Tableau 17. Emplacement d'installation par défaut des modules de langue d'IBM Security Directory Server

Système d'exploitation	**Emplacement d'installation du module de langue**
Linux	`/opt/ibm/ldap/V6.3.1/nls/msg`
AIX et Solaris	`/opt/IBM/ldap/V6.3.1/nls/msg`

Chapitre 12. Installation avec les utilitaires de ligne de commande du système d'exploitation

Vous pouvez installer IBM Security Directory Server à l'aide des utilitaires de ligne de commande du système d'exploitation si votre système ne prend pas en charge X11.

ATTENTION :

- **Les installations sur un ordinateur donné doivent toujours être exécutées avec la même méthode. Vous devez réaliser l'installation d'IBM Security Directory Server avec IBM Installation Manager ou avec les utilitaires de ligne de commande du système d'exploitation, mais pas avec les deux. Si vous mélangez les deux modes d'installation, certains modules de fonction peuvent ne pas s'installer.**
- **Vous devez éviter d'installer manuellement DB2 et Embedded WebSphere Application Server dans le chemin d'installation par défaut utilisé par IBM Installation Manager. Cela pourrait faire échouer les opérations d'installation, de modification ou de désinstallation exécutées avec IBM Installation Manager. Pour plus d'informations sur le chemin d'installation par défaut, voir «Emplacements d'installation par défaut», à la page 27.**

Avant d'installer IBM Security Directory Server, procurez-vous la source de l'installation. Le produit IBM Security Directory Server est disponible sous la forme de fichiers archive ou d'une image installable. Vous pouvez créer des DVD d'installation à partir de l'image installable.

Préparez le support d'installation. Pour plus d'informations, voir «Préparation du support d'installation», à la page 6.

Important : Pour utiliser IBM Security Directory Server en tant que serveur d'annuaire complet, installez une version compatible d'IBM DB2 si cela n'est pas déjà fait. Vous devez configurer le chemin et la version d'IBM DB2 dans le fichier `ldapdb.properties`.

Installation à l'aide des utilitaires AIX

Vous pouvez utiliser les utilitaires de ligne de commande AIX pour installer IBM Security Directory Server sur un système AIX.

Vous pouvez utiliser l'un des utilitaires suivants pour l'installation d'IBM Security Directory Server :

SMIT La méthode d'installation recommandée est celle de l'utilitaire. Pour plus d'informations, voir «Installation avec SMIT», à la page 72.

installp
Pour plus d'informations, voir «Installation avec la commande **installp**», à la page 73.

Modules pour l'installation sur un système AIX

Pour utiliser IBM Security Directory Server en tant que serveur d'annuaire complet, serveur proxy ou client sur un système AIX, vous devez installer les modules appropriés.

Modules et ensembles de fichiers

IBM Security Directory Server contient les modules destinés à un système AIX. Chaque module contient un ou plusieurs ensembles de fichiers.

Tableau 18. Modules et ensembles de fichiers qu'ils contiennent

Module	Ensembles de fichiers associés au module
idsldap.license631	idsldap.license631.rte - Licence
idsldap.cltbase631	• idsldap.cltbase631.rte - Client de base (exécution) • idsldap.cltbase631.adt - Client de base (SDK)
idsldap.clt32bit631	• idsldap.clt32bit631.rte - Client C 32 bits (sans SSL et TLS)
idsldap.clt64bit631	• idsldap.clt64bit631.rte - Client C 64 bits (sans SSL et TLS)
idsldap.clt_max_crypto32bit631	• idsldap.clt_max_crypto32bit631.rte - Client C 32 bits (avec SSL et TLS)
idsldap.clt_max_crypto64bit631	• idsldap.clt_max_crypto64bit631.rte - Client C 64 bits (avec SSL et TLS)
idsldap.cltjava631	• idsldap.cltjava631.rte - Client Java
idsldap.srvbase64bit631	• idsldap.srvbase64bit631.rte - Serveur (Base)
idsldap.srv_max_cryptobase64bit631	• idsldap.srv_max_cryptobase64bit631.rte - Serveur (Base - SSL)
idsldap.srvproxy64bit631	• idsldap.srvproxy64bit631.rte - Serveur proxy 64 bits
idsldap.srv64bit631	• idsldap.srv64bit631.rte - Serveur d'annuaire 64 bits
idsldap.webadmin631	• idsldap.webadmin631.rte - Outil d'administration Web (sans SSL et TLS)
idsldap.webadmin_max_crypto631	• idsldap.webadmin_max_crypto631.rte - Outil d'administration Web (avec SSL et TLS)
idsldap.msg631.en_US	Non disponible
idsldap.ent631	• idsldap.ent631.rte - IBM Directory Server - Droits d'utilisation (fourni uniquement sur Passport Advantage)

Séquence d'installation

Vous pouvez installer toutes les fonctions simultanément. Si vous les installez séparément, vous devez respecter l'ordre indiqué.

Important :

- Si vous voulez utiliser SSL (Secure Socket Layer) ou TLS (Transport Layer Security), vous devez installer une version prise en charge d'IBM Global Security Kit.
- Pour la prise en charge de Kerberos sur les systèmes AIX, une version de Network Authentication Service prise en charge est nécessaire.

Remarque : Si l'ordinateur ne prend pas en charge X11, vous pouvez ignorer l'installation du composant JDK fourni dans IBM JDK. Si le composant JDK n'est pas installé, vous risquez de ne pas pouvoir utiliser l'outil d'administration d'instance ou l'outil de configuration.

Tableau 19. Séquence d'installation de la fonction client

Client 32 bits (sans SSL et TLS)	Client 32 bits (avec SSL et TLS)	Client 64 bits (sans SSL et TLS)	Client 64 bits (avec SSL et TLS)
1. idsldap.cltbase631 2. idsldap.clt32bit631 3. idsldap.cltjava631	1. idsldap.cltbase631 2. idsldap.clt32bit631 3. idsldap.clt_max_crypto32bit631 4. idsldap.cltjava631	1. idsldap.cltbase631 2. idsldap.clt64bit631 3. idsldap.cltjava631	1. idsldap.cltbase631 2. idsldap.clt64bit631 3. idsldap.clt_max_crypto32bit631 4. idsldap.cltjava631

Remarque : Lorsque vous utilisez le fichier archivé Client-Server avec les droits d'utilisation ou une image ISO avec les droits d'utilisation pour l'installation d'IBM Security Directory Server, vous devez d'abord accepter les termes de la licence et installer le module idsldap.license631.

Tableau 20. Séquence d'installation de la fonction de serveur d'annuaire complet

Serveur d'annuaire complet 64 bits (sans SSL et TLS)	Serveur d'annuaire complet 64 bits (avec SSL et TLS)
1. idsldap.license631 2. idsldap.cltbase631 3. idsldap.clt64bit631 4. idsldap.cltjava631 5. idsldap.srvbase64bit631 6. idsldap.srv64bit631 7. idsldap.msg631.en_US 8. idsldap.ent631	1. idsldap.license631 2. idsldap.cltbase631 3. idsldap.clt64bit631 4. idsldap.clt_max_crypto64bit631 5. idsldap.cltjava631 6. idsldap.srvbase64bit631 7. idsldap.srv_max_cryptobase64bit631 8. idsldap.srv64bit631 9. idsldap.msg631.en_US 10. idsldap.ent631

Tableau 21. Séquence d'installation de la fonction de serveur proxy

Serveur proxy 64 bits (sans SSL et TLS)	Serveur proxy 64 bits (avec SSL et TLS)
1. idsldap.license631 2. idsldap.cltbase631 3. idsldap.clt64bit631 4. idsldap.cltjava631 5. idsldap.srvbase64bit631 6. idsldap.srvproxy64bit631 7. idsldap.msg631.en_US 8. idsldap.ent631	1. idsldap.license631 2. idsldap.cltbase631 3. idsldap.clt64bit631 4. idsldap.clt_max_crypto64bit631 5. idsldap.cltjava631 6. idsldap.srvbase64bit631 7. idsldap.srv_max_cryptobase64bit631 8. idsldap.srvproxy64bit631 9. idsldap.msg631.en_US 10. idsldap.ent631

Remarque : Pour utiliser l'outil d'administration Web, vous devez le déployer sur un serveur d'applications Web. Pour plus d'informations sur l'installation d'Embedded WebSphere Application Server, voir «Installation manuelle d'Embedded WebSphere Application Server», à la page 113.

Tableau 22. Module d'installation de l'outil d'administration Web

Outil d'administration Web (sans SSL et TLS)	Outil d'administration Web (avec SSL et TLS)
1. idsldap.license631 2. idsldap.webadmin631	1. idsldap.license631 2. idsldap.webadmin_max_crypto631

Lorsque vous installez l'outil d'administration Web, les fichiers DSML (Directory Services Markup Language) sont aussi copiés sur l'ordinateur. Pour plus d'informations sur DSML, voir Annexe A, «Directory Services Markup Language», à la page 253.

Installation avec SMIT

Utilisez la commande **smit** pour exécuter l'installation d'IBM Security Directory Server sur un système AIX.

Avant de commencer

Vous devez préparer le support d'installation d'IBM Security Directory Server. Voir «Préparation du support d'installation», à la page 6.

Pourquoi et quand exécuter cette tâche

Le programme d'installation **smit** installe IBM Security Directory Server sur un système AIX. Si une version compatible d'IBM DB2 est installée sur le système, le processus d'installation met à jour le chemin et la version de DB2 dans le fichier `ldapdb.properties`.

Procédure

1. Connectez-vous en tant qu'utilisateur root.
2. Accédez à l'invite de commande.
3. Lancez la commande **idsLicense**.

   ```
   ./idsLicense
   ```
4. Si vous acceptez les dispositions du contrat de licence, entrez 1. Vous disposez des options ci-après.
   - 1 : Accepter le contrat de licence.
   - 2 : Refuser le contrat de licence et quitter l'installation.
   - 3 : Imprimer le contrat de licence.
   - 4 : Lire les conditions non-IBM du contrat de licence.
   - 99 : Revenir à l'écran précédent.

   Si vous acceptez les termes du contrat de licence, un fichier `LAPID` et un dossier `license` sont créés dans l'emplacement d'installation d'IBM Security Directory Server. Le dossier license contient les fichiers de licence d'IBM Security Directory Server dans toutes les langues prises en charge.

   Important : Ne modifiez pas le fichier `LAPID` ni les fichiers du dossier license.
5. Lancez la commande **smit install**. La fenêtre **Maintenance et installation de logiciels** s'ouvre.
6. Cliquez sur **Installation et mise à jour des logiciels** > **Installation et mise à jour de tous les niveaux de logiciels disponibles**.
7. Sélectionnez votre support d'installation.
   - Si vous effectuez l'installation à partir du DVD, procédez comme suit.
     a. Cliquez sur **Liste** pour accéder à l'unité contenant les images d'IBM Security Directory Server.
   - Si vous effectuez l'installation à partir du fichier archive non compressé, entrez **.** dans la zone **Répertoire/unité d'entrée pour le logiciel**.

8. Cliquez sur **Do**.
9. Placez le curseur sur **Software to install**, puis procédez comme suit.
   a. Pour installer l'ensemble de fichiers `idsldap`, tapez `idsldap`.
   b. Cliquez sur **Liste** afin d'afficher tous les ensembles de fichiers, puis sélectionnez ceux que vous souhaitez installer.
   c. Cliquez sur **OK**.
10. Pour démarrer l'installation, cliquez sur **OK**.
11. Vérifiez le récapitulatif d'installation à la fin de la sortie pour vous assurer que tous les ensembles de fichiers sélectionnés sont installés.
12. Une fois l'installation terminée, cliquez sur **Done**.
13. Pour quitter le programme **SMIT**, appuyez sur la touche `F12`.
14. Vérifiez que l'installation d'IBM Security Directory Server a abouti. Pour plus d'informations, voir «Vérification des modules d'IBM Security Directory Server», à la page 87.

Résultats

Le programme d'installation installe IBM Security Directory Server dans le répertoire `/opt/IBM/ldap/V6.3.1` du système AIX. Si une version compatible d'IBM DB2 est installée sur le système, le processus d'installation met à jour le chemin et la version de DB2 dans le fichier `ldapdb.properties`.

Que faire ensuite

Après l'installation d'IBM Security Directory Server, vous devez réaliser l'opération suivante :

- Pour utiliser IBM Security Directory Server en tant que serveur d'annuaire complet, créez une instance de serveur d'annuaire. Voir «Création de l'instance de serveur d'annuaire par défaut», à la page 138.
- Pour utiliser IBM Security Directory Server en tant que serveur proxy, créez une instance de serveur proxy. Voir «Création d'une instance de serveur proxy avec des paramètres personnalisés», à la page 148.

Installation avec la commande `installp`

Utilisez la commande **`installp`** pour exécuter l'installation d'IBM Security Directory Server sur un système AIX.

Avant de commencer

Vous devez préparer le support d'installation d'IBM Security Directory Server. Voir «Préparation du support d'installation», à la page 6.

Pourquoi et quand exécuter cette tâche

Le programme d'installation **`installp`** installe IBM Security Directory Server sur un système AIX. Si une version compatible d'IBM DB2 est installée sur le système, le processus d'installation met à jour le chemin et la version de DB2 dans le fichier `ldapdb.properties`.

Procédure

1. Connectez-vous en tant qu'utilisateur root.
2. Accédez à l'invite de commande.

3. A partir du répertoire de travail en cours, passez dans le répertoire où les éléments installables d'IBM Security Directory Server sont stockés.
4. Lancez la commande **idsLicense**.

   ```
   ./idsLicense
   ```

5. Si vous acceptez les dispositions du contrat de licence, entrez 1. Vous disposez des options ci-après.
   - 1 : Accepter le contrat de licence.
   - 2 : Refuser le contrat de licence et quitter l'installation.
   - 3 : Imprimer le contrat de licence.
   - 4 : Lire les conditions non-IBM du contrat de licence.
   - 99 : Revenir à l'écran précédent.

   Si vous acceptez les termes du contrat de licence, un fichier `LAPID` et un dossier `license` sont créés dans l'emplacement d'installation d'IBM Security Directory Server. Le dossier license contient les fichiers de licence d'IBM Security Directory Server dans toutes les langues prises en charge.

   Important : Ne modifiez pas le fichier `LAPID` ni les fichiers du dossier license.
6. Déterminez quels modules IBM Security Directory Server vous souhaitez installer.

   ```
   installp -ld . | grep idsldap
   ```

   La liste de tous les modules installables IBM Security Directory Server s'affiche.
7. Exécutez la commande ci-après pour installer les modules.

   ```
   installp -acgXd . noms_module
   ```

   Pour installer tous les modules d'IBM Security Directory Server à partir du chemin en cours, exécutez la commande ci-après.

   ```
   installp -acgXd . idsldap
   ```

8. Lorsque l'installation est terminée, le système génère un récapitulatif d'installation.
9. Vérifiez que l'installation d'IBM Security Directory Server a abouti. Pour plus d'informations, voir «Vérification des modules d'IBM Security Directory Server» , à la page 87.

Résultats

Le programme d'installation installe IBM Security Directory Server dans le répertoire `/opt/IBM/ldap/V6.3.1` du système AIX. Si une version compatible d'IBM DB2 est installée sur le système, le processus d'installation met à jour le chemin et la version de DB2 dans le fichier `ldapdb.properties`.

Que faire ensuite

Après l'installation d'IBM Security Directory Server, vous devez réaliser les opérations ci-après.

- Pour utiliser IBM Security Directory Server en tant que serveur d'annuaire complet, créez une instance de serveur d'annuaire. Pour plus d'informations, voir «Création de l'instance de serveur d'annuaire par défaut», à la page 138.
- Pour utiliser IBM Security Directory Server en tant que serveur proxy, créez une instance de serveur proxy. Pour plus d'informations, voir «Création d'une instance de serveur proxy avec des paramètres personnalisés», à la page 148.

Installation à l'aide des utilitaires Linux

Vous pouvez utiliser les utilitaires de ligne de commande Linux pour installer IBM Security Directory Server sur un système Linux.

Différents modules d'IBM Security Directory Server correspondent aux différents systèmes d'exploitation et aux différentes architectures. Vous devez sélectionner le module d'installation adapté à votre ordinateur. Pour plus d'informations sur le nom des modules, voir «Modules pour l'installation sur un système Linux».

Modules pour l'installation sur un système Linux

Pour utiliser IBM Security Directory Server en tant que serveur d'annuaire complet, serveur proxy ou client sur un système Linux, vous devez installer les modules appropriés.

Modules destinés aux différents systèmes Linux

Tableau 23. Modules IBM Security Directory Server destinés aux différents systèmes Linux

Modules d'IBM Security Directory Server	AMD64 Opteron/EM64T Linux	System i ou System p	System x	System z
IBM Directory Server - Licence	idsldap-license631-6.3.1-0.x86_64.rpm	idsldap-license631-6.3.1-0.ppc.rpm	idsldap-license631-6.3.1-0.i386.rpm	idsldap-license631-6.3.1-0.s390.rpm
IBM Directory Server - Client de base	idsldap-cltbase631-6.3.1-0.x86_64.rpm	idsldap-cltbase631-6.3.1-0.ppc.rpm	idsldap-cltbase631-6.3.1-0.i386.rpm	idsldap-cltbase631-6.3.1-0.s390.rpm
IBM Directory Server - Client 32 bits	idsldap-clt32bit631-6.3.1-0.x86_64.rpm	idsldap-clt32bit631-6.3.1-0.ppc.rpm	idsldap-clt32bit631-6.3.1-0.i386.rpm	idsldap-clt32bit631-6.3.1-0.s390.rpm
IBM Directory Server - Client 64 bits	idsldap-clt64bit631-6.3.1-0.x86_64.rpm	idsldap-clt64bit631-6.3.1-0.ppc64.rpm	Non disponible	idsldap-clt64bit631-6.3.1-0.s390x.rpm
IBM Directory Server - Client Java	idsldap-cltjava631-6.3.1-0.x86_64.rpm	idsldap-cltjava631-6.3.1-0.ppc.rpm	idsldap-cltjava631-6.3.1-0.i386.rpm	idsldap-cltjava631-6.3.1-0.s390.rpm
IBM Directory Server - Serveur de base	idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm	idsldap-srvbase64bit631-6.3.1-0.ppc64.rpm	idsldap-srvbase32bit631-6.3.1-0.i386.rpm	idsldap-srvbase64bit631-6.3.1-0.s390x.rpm
IBM Directory Server - Serveur proxy	idsldap-srvproxy64bit631-6.3.1-0.x86_64.rpm	idsldap-srvproxy64bit631-6.3.1-0.ppc64.rpm	idsldap-srvproxy32bit631-6.3.1-0.i386.rpm	idsldap-srvproxy64bit631-6.3.1-0.s390x.rpm
IBM Directory Server - Serveur 32 bits	Non disponible	Non disponible	idsldap-srv32bit631-6.3.1-0.i386.rpm	Non disponible
IBM Directory Server - Serveur 64 bits	idsldap-srv64bit631-6.3.1-0.x86_64.rpm	idsldap-srv64bit631-6.3.1-0.ppc64.rpm	Non disponible	idsldap-srv64bit631-6.3.1-0.s390x.rpm
IBM Directory Server - Outil d'administration Web	idsldap-webadmin631-6.3.1-0.x86_64.rpm	idsldap-webadmin631-6.3.1-0.ppc.rpm	idsldap-webadmin631-6.3.1-0.i386.rpm	idsldap-webadmin631-6.3.1-0.s390.rpm
IBM Directory Server - Messages en anglais	idsldap-msg631-en-6.3.1-0.x86_64.rpm	idsldap-msg631-en-6.3.1-0.ppc.rpm	idsldap-msg631-en-6.3.1-0.i386.rpm	idsldap-msg631-en-6.3.1-0.s390.rpm
IBM Directory Server - Droits d'utilisation (fourni uniquement sur Passport Advantage)	idsldap-ent631-6.3.1-0.x86_64.rpm	idsldap-ent631-6.3.1-0.ppc.rpm	idsldap-ent631-6.3.1-0.i386.rpm	idsldap-ent631-6.3.1-0.s390.rpm

Dépendances des modules

L'installation de certains modules nécessite l'installation préalable des éléments dont ils dépendent.

Remarque : Lorsque vous utilisez le fichier archivé Client-Server avec les droits d'utilisation ou une image ISO avec les droits d'utilisation pour l'installation d'IBM Security Directory Server, vous devez d'abord accepter les termes de la licence et installer le module `idsldap-license631-6.3.1-0.arch.rpm`.

Le tableau montre la dépendance des modules sous AMD64 Opteron/EM64T Linux. Pour System z, System i ou System p ou System x Linux, remplacez les noms des modules par les noms appropriés.

Tableau 24. Modules et modules dépendants

Nom du module	Dépend de
idsldap-clt32bit631-6.3.1-0.x86_64.rpm	idsldap-cltbase631-6.3.1-0.x86_64.rpm
idsldap-clt64bit631-6.3.1-0.x86_64.rpm	idsldap-cltbase631-6.3.1-0.x86_64.rpm
idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm	1. idsldap-license631-6.3.1-0.x86_64.rpm 2. idsldap-cltbase631-6.3.1-0.x86_64.rpm 3. idsldap-clt64bit631-6.3.1-0.x86_64.rpm
idsldap-srv64bit631-6.3.1-0.x86_64.rpm	1. idsldap-license631-6.3.1-0.x86_64.rpm 2. idsldap-cltbase631-6.3.1-0.x86_64.rpm 3. idsldap-clt64bit631-6.3.1-0.x86_64.rpm 4. idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm
idsldap-srvproxy64bit631-6.3.1-0.x86_64.rpm	1. idsldap-license631-6.3.1-0.x86_64.rpm 2. idsldap-cltbase631-6.3.1-0.x86_64.rpm 3. idsldap-clt64bit631-6.3.1-0.x86_64.rpm 4. idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm

Séquence d'installation

Vous pouvez installer toutes les fonctions simultanément. Si vous les installez séparément, vous devez respecter l'ordre indiqué.

Important : Si vous voulez utiliser SSL (Secure Socket Layer) ou TLS (Transport Layer Security), vous devez installer une version prise en charge d'IBM Global Security Kit.

AMD64 Opteron/EM64T Linux est utilisé dans l'exemple de séquence d'installation. For System z, System i or System p ou System x Linux, remplacez les noms des modules par les noms appropriés.

Tableau 25. Séquence d'installation de la fonction client

Client 32 bits	Client 64 bits
1. idsldap-cltbase631-6.3.1-0.x86_64.rpm 2. idsldap-clt32bit631-6.3.1-0.x86_64.rpm 3. idsldap-cltjava631-6.3.1-0.x86_64.rpm	1. idsldap-cltbase631-6.3.1-0.x86_64.rpm 2. idsldap-clt64bit631-6.3.1-0.x86_64.rpm 3. idsldap-cltjava631-6.3.1-0.x86_64.rpm

Tableau 26. Séquence d'installation de la fonction de serveur d'annuaire complet et de serveur proxy

Serveur d'annuaire complet 64 bits	Serveur proxy 64 bits
1. idsldap-license631-6.3.1-0.x86_64.rpm	1. idsldap-license631-6.3.1-0.x86_64.rpm
2. idsldap-cltbase631-6.3.1-0.x86_64.rpm	2. idsldap-cltbase631-6.3.1-0.x86_64.rpm
3. idsldap-clt64bit631-6.3.1-0.x86_64.rpm	3. idsldap-clt64bit631-6.3.1-0.x86_64.rpm
4. idsldap-cltjava631-6.3.1-0.x86_64.rpm	4. idsldap-cltjava631-6.3.1-0.x86_64.rpm
5. idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm	5. idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm
6. idsldap-srv64bit631-6.3.1-0.x86_64.rpm	6. idsldap-srvproxy64bit631-6.3.1-0.x86_64.rpm
7. idsldap-msg631-en-6.3.1-0.x86_64.rpm	7. idsldap-msg631-en-6.3.1-0.x86_64.rpm
8. idsldap-ent631-6.3.1-0.x86_64.rpm	8. idsldap-ent631-6.3.1-0.x86_64.rpm

Remarque : Pour utiliser l'outil d'administration Web, vous devez le déployer sur un serveur d'applications Web. Pour plus d'informations sur l'installation d'Embedded WebSphere Application Server, voir «Installation manuelle d'Embedded WebSphere Application Server», à la page 113.

Tableau 27. Module d'installation de l'outil d'administration Web

Outil d'administration Web
1. idsldap-license631-6.3.1-0.x86_64.rpm
2. idsldap-webadmin631-6.3.1-0.x86_64.rpm

Lorsque vous installez l'outil d'administration Web, les fichiers DSML (Directory Services Markup Language) sont aussi copiés sur l'ordinateur. Pour plus d'informations sur DSML, voir Annexe A, «Directory Services Markup Language», à la page 253.

Installation avec les utilitaires Linux

Utilisez la commande **rpm** pour exécuter l'installation d'IBM Security Directory Server sur un système Linux.

Avant de commencer

Vous devez préparer le support d'installation d'IBM Security Directory Server. Voir «Préparation du support d'installation», à la page 6.

Pourquoi et quand exécuter cette tâche

Le programme d'installation **rpm** installe IBM Security Directory Server sur un système Linux. Si une version compatible d'IBM DB2 est installée sur le système, le processus d'installation met à jour le chemin et la version de DB2 dans le fichier `ldapdb.properties`.

Procédure

1. Connectez-vous en tant qu'utilisateur root.
2. Accédez à l'invite de commande.

3. Le répertoire de travail en cours doit être celui qui contient l'installable d'IBM Security Directory Server.
4. Lancez la commande **idsLicense**.

   ```
   ./idsLicense
   ```
5. Si vous acceptez les dispositions du contrat de licence, entrez 1. Vous disposez des options ci-après.
   - 1 : Accepter le contrat de licence.
   - 2 : Refuser le contrat de licence et quitter l'installation.
   - 3 : Imprimer le contrat de licence.
   - 4 : Lire les conditions non-IBM du contrat de licence.
   - 99 : Revenir à l'écran précédent.

   Si vous acceptez les termes du contrat de licence, un fichier `LAPID` et un dossier `license` sont créés dans l'emplacement d'installation d'IBM Security Directory Server. Le dossier license contient les fichiers de licence d'IBM Security Directory Server dans toutes les langues prises en charge.

   Important : Ne modifiez pas le fichier `LAPID` ni les fichiers du dossier license.
6. Exécutez la commande ci-après pour installer le module.

   ```
   rpm -ivh nom_module
   ```

   Pour installer tous les modules d'IBM Security Directory Server, exécutez la commande ci-après.

   ```
   rpm -ivh idsldap*
   ```
7. Vérifiez que l'installation d'IBM Security Directory Server a abouti. Pour plus d'informations, voir «Vérification des modules d'IBM Security Directory Server» , à la page 87.

Résultats

Le programme d'installation installe IBM Security Directory Server dans le répertoire `/opt/ibm/ldap/V6.3.1` du système Linux. Si une version compatible d'IBM DB2 est installée sur le système, le processus d'installation met à jour le chemin et la version de DB2 dans le fichier `ldapdb.properties`.

Que faire ensuite

Après l'installation d'IBM Security Directory Server, vous devez réaliser l'opération suivante :

- Pour utiliser IBM Security Directory Server en tant que serveur d'annuaire complet, créez une instance de serveur d'annuaire. Pour plus d'informations, voir «Création de l'instance de serveur d'annuaire par défaut», à la page 138.
- Pour utiliser IBM Security Directory Server en tant que serveur proxy, créez une instance de serveur proxy. Pour plus d'informations, voir «Création d'une instance de serveur proxy avec des paramètres personnalisés», à la page 148.

Installation à l'aide des utilitaires Solaris

Vous pouvez utiliser les utilitaires de ligne de commande Solaris pour installer IBM Security Directory Server sur un système Solaris.

IBM Security Directory Server fournit le même ensemble de modules pour les ordinateurs avec des architectures différentes. Certains modules sont disponibles

pour les systèmes d'exploitation Sun SPARC Solaris et AMD64 Opteron/EM64T Solaris. Les noms des modules et des fichiers sont identiques pour ces deux systèmes d'exploitation. Pour plus d'informations sur le nom des modules, voir «Modules pour l'installation sur un système Solaris».

Lorsque vous installez les modules d'IBM Security Directory Server, vous ne devez pas utiliser la valeur système par défaut ALL. Si vous choisissez ALL, le système ne prend pas les modules dans le bon ordre, et l'installation échoue.

Modules pour l'installation sur un système Solaris

Pour utiliser IBM Security Directory Server en tant que serveur d'annuaire complet, serveur proxy ou client sur un système Solaris, vous devez installer les modules appropriés.

Modules pour les systèmes Solaris

Important : Les noms des modules et des fichiers sont identiques pour les systèmes d'exploitation Solaris SPARC et AMD64 Opteron/EM64T Solaris.

Tableau 28. Modules IBM Security Directory Server destinés aux différents systèmes Solaris

Modules d'IBM Security Directory Server	Noms de module	Nom du fichier
IBM Directory Server - Licence	IDSllicense631	idsldap-license631.pkg
IBM Directory Server - Client de base	IDSlbc631	idsldap.cltbase631.pkg
IBM Directory Server - Client 32 bits	IDSl32c631	idsldap.clt32bit631.pkg
IBM Directory Server - Client 64 bits	IDSl64c631	idsldap.clt64bit631.pkg
IBM Directory Server - Client Java	IDSljc631	idsldap.cltjava631.pkg
IBM Directory Server - Serveur de base	IDSlbs631	idsldap.srvbase64bit631.pkg
IBM Directory Server - Serveur proxy	IDSl64p631	idsldap.srvproxy64bit631.pkg
IBM Directory Server - Serveur 64 bits	IDSl64s631	idsldap.srv64bit631.pkg
IBM Directory Server - Outil d'administration Web	IDSlweb631	idsldap.webadmin631.pkg
IBM Directory Server - Messages en anglais	IDSlen631	idsldap.msg631.en.pkg
IBM Directory Server - Droits d'utilisation (fourni uniquement sur Passport Advantage)	IDSlent631	idsldap.ent631.pkg

Dépendances des modules

L'installation de certains modules nécessite l'installation préalable des éléments dont ils dépendent.

Tableau 29. Modules et modules dépendants

Nom du module	Dépend de
idsldap.clt32bit631.pkg	idsldap.cltbase631.pkg
idsldap.clt64bit631.pkg	idsldap.cltbase631.pkg
idsldap.srvbase64bit631.pkg	1. idsldap-license631.pkg 2. idsldap.cltbase631.pkg 3. idsldap.clt64bit631.pkg

Tableau 29. Modules et modules dépendants (suite)

Nom du module	Dépend de
idsldap.srv64bit631.pkg	1. idsldap-license631.pkg 2. idsldap.cltbase631.pkg 3. idsldap.clt64bit631.pkg 4. idsldap.srvbase64bit631.pkg
idsldap.srvproxy64bit631.pkg	1. idsldap-license631.pkg 2. idsldap.cltbase631.pkg 3. idsldap.clt64bit631.pkg 4. idsldap.srvbase64bit631.pkg

Séquence d'installation

Lorsque vous installez les modules sur un système Solaris, vous devez respecter l'ordre indiqué.

Important : Si vous voulez utiliser SSL (Secure Socket Layer) ou TLS (Transport Layer Security), vous devez installer une version prise en charge d'IBM Global Security Kit.

Tableau 30. Séquence d'installation de la fonction client

Client 32 bits	Client 64 bits
1. idsldap.cltbase631.pkg 2. idsldap.clt32bit631.pkg 3. idsldap.cltjava631.pkg	1. idsldap.cltbase631.pkg 2. idsldap.clt64bit631.pkg 3. idsldap.cltjava631.pkg

Remarque : Lorsque vous utilisez le fichier archivé Client-Server avec les droits d'utilisation ou une image ISO avec les droits d'utilisation pour l'installation d'IBM Security Directory Server, vous devez d'abord accepter les termes de la licence et installer le module idsldap-license631.pkg.

Tableau 31. Séquence d'installation de la fonction de serveur d'annuaire complet et de serveur proxy

Serveur d'annuaire complet 64 bits	Serveur proxy 64 bits
1. idsldap-license631.pkg 2. idsldap.cltbase631.pkg 3. idsldap.clt64bit631.pkg 4. idsldap.cltjava631.pkg 5. idsldap.srvbase64bit631.pkg 6. idsldap.srv64bit631.pkg 7. idsldap.msg631.en.pkg 8. idsldap.ent631.pkg	1. idsldap-license631.pkg 2. idsldap.cltbase631.pkg 3. idsldap.clt64bit631.pkg 4. idsldap.cltjava631.pkg 5. idsldap.srvbase64bit631.pkg 6. idsldap.srvproxy64bit631.pkg 7. idsldap.msg631.en.pkg 8. idsldap.ent631.pkg

Remarque : Pour utiliser l'outil d'administration Web, vous devez le déployer sur un serveur d'applications Web. Pour plus d'informations sur l'installation d'Embedded WebSphere Application Server, voir «Installation manuelle d'Embedded WebSphere Application Server», à la page 113.

Tableau 32. Module d'installation de l'outil d'administration Web

Outil d'administration Web
1. idsldap-license631.pkg 2. idsldap.webadmin631.pkg

Lorsque vous installez l'outil d'administration Web, les fichiers DSML (Directory Services Markup Language) sont aussi copiés sur l'ordinateur. Pour plus d'informations sur DSML, voir Annexe A, «Directory Services Markup Language», à la page 253.

Installation à l'aide des utilitaires Solaris

Utilisez la commande **pkgadd** pour installer IBM Security Directory Server sur un système Solaris.

Avant de commencer

Accédez au support d'installation d'IBM Security Directory Server. Voir «Préparation du support d'installation», à la page 6.

Pourquoi et quand exécuter cette tâche

Le programme d'installation **pkgadd** installe IBM Security Directory Server sur un système Solaris. Si une version compatible d'IBM DB2 est installée sur le système, le processus d'installation met à jour le chemin et la version de DB2 dans le fichier `ldapdb.properties`.

Procédure

1. Connectez-vous en tant qu'utilisateur root.
2. Accédez à l'invite de commande.
3. Le répertoire de travail en cours doit être celui qui contient l'installable d'IBM Security Directory Server.
4. Lancez la commande **idsLicense**.

   ```
   ./idsLicense
   ```

5. Si vous acceptez les dispositions du contrat de licence, entrez 1. Vous disposez des options ci-après.
   - 1 : Accepter le contrat de licence.
   - 2 : Refuser le contrat de licence et quitter l'installation.
   - 3 : Imprimer le contrat de licence.
   - 4 : Lire les conditions non-IBM du contrat de licence.
   - 99 : Revenir à l'écran précédent.

   Si vous acceptez les termes du contrat de licence, un fichier `LAPID` et un dossier `license` sont créés dans l'emplacement d'installation d'IBM Security Directory Server. Le dossier license contient les fichiers de licence d'IBM Security Directory Server dans toutes les langues prises en charge.

   Important : Ne modifiez pas le fichier `LAPID` ni les fichiers du dossier license.
6. Exécutez la commande ci-après pour installer un module.

Remarque : Les modules d'IBM Security Directory Server doivent être installés dans un ordre spécifique sur un système Solaris. Pour plus d'informations, voir «Modules pour l'installation sur un système Solaris», à la page 79.

```
pkgadd -d nom_module
```

7. Vérifiez que l'installation d'IBM Security Directory Server a abouti. Pour plus d'informations, voir «Vérification des modules d'IBM Security Directory Server» , à la page 87.

Résultats

Le programme d'installation installe IBM Security Directory Server dans le répertoire `/opt/IBM/ldap/V6.3.1` du système Solaris. Si une version compatible d'IBM DB2 est installée sur le système, le processus d'installation met à jour le chemin et la version de DB2 dans le fichier `ldapdb.properties`.

Que faire ensuite

Après l'installation d'IBM Security Directory Server, vous devez réaliser l'opération suivante :

- Pour utiliser IBM Security Directory Server en tant que serveur d'annuaire complet, créez une instance de serveur d'annuaire. Pour plus d'informations, voir «Création de l'instance de serveur d'annuaire par défaut», à la page 138.
- Pour utiliser IBM Security Directory Server en tant que serveur proxy, créez une instance de serveur proxy. Pour plus d'informations, voir «Création d'une instance de serveur proxy avec des paramètres personnalisés», à la page 148.

Installation à l'aide des utilitaires HP-UX

Vous pouvez utiliser les utilitaires de ligne de commande HP-UX pour installer IBM Security Directory Server sur un système HP-UX.

IBM Security Directory Server fournit des modules client seul pour HP-UX sur les systèmes Itanium (serveurs à processeurs Intel IA64). Pour plus d'informations, voir «Modules pour l'installation sur un système HP-UX Itanium».

Modules pour l'installation sur un système HP-UX Itanium

Pour utiliser IBM Security Directory Server en tant que client sur un système HP-UX, vous devez installer les modules appropriés.

Modules pour les systèmes HP-UX

IBM Security Directory Server fournit un module client seul pour HP-UX sur les systèmes Itanium (serveurs à processeurs Intel IA64).

Tableau 33. Modules IBM Security Directory Server destinés aux systèmes HP-UX

Modules d'IBM Security Directory Server	Nom des modules
IBM Directory Server - Client de base	`idsldap.cltbase631.depot`
IBM Directory Server - Client 32 bits	`idsldap.clt32bit631.depot`
IBM Directory Server - Client 64 bits	`idsldap.clt64bit631.depot`
IBM Directory Server - Client Java	`idsldap.cltjava631.depot`
IBM Directory Server - Licence	`idsldap.license631.depot`

Dépendances des modules

L'installation de certains modules nécessite l'installation préalable des éléments dont ils dépendent.

Tableau 34. Modules et modules dépendants

Nom du module	Dépend de
idsldap.clt32bit631.depot	idsldap.cltbase631.depot
idsldap.clt64bit631.depot	idsldap.cltbase631.depot

Séquence d'installation

Lorsque vous installez les modules sur un système HP-UX, vous devez respecter l'ordre indiqué.

Important : Si vous voulez utiliser SSL (Secure Socket Layer) ou TLS (Transport Layer Security), vous devez installer une version prise en charge d'IBM Global Security Kit.

Tableau 35. Séquence d'installation de la fonction client

Client 32 bits	Client 64 bits
1. idsldap.cltbase631.depot 2. idsldap.clt32bit631.depot 3. idsldap.cltjava631.depot	1. idsldap.cltbase631.depot 2. idsldap.clt64bit631.depot 3. idsldap.cltjava631.depot

Installation à l'aide des utilitaires HP-UX

Vous utiliser la commande **swinstall** pour installer IBM Security Directory Server sur un système HP-UX.

Avant de commencer

Vous devez préparer le support d'installation d'IBM Security Directory Server. Voir «Préparation du support d'installation», à la page 6.

Pourquoi et quand exécuter cette tâche

Le programme d'installation **pkgadd** installe IBM Security Directory Server sur un système Solaris. Si une version compatible d'IBM DB2 est installée sur le système, le processus d'installation met à jour le chemin et la version de DB2 dansle fichier `ldapdb.properties`.

Procédure

1. Connectez-vous en tant qu'utilisateur root.
2. Accédez à l'invite de commande.
3. Le répertoire de travail en cours doit être celui qui contient l'installable d'IBM Security Directory Server.
4. Exécutez la commande suivante pour installer les modules.

```
swinstall -s chemin_installable_sds/idsldap.cltbase631.depot \*
swinstall -s chemin_installable_sds/idsldap.clt32bit631.depot \*
swinstall -s chemin_installable_sds/idsldap.clt64bit631.depot \*
swinstall -s chemin_installable_sds/idsldap.cltjava631.depot \*
```

5. Vérifiez que l'installation d'IBM Security Directory Server a abouti. Pour plus d'informations, voir «Vérification des modules d'IBM Security Directory Server» , à la page 87.

Résultats

Le programme d'installation installe IBM Security Directory Server dans le répertoire `/opt/IBM/ldap/V6.3.1` du système HP-UX.

Chapitre 13. Vérification des fonctions d'IBM Security Directory Server

Après l'installation, la modification ou la désinstallation d'IBM Security Directory Server, vous devez vérifier si les fonctions du produit ont été correctement installées, modifiées ou désinstallées.

Vous pouvez utiliser IBM Installation Manager ou les utilitaires du système d'exploitation pour vérifier l'installation, la modification ou la désinstallation.

Vérification des fonctions IBM Security Directory Server à l'aide d'IBM Installation Manager

Utilisez IBM Installation Manager pour vérifier les fonctions d'IBM Security Directory Server et les logiciels corequis installés à l'aide de ce produit.

Procédure

1. Démarrez IBM Installation Manager.

   Windows
   Dans le menu **Démarrer**, cliquez sur **Tous les programmes** > **IBM Installation Manager** > **IBM Installation Manager**.

   AIX et Linux
   Entrez la commande ci-après à l'invite de commande. Modifiez le chemin par défaut suivant si IBM Installation Manager est installé à un emplacement différent.

   ```
   /opt/IBM/InstallationManager/eclipse/IBMIM
   ```

2. Dans la page **IBM Installation Manager**, cliquez sur **Fichier** > **Afficher les modules installés**.
3. Dans la liste des modules et des correctifs installés de la page **Modules installés**, développez **IBM Security Directory Server**.
4. Dans la liste des modules et des correctifs installés, cliquez sur la versiond'IBM Security Directory Server dont vous voulez voir les fonctions .
5. Dans la zone **Détails**, vérifiez l'installation des fonctions et des produits corequis.
6. Pour fermer la page **Modules installés**, cliquez sur **Fermer**.
7. Pour fermer **IBM Installation Manager**, cliquez sur **Fichier** > **Quitter**.

Vérification des fonctions d'IBM Security Directory Server sous Windows

Vous pouvez savoir si l'installation, la modification ou la désinstallation d'IBM Security Directory Server a abouti en vérifiant le registre Microsoft Windows.

Pourquoi et quand exécuter cette tâche

Microsoft Windows conserve dans son registre des entrées qui permettent de suivre la présence des logiciels sur un système Windows. Après l'installation, la modification ou l'installation réussie des fonctions d'IBM Security Directory Server, les entrées du registre sont modifiées et conservent la trace de la dernière mise à

jour du système. ci-après figure un exemple des entrées du registre après une installation réussie des fonctions d'IBM Security Directory Server. Lorsque vous modifiez ou désinstallez les fonctions d'IBM Security Directory Server, les entrées du registre qui correspondent aux fonctions sont modifiées et montrent le dernier statut des fonctions. Les entrées de registre sont celles de Microsoft Windows sur une architecture AMD64/EM64T.

Procédure

1. Connectez-vous au système Windows avec les privilège d'administrateur.
2. Accédez à l'invite de commande, et entrez la commande ci-après.
   ```
   regedit
   ```
3. Dans la fenêtre **Editeur du Registre**, cliquez sur **Poste de travail** > **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **Wow6432NODE** > **IBM** > **IDSLDAP** > **6.3.1**.

   Remarque : Pour vérifier l'installation IBM Security Directory Server sur un système Microsoft Windows sur une architecture Intel x86 (IA32), développez **Poste de travail** > **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **IBM** > **IDSLDAP** > **6.3.1**.
   `Poste de travail\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1` montre les versions principales des fonctions d'IBM Security Directory Server qui sont installées sur le système.

   ```
   BaseServerMajorVersion      6.3.1
   BitMode   64
   ClientMajorVersion          6.3.1
   JavaClientMajorVersion      6.3.1
   LDAPHome                    rép_installation
   ProxyServerMajorVersion     6.3.1
   ServerMajorVersion          6.3.1
   WebadminMajorVersion        6.3.1
   WebSphereAppSrvMajorVersion 7.0
   ```

   Les versions secondaires des fonctions d'IBM Security Directory Server qui sont installées sur le système figurent sous `Poste de travail\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1`. Par exemple :

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\BaseServer\
            BaseServerMinorVersion 1.0

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\Client\
            ClientMinorVersion 1.0

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\JavaClient\
            JavaClientMinorVersion 1.0

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\ProxyServer\
            ProxyServerMinorVersion 1.0

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\Server\
            ServerMinorVersion 1.0

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\Webadmin\
            WebadminMinorVersion 1.0

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\WebSphereAppSrv\
            WebSphereAppSrvMinorVersion 0.25
   ```
4. Pour fermer la fenêtre **Editeur du Registre**, cliquez sur **Fichier** > **Quitter**.

Vérification des modules d'IBM Security Directory Server

Vous pouvez savoir si l'installation d'IBM Security Directory Server a abouti en vérifiant les modules d'IBM Security Directory Server sur le système.

Pourquoi et quand exécuter cette tâche

Après l'installation d'IBM Security Directory Server, vous devez vérifier que les modules sont au niveau requis : Vous pouvez interroger les numéros de version des modules d'IBM Security Directory Server.

Procédure

1. Connectez-vous en tant qu'utilisateur root.
2. Accédez à l'invite de commande, et entrez la commande ci-après.

Système d'exploitation	Commande d'interrogation des modules :
AIX	`lslpp -l 'idsldap*'`
Linux	`rpm -qa | grep -i idsldap`
Solaris	`pkginfo | grep IDSl` `pkgparam nom_module VERSION`
HP-UX	`swlist | grep -i idsldap`

Résultats

La commande liste les modules d'IBM Security Directory Server qui sont installés sur le système.

Vérification de la version de l'outil d'administration Web

Pour vérifier si l'installation ou la mise à niveau de l'outil d'administration Web a réussi, vous devez vérifier sa version.

Procédure

1. Connectez-vous avec les privilèges d'administrateur.
2. Accédez au répertoire *rép_installation_ds*`/idstools`. *rép_installation_ds* est l'emplacement d'installation d'IBM Security Directory Server. Les emplacements suivants sont les emplacements par défaut pour différents systèmes d'exploitation :

Tableau 36. Emplacement d'installation par défaut d'IBM Security Directory Server sur différents systèmes d'exploitation

Systèmes d'exploitation	Emplacement d'installation par défaut
Microsoft Windows	`c:\Program Files\IBM\ldap\V6.3.1`
AIX et Solaris	`/opt/IBM/ldap/V6.3.1`
Linux	`/opt/ibm/ldap/V6.3.1`

3. Exécutez la commande ci-après.

Systèmes d'exploitation	Commande à exécuter :
Microsoft Windows	`deploy_IDSWebApp.bat -v`
AIX, Linux et Solaris	`deploy_IDSWebApp -v`

La commande affiche les informations suivantes :

- La version et la date de la commande **deploy_IDSWebApp**.
- La version et la date du fichier IDSWebApp.war installé.
- La version et la date du fichier IDSWebApp.war déployé.

Que faire ensuite

Vous devez vérifier les valeurs ci-après.

1. Vérifiez si la version et la date du fichier IDSWebApp.war installé sont différentes de celles du fichier IDSWebApp.war déployé.
2. Si les valeurs sont différentes, déployez la dernière version de l'outil d'administration Web sur le serveur d'applications Web.

Vérification de l'installation d'IBM Global Security Kit sous Windows

Sous Windows, vérifiez la bonne installation d'IBM Global Security Kit (GSKit) à l'aide du statut de l'installation.

Procédure

1. Accédez au fichier gskitinst.log.

Système d'exploitation	Chemin d'accès par défaut :
Windows	C:\Program Files\IBM\ldap\V6.3.1\var

2. Vérifiez si le répertoire suivant a été créé : C:\Program Files\IBM\gsk8
3. Vérifiez si le fichier gskitinst.log contient la valeur EXIT 0. Si l'installation d'IBM Global Security Kit est réussie, la valeur 0 est définie. Dans le cas contraire, la valeur est différente de 0.
4. Facultatif : Si l'installation d'IBM Global Security Kit a échoué, les détails de l'erreur sont enregistrés dans le fichier C:\Program Files\IBM\ldap\V6.3.1\var\gskitinsterr.log.

Vérification de l'installation d'IBM Global Security Kit sous AIX, Linux, Solaris et HP-UX

Vérifiez que l'installation d'IBM Global Security Kit (GSKit) est correcte.

Pourquoi et quand exécuter cette tâche

Après l'installation d'IBM Global Security Kit, vous devez vérifier que les modules sont au niveau requis : Vous pouvez interroger le numéro de version d'IBM Global Security Kit.

Procédure

1. Connectez-vous en tant qu'utilisateur root.
2. Accédez à l'invite de commande, et entrez la commande ci-après.

Système d'exploitation	Commande à exécuter :
AIX	lslpp -al | grep -i gsk
Linux	rpm -qa | grep -i gsk
Solaris	pkginfo | grep gsk pkgparam nom_module VERSION

Système d'exploitation	Commande à exécuter :
HP-UX	`swlist | grep -i gsk`

Chapitre 14. Mise à niveau d'une instance d'une version précédente

Pour convertir une instance existante en instance fonctionnelle d'une version plus récente tout en conservant les fichiers de configuration existants, vous devez réaliser une mise à niveau de l'instance.

Le processus de mise à niveau conserve les modifications apportées aux définitions de schéma et aux fichiers de configuration, ainsi que les données d'une instance de serveur d'annuaire.

La mise à niveau d'une instance d'une version précédente se fait par la procédure suivante :

1. Installez IBM Security Directory Server.
2. Mettez à niveau l'instance d'une version précédente.

Le serveur et le client IBM Security Directory Server version 6.3.1 peuvent coexister avec les serveurs et les clients des versions 6.0, 6.1, 6.2 et 6.3.

Vous pouvez mettre à niveau directement des instances de serveur d'annuaire à partir des versions suivantes vers IBM Security Directory Server version 6.3.1 :

- IBM Security Directory Server version 6.3
- IBM Security Directory Server version 6.2
- IBM Security Directory Server version 6.1

Important : La mise à niveau directe des instances d'IBM Security Directory Server version 6.0 vers IBM Security Directory Server version 6.3.1 n'est pas prise en charge. Vous pouvez mettre à niveau des instances 6.0 vers 6.1, 6.2 ou 6.3, puis vers 6.3.1.

Vous disposez des méthodes suivantes pour mettre à niveau une instance d'une version précédente :

- Mise à niveau d'une instance existante sur un ordinateur local à l'aide de l'outil d'administration d'instance (**idsxinst**) d'IBM Security Directory Server ou de la commande **idsimigr**. Vous ne devez pas supprimer l'instance de serveur d'annuaire que vous souhaitez mettre à niveau. Pour une instance de serveur d'annuaire complet, n'annulez pas la configuration de la base de données. La mise à niveau n'est pas prise en charge si l'instance de serveur d'annuaire est désinstallée ou si la configuration de sa base de données est annulée.
- Mise à niveau d'une instance sur un ordinateur distant à l'aide des commandes **migbkup** et **idsimigr**. Pour plus d'informations, voir «Mise à niveau d'une instance distante d'une version précédente à l'aide de la commande **idsimigr**», à la page 97.

Avertissement : Pour pouvoir effectuer une reprise en cas d'échec de la mise à niveau, vous devez sauvegarder les fichiers de schéma et de configuration et la base de données de l'instance.

Mise à niveau de la base de données DB2

Lorsque vous mettez à niveau une instance, la base de données associée est également mise à niveau si la version de DB2 est inférieure à la version prise en charge par IBM Security Directory Server version 6.3.1. La commande **idsdbmigr** s'exécute en interne pour mettre à niveau la base de données DB2.

Important : La mise à niveau directe d'une instance de serveur d'annuaire qui est configurée avec DB2 version 9.1, vers une instance dotée de DB2 version 10.1.0.2 ou d'une version suivante, n'est pas prise en charge. Vous pouvez mettre à niveau une instance configurée avec DB2 version 9.1, vers une instance dotée de DB2 version 10.1.0.2 ou d'une version suivante, en utilisant l'une des méthodes suivantes :

- Mettez à niveau l'instance dotée de DB2 version 9.1 vers une instance dotée de DB2 version 9.5, puis vers une instance dotée de DB2 version 10.1.0.2 ou d'une version suivante.
- Mettez à niveau l'instance dotée de DB2 version 9.1 vers une instance dotée de DB2 version 9.7, puis vers une instance dotée de DB2 version 10.1.0.2 ou d'une version suivante.

Mise à niveau d'une installation client

Si vous avez installé les fonctions client seul à l'aide du programme d'installation du client IBM Security Directory Server, la mise à niveau n'est pas nécessaire. Les clients des version 6.0, 6.1, 6.2 et 6.3 peuvent coexister avec le serveur et le client de la version 6.3.1.

Configuration de l'environnement avant la mise à niveau d'une instance

Vous devez configurer l'environnement du serveur d'annuaire avant de mettre à niveau une instance existante.

Avant de commencer

Vous devez effectuer les tâches suivantes avant de configurer l'environnement :

- Accédez au support d'installation d'IBM Security Directory Server.
- Installez IBM Security Directory Server version 6.3.1. Voir «Démarrage de l'installation», à la page 28.
- Connectez-vous en tant qu'utilisateur root sur les systèmes d'exploitation AIX, Linux ou Solaris, et en tant que membre du groupe des administrateurs sur le système d'exploitation Windows.

Procédure

1. Vérifiez que le système d'exploitation de l'instance à mettre à niveau est pris en charge par IBM Security Directory Server version 6.3.1.
2. Vérifiez que l'instance de la version précédente à mettre à niveau démarre normalement. Pour mettre à niveau une instance de serveur d'annuaire, vous devez configurer la base de données si cela n'est pas déjà fait.

   Avertissement : La mise à niveau d'un serveur proxy ou d'un serveur d'annuaire n'est pas prise en charge si le serveur ne démarre pas normalement.

3. Effectuez une sauvegarde hors ligne de l'instance à mettre à niveau. Pour une instance de serveur d'annuaire, sauvegardez les bases de données et les paramètres DB2. Pour plus d'informations, voir la commande **idsdbback** dans le manuel *Command Reference*.
4. Pour sauvegarder les fichiers de schéma et de configuration, exécutez la commande **migbkup** :

Système d'exploitation	Commande à exécuter :
Microsoft Windows	**migbkup.bat** unité\idsslapd-nom_instance rép_sauvegarde
AIX, Linux et Solaris	**migbkup** rép_base_utilisateur/idsslapd-nom_instance rép_sauvegarde

La commande **migbkup** est dans le sous-répertoire tools du support d'installation d'IBM Security Directory Server. Si l'installation d'IBM Security Directory Server est terminée, la commande **migbkup** est dans le dossier sbin du répertoire d'installation d'IBM Security Directory Server. Voici le répertoire d'installation par défaut sur différents systèmes d'exploitation :

Microsoft Windows
C:\Program Files\IBM\ldap\V6.3.1

AIX et Solaris
/opt/IBM/ldap/V6.3.1

Linux /opt/ibm/ldap/V6.3.1

La commande **migbkup** sauvegarde les fichiers suivants :

- ibmslapd.conf
- V3.config.at
- V3.config.oc
- V3.ibm.at
- V3.ibm.oc
- V3.system.at
- V3.system.oc
- V3.user.at
- V3.user.oc
- V3.modifiedschema
- V3.ldapsyntaxes
- V3.matchingrules
- ibmslapdcfg.ksf
- ibmslapddir.ksf
- perftune_stat.log
- perftune_input.conf
- ibmdiradmService.cmd (pour Windows)
- ibmslapdService.cmd (pour Windows)

La commande **migbkup** crée les fichiers suivants :

- db2info contient le chemin et la version de l'instance de DB2 qui est utilisée par l'instance de serveur d'annuaire. La commande **idsimigr** ou l'outil d'administration d'instance utilise ce fichier pour mettre à niveau l'instance et

la base de données DB2 lorsque vous mettez à niveau une instance de serveur d'annuaire. Ce fichier n'est pas disponible pour les instances de serveur proxy.
- `platforminfo` contient les informations relatives au système d'exploitation et au type de processus.

5. Si vous avez modifié manuellement le fichier `V3.modifiedschema` d'une instance pour une mise à niveau, le fichier ne doit contenir aucun identificateur d'objet (OID) pour les classes d'objet ou les attributs. Si le fichier contient des identificateurs d'objet en double, ils ne sont pas conservés pendant la mise à niveau. Si les fichiers de schéma en contiennent, les identificateurs d'objet de `V3.modifiedschema` sont conservés. Si les fichiers de schéma ne contiennent pas les attributs ou les classes d'objets, le démarrage du serveur d'administration ou du processus `idsslapd` peut échouer. Dans ce cas, vous devez ajouter manuellement les classes d'objets ou les attributs manquants dans les fichiers de schéma avant de démarrer les serveurs.
6. Si vous avez configuré l'instance avec des fichiers de schéma personnalisés, copiez ces fichiers manuellement dans le répertoire de sauvegarde. Lorsque vous sauvegardez les fichiers de schéma et de configuration, la commande **migbkup** sauvegarde les fichiers de schéma personnalisés. Cependant, ces fichiers ne sont pas forcément utilisés lors de la mise à niveau de l'instance.

Que faire ensuite

Lorsque vous avez configuré l'environnement, lancez la commande **idsimigr** ou l'outil d'administration d'instance pour mettre à niveau une instance à partir d'une version précédente. Pour mettre à niveau une instance, utilisez l'une des méthodes suivantes :

- «Mise à niveau d'une instance d'une version précédente à l'aide de la commande **idsimigr**»
- «Mise à niveau d'une instance d'une version précédente à l'aide de l'outil d'administration d'instance», à la page 153

Mise à niveau d'une instance d'une version précédente à l'aide de la commande `idsimigr`

Utiliser la commande **idsimigr** pour mettre à niveau une instance de serveur de répertoire ou de serveur proxy d'une version précédente.

Avant de commencer

Vous devez effectuer les tâches suivantes avant de mettre à niveau une instance à l'aide de la commande **idsimigr** :

- Terminez l'installation d'IBM Security Directory Server. Voir «Démarrage de l'installation», à la page 28.
- Avant de mettre à niveau une instance, configurez l'environnement. Voir «Configuration de l'environnement avant la mise à niveau d'une instance», à la page 92.
- Connectez-vous en tant qu'utilisateur root sur les systèmes d'exploitation AIX, Linux ou Solaris, et en tant que membre du groupe des administrateurs sur le système d'exploitation Windows.

Vous pouvez aussi mettre à niveau une instance existant sur un ordinateur à l'aide de l'outil d'administration d'instance. Pour plus d'informations, voir «Mise à

niveau d'une instance d'une version précédente à l'aide de l'outil d'administration d'instance», à la page 153.

Pourquoi et quand exécuter cette tâche

Une fois la mise à niveau à partir d'une version précédente effectuée, l'instance devient une instance parfaitement fonctionnelle d'IBM Security Directory Server.

Procédure

1. Accédez à l'invite de commande.
2. Accédez au répertoire `sbin`. Voici le répertoire d'installation par défaut sur les différents systèmes d'exploitation :

   Microsoft Windows
   `C:\Program Files\IBM\ldap\V6.3.1\sbin`

   AIX et Solaris
   `/opt/IBM/ldap/V6.3.1/sbin`

   Linux `/opt/ibm/ldap/V6.3.1/sbin`
3. Arrêtez le processus `ibmslapd` et le serveur d'administration de l'instance que vous voulez mettre à niveau.

   ```
   ibmslapd -I nom_instance -k
   ibmdiradm -I nom_instance -k
   ```
4. Ne désinstallez pas la version de produit d'IBM Security Directory Server qui est associée à l'instance que vous voulez mettre à niveau.
5. Exécutez la commande **idsimigr** pour mettre à niveau l'instance vers la version actuelle d'IBM Security Directory Server.

   ```
   idsimigr -I nom_instance
   ```
6. Démarrez le processus `ibmslapd` et le serveur d'administration de l'instance.

   ```
   ibmslapd -I nom_instance -n
   ibmdiradm -I nom_instance
   ```
7. Effectuez une sauvegarde hors ligne de l'instance. Voir «Sauvegarde du serveur d'annuaire», à la page 194.

Mise à niveau d'une instance d'une version précédente vers un autre ordinateur

Vous pouvez mettre à niveau une instance existante d'une version précédente qui se trouve sur un ordinateur sur un autre ordinateur.

Vous pouvez vouloir mettre à niveau à distance une instance existante pour les raisons suivantes :

- Le système d'exploitation d'un ordinateur sur lequel existe une instance d'une version précédente n'est pas pris en charge par IBM Security Directory Server version 6.3.1. Vous ne souhaitez pas forcément mettre à niveau ou modifier le système d'exploitation sur l'ordinateur.
- Vous voulez installer IBM Security Directory Server version 6.3.1 sur un ordinateur dont le système d'exploitation diffère de celui sur lequel une version précédente existe. Cependant, vous voulez créer une instance avec ces informations, en tant qu'instance d'une version précédente. Par exemple, vous avez une instance existante d'une version précédente sur un système Linux AMD64/EM64T, mais vous voulez installer le serveur 6.3.1 sur un système AIX. Dans ce cas, les deux systèmes d'exploitation doivent être du même type endian. Si le premier ordinateur est de type little endian, le second système doit

également être de type little endian. Le type endian varie selon l'organisation des bits utilisés pour représenter les données en mémoire. Si les systèmes d'exploitation n'ont pas le même type endian, la mise à niveau d'une instance n'est pas prise en charge.

La procédure de mise à niveau à distance est similaire à la procédure de mise à niveau locale (sur le même ordinateur). Il existe cependant une différence, qui est que vous devez copier les fichiers de sauvegarde de l'ordinateur sur lequel vous avez installé IBM Security Directory Server version 6.3.1.

Remarque : Si vous mettez à niveau une instance distante à partir d'un ordinateur qui participe à une réplication, effectuez les opérations ci-après.

- Activez la réplication avec le système source comme fournisseur.
- Activez la réplication avec le système cible comme consommateur.

La réplication permet de s'assurer que les mises à jour sont placées en file d'attente et peuvent être répliquées lors de la mise en ligne du système cible. Vous devez activer la réplication avant de sauvegarder une instance sur le système source.

Systèmes d'exploitation pris en charge pour la mise à niveau d'une instance distante

Pour mettre à niveau une instance distance sur le système d'exploitation cible approprié, vous devez identifier les systèmes d'exploitation source et cible de l'instance.

Tableau 37. Systèmes d'exploitation source et cible pris en charge pour la mise à niveau d'une instance distante

	Système d'exploitation : système cible (IBM Security Directory Server version 6.3.1)								
Système d'exploita--tion : système source (IBM Security Directory Server 6.3 ou version anté--rieure) ↓	**Intel 32 bits Windows**	**AMD64/ EM64T Windows**	**System x Linux (32 bits)**	**AMD64/ EM64T Linux**	**Linux System i et System p**	**Linux System z**	**AIX**	**Solaris SPARC**	**Solaris X64**
Windows Intel 32 bits	✓	✓	✓	✓					✓
Windows AMD/ EM64T	✓	✓	✓	✓					✓
Linux System x (32 bits)	✓	✓	✓	✓					✓
AMD/ EM64T Linux	✓	✓	✓	✓					✓
Linux System i et System p					✓	✓	✓	✓	

Tableau 37. Systèmes d'exploitation source et cible pris en charge pour la mise à niveau d'une instance distante (suite)

	Système d'exploitation : système cible (IBM Security Directory Server version 6.3.1)								
Système d'exploita--tion : système source (IBM Security Directory Server 6.3 ou version anté--rieure) ↓	**Intel 32 bits Windows**	**AMD64/ EM64T Windows**	**System x Linux (32 bits)**	**AMD64/ EM64T Linux**	**Linux System i et System p**	**Linux System z**	**AIX**	**Solaris SPARC**	**Solaris X64**
System z Linux					✓	✓	✓	✓	
AIX					✓	✓	✓	✓	
Solaris SPARC					✓	✓	✓	✓	
Solaris X64	✓	✓	✓	✓					✓

Mise à niveau d'une instance distante d'une version précédente à l'aide de la commande `idsimigr`

Utilisez la commande **idsimigr** avec le paramètre **-u** pour mettre à niveau vers la version 6.3.1 une instance distante de serveur d'annuaire ou de serveur proxy d'une version précédente.

Avant de commencer

Vous devez effectuer les tâches suivantes avant de mettre à niveau une instance à l'aide de la commande **idsimigr** et du paramètre **-u** :

- Avant de mettre à niveau une instance, configurez l'environnement. Voir «Configuration de l'environnement avant la mise à niveau d'une instance», à la page 92.
- Connectez-vous en tant qu'utilisateur root sur les systèmes d'exploitation AIX, Linux ou Solaris, et en tant que membre du groupe des administrateurs sur le système d'exploitation Windows.

Vous pouvez aussi mettre à niveau une instance distante avec des fichiers de configuration en utilisant l'outil d'administration d'instance. Pour plus d'informations, voir «Mise à niveau d'une instance distante d'une version précédente à l'aide de l'outil d'administration d'instance», à la page 154.

Pourquoi et quand exécuter cette tâche

Lorsque le processus de mise à niveau est terminé, la commande **idsimigr** crée sur le poste une instance à la version 6.3.1 en utilisant les informations de l'instance distante.

Procédure

1. A l'aide de la commande **idsdb2ldif**, sauvegardez la base de données de l'instance de serveur d'annuaire qui se trouve sur l'ordinateur distant.

Important : Si vous mettez à niveau une instance de serveur proxy, ne sauvegardez pas la base de données. Aucune base de données n'est associée à un serveur proxy.

```
idsdb2ldif -I nom_instance -o sortie_instance.ldif
```

Pour plus d'informations sur la commande **idsdb2ldif**, consultez le manuel *Command Reference*.

2. Terminez l'installation d'IBM Security Directory Server sur l'ordinateur sur lequel vous voulez mettre à jour l'instance distante. Voir «Démarrage de l'installation», à la page 28.
3. Pour sauvegarder les fichiers de schéma et de configuration de l'instance distante, exécutez la commande **migbkup** de la version cible de la mise à niveau :

Système d'exploitation	Commande à exécuter :
Microsoft Windows	**migbkup.bat** unité\idsslapd-nom_instance rép_sauvegarde
AIX, Linux et Solaris	**migbkup** rép_base_utilisateur/idsslapd-nom_instance rép_sauvegarde

La commande **migbkup** est dans le sous-répertoire tools du support d'installation d'IBM Security Directory Server.

4. Copiez le répertoire de sauvegarde, rép_sauvegarde, que vous avez créé avec **migbkup**, de l'ordinateur distant vers l'ordinateur sur lequel IBM Security Directory Server est installé.
5. Facultatif : Copiez le fichier de sauvegarde de la base de données inst_out.ldif, de l'ordinateur distant vers l'ordinateur sur lequel IBM Security Directory Server est installé.
6. Lancez la commande **idsimigr** avec le paramètre **-u** pour créer une instance avec les données de sauvegarde de l'instance distante.

   ```
   idsimigr -u rép_sauvegarde
   ```

7. Configurez la base de données, le suffixe et le nom distinctif et le mot de passe de l'administrateur de l'instance de serveur d'annuaire.

   Important : Si vous mettez à niveau une instance de serveur proxy, ne lancez pas la commande **idscfgdb** pour configurer une base de données.

   ```
   idscfgdb -I nom_instance –a ID_admin_bd –w mdp_admin_bd –t nom_bd –l emplacement_bd
   idscfgsuf -I nom_instance –s suffixe
   idsdnpw -I nom_instance –u DN_admin –p mdp_admin
   ```

8. Facultatif : Exécutez la commande **idsldif2db** pour importer le fichier de sauvegarde de base de données, sortie_instance.ldif, dans l'instance de serveur d'annuaire mise à niveau.
9. Démarrez le processus ibmslapd et le serveur d'administration de l'instance.

   ```
   ibmslapd -I nom_instance -n
   ibmdiradm -I nom_instance
   ```

10. Sauvegardez l'instance. Pour plus d'informations, voir «Sauvegarde du serveur d'annuaire», à la page 194.

Liens aux utilitaires client et serveur

Vous pouvez employer la commande **idslink** pour définir les liens aux utilitaires de ligne de commande du serveur et aux bibliothèques.

Après avoir installé IBM Security Directory Server, vous pouvez définir des liens vers les utilitaires client et serveur. Ces liens ne sont pas définis automatiquement pendant l'installation.

Si vous aviez configuré des liens vers les utilitaires d'une version précédente d'IBM Security Directory Server, ceux-ci restent tant que vous ne les modifiez pas. Pour supprimer les liens définis par la commande `idslink`, utilisez la commande **idsrmlink**.

Vous pouvez utiliser la commande **idslink** pour définir les liens aux utilitaires de ligne de commande (par exemple **idsldapmodify** et **idsldapadd**) et aux bibliothèques (par exemple `libibmldap.so`). Ces liens pointent vers l'emplacement des utilitaires et des bibliothèques IBM Security Directory Server.

Pour plus d'informations sur les commandes **idslink** et **idsrmlink**, voir le manuel *Command Reference*.

Chapitre 15. Migration des données et des solutions d'une instance d'une version précédente

Vous pouvez migrer des données d'annuaire et/ou des solutions qui sont configurées avec une instance d'une version précédente pour les utiliser dans la version 6.3.1.

Migration des données DB2 data depuis IBM DB2 Enterprise Server Edition (ESE) vers IBM DB2 Workspace Server Edition (WSE)

Sous System x Linux (architecture Intel 32 bits), IBM DB2 ESE versions 9.7 et suivantes n'est pas pris en charge. Sous System x Linux, IBM Security Directory Server utilise IBM DB2 WSE version 9.7, Fix Pack 6 ou groupe de correctif ultérieur, pour créer et configurer la base de données.

Lorsque vous mettez à niveau un instance de la version 6.1 ou 6.2 contenant des données vers la version 6.3.1, vous pouvez être amené à exécuter la mise à niveau à distance de l'instance. Vous pouvez mettre à niveau une instance 6.3 avec DB2 WSE version 9.7 ou version ultérieure vers une instance 6.3.1 avec DB2 WSE version 9.7 ou ultérieure. Sous System x Linux, la mise à niveau directe d'une instance 6.1 ou 6.2 avec DB2 ESE version 9.1 ou ultérieure vers une instance 6.3.1 avec DB2 WSE version 9.7 ou ultérieure peut échouer. Pour plus d'informations sur la façon de migrer une base de données DB2 ESE vers DB2 WSE, voir «Migration d'une instance avec une base de données DB2 ESE vers une instance avec une base de données DB2 WSE», à la page 102.

Migration des solutions de serveur d'annuaire basées sur IBM Security Directory Integrator

Pour utiliser dans une instance 6.3.1 des solutions configurées avec une version d'instance précédente, vous devez migrer ces solutions.

Les solutions suivantes sont prises en charge :

- L'outil de gestion des journaux
- Le protocole SNMP (Simple Network Management Protocol)
- La synchronisation Active Directory

Pour plus d'informations sur les solutions de serveur d'annuaire, consultez la rubrique *Administration* dans la documentation du produit IBM Security Directory Server.

Pour que la solution fonctionne, l'ordinateur doit contenir IBM Security Directory Integrator version 7.1. Pour plus d'informations sur l'installation et l'administration d'IBM Security Directory Integrator, consultez la section *Installation et administration* de la documentation du produit à l'adresse http://www-01.ibm.com/support/knowledgecenter/SSCQGF/welcome.

Si le chemin d'installation d'IBM Security Directory Integrator est différent du chemin d'installation par défaut, définissez-le dans la variable *IDS_LDAP_TDI_HOME*. Les chemins d'installation suivants sont les chemins par défaut pour IBM Security Directory Integrator version 7.1 sur les différents systèmes d'exploitation :

AIX, Linux et Solaris

```
/opt/IBM/TDI/V7.1
```

Windows

```
C:\Program Files\IBM\TDI\V7.1
```

Migration d'une instance avec une base de données DB2 ESE vers une instance avec une base de données DB2 WSE

Pour mettre à niveau une instance 6.1 ou 6.2 avec DB2 ESE vers une instance 6.3.1 avec DB2 WSE, migrez les données de la base de données DB2 ESE vers la base de données DB2 WSE.

Avant de commencer

Vous devez effectuer les tâches suivantes avant de migrer les données d'une instance d'une version précédente vers une instance à la version 6.3.1 :

- Installez IBM Security Directory Server version 6.3.1 avec IBM DB2 WSE. Voir «Démarrage de l'installation», à la page 28.
- Avant de mettre à niveau une instance, configurez l'environnement. Voir «Configuration de l'environnement avant la mise à niveau d'une instance», à la page 92.
- Connectez-vous en tant qu'utilisateur root sur les systèmes d'exploitation AIX, Linux ou Solaris, et en tant que membre du groupe des administrateurs sur le système d'exploitation Windows.

Procédure

1. Arrêtez l'instance de serveur d'annuaire dont vous souhaitez migrer les données d'annuaire.
2. Lancez la commande **migbkup** fournie avec IBM Security Directory Server version 6.3.1 pour sauvegarder l'instance. Voir «Configuration de l'environnement avant la mise à niveau d'une instance», à la page 92. Pour plus d'informations sur la commande **migbkup**, consultez le manuel *Command Reference*.
3. Sauvegardez la base de données de l'instance de serveur d'annuaire dont vous souhaitez migrer les données. Pour sauvegarder la base de données d'une instance, par exemple `dsrdbm01`, effectuez les opérations ci-après.
   a. Entrez dans le contexte utilisateur du propriétaire de l'instance DB2.
      ```
      su - dsrdbm01
      ```
   b. Lancez `db2profile` pour l'utilisateur.
      ```
      sqllib/db2profile
      ```
   c. Sauvegardez la base de données DB2 de l'instance.
      ```
      db2 backup database dsrdbm01 to rép_sauvegarde_bd
      ```
      Le propriétaire de la base de données doit disposer des droits en lecture, écriture et exécution sur le répertoire de sauvegarde de la base de données, `rép_sauvegarde_bd`.
   d. Sauvegardez la base de données du journal des modifications si elle est configurée pour l'instance de serveur d'annuaire.
      ```
      db2 backup db ldapclog to rép_sauvegarde_journal_modifications
      ```
      Le propriétaire de la base de données doit disposer des droits en lecture, écriture et exécution sur le répertoire de sauvegarde du journal des modifications, `rép_sauvegarde_journal_modifications`.
   e. Exécutez la commande `exit` pour quitter le contexte utilisateur.

4. Supprimez l'instance du serveur d'annuaire avec la base de données. Pour plus d'informations sur la suppression d'une instance avec sa base de données, voir «Suppression d'une instance à l'aide de l'utilitaire de ligne de commande», à la page 170.
5. Le répertoire de travail en cours doit être le sous-répertoire `sbin` du répertoire d'installation d'IBM Security Directory Server version 6.3.1 .
6. Pour utiliser le répertoire de sauvegarde de l'instance pour la mise à niveau à distance d'une instance, lancez la commande **idsimigr** avec la syntaxe ci-après.

   ```
   idsimigr -I dsrdbm01 -u rép_sauvegarde_instance -l rép_base_instance -n
   ```
7. Pour configurer l'instance, lancez la commande **idscfgdb** avec la syntaxe ci-après.

   ```
   idscfgdb -I dsrdbm01 -a propriétaire_bd -w mdp
    -t dsrdbm01 -l rép_base_instance -n
   ```
8. Si la base de données du journal des modifications était configurée pour l'instance, configurez-la à nouveau pour l'instance :

   ```
   idscfgchglg -I dsrdbm01 -n
   ```
9. Restaurez la base de données à partir d'une image de sauvegarde. Pour restaurer la base de données d'une instance, par exemple `dsrdbm01`, effectuez les opérations ci-après.
   a. Entrez dans le contexte utilisateur du propriétaire de l'instance DB2.

      ```
      su - dsrdbm01
      ```
   b. Restaurez la base de données DB2 de l'instance.

      ```
      db2 restore database dsrdbm01 from rép_sauvegarde_bd replace existing
      ```
   c. Restaurez la base de données du journal des modifications si elle est configurée pour l'instance de serveur d'annuaire.

      ```
      db2 restore db ldapclog from  rép_sauvegarde_journal_modifications
      ```
   d. Exécutez la commande `exit` pour quitter le contexte utilisateur.
10. Pour cataloguer la base de données restaurée, exécutez les commandes suivantes :

    ```
    su - dsrdbm01
    db2 uncatalog database dsrdbm01
    db2 catalog database dsrdbm01 as dsrdbm01 authentication server
    exit
    ```
11. Pour cataloguer la base de données du journal des modifications restaurée, exécutez les commandes suivantes :

    ```
    su - dsrdbm01
    db2 uncatalog database ldapclog
    db2 catalog database ldapclog as ldapclog authentication server
    exit
    ```
12. Démarrez le serveur d'annuaire et le serveur d'administration.

    ```
    ibmslapd -I dsrdbm01 -n -t
    ibmdiradm -I dsrdbm01
    ```

Migration de la solution de gestion des journaux

Vous pouvez migrer la solution de gestion des journaux qui est configurée avec une instance d'une version précédente vers une instance à la version 6.3.1.

Avant de commencer

Vous devez effectuer les tâches suivantes avant de migrer la solution de gestion des journaux d'une instance d'une version précédente vers une instance à la version 6.3.1 :

- Installez IBM Security Directory Server version 6.3.1. Voir «Démarrage de l'installation», à la page 28.
- Installez IBM Security Directory Integrator version 7.1 sur l'ordinateur s'il n'y est pas.
- Connectez-vous en tant qu'utilisateur root sur les systèmes d'exploitation AIX, Linux ou Solaris, et en tant que membre du groupe des administrateurs sur le système d'exploitation Windows.

Procédure

1. Sauvegardez le fichier `solution.properties` qui se trouve dans le répertoire *rép_instance_DS*`/idsslapd-`*nom_instance*`/etc/logmgmt` de votre instance de serveur d'annuaire existante.
2. Mettez à niveau la version précédente de l'instance vers la version 6.3.1. Voir Chapitre 14, «Mise à niveau d'une instance d'une version précédente», à la page 91.
3. Supprimez tous les fichiers et les sous-répertoires contenus dans le répertoire *rép_instance_DS*`/idsslapd-`*nom_instance*`/etc/logmgmt` de l'instance mise à niveau.
4. Si votre version d'IBM Security Directory Integrator est antérieure à la version 7.1, installez IBM Security Directory Integrator version 7.1.
5. Entrez dans le contexte utilisateur du propriétaire de l'instance du serveur d'annuaire.

   ```
   su - propriétaire_instance
   ```

6. Copiez les fichiers suivants :
   a. Copiez les fichiers et les répertoires de*rép_installation_Directory_Integrator_v7.1*`/etc` dans *rép_instance_DS*`/idsslapd-`*nom_instance*`/etc/logmgmt`.
   b. Copiez les fichiers et les répertoires de*rép_installation_Directory_Integrator_v7.1*`/serverapi` dans *rép_instance_DS*`/idsslapd-`*nom_instance*`/etc/logmgmt`.
   c. Copiez *rép_installation_Directory_Integrator_v7.1*`/idisrv.sth` dans *rép_instance_DS*`/idsslapd-`*nom_instance*`/etc/logmgmt`.
   d. Copiez *rép_installation_Directory_Integrator_v7.1*`/testserver.jks` dans *rép_instance_DS*`/idsslapd-`*nom_instance*`/etc/logmgmt`.
7. Créez un répertoire portant le nom `logs` dans *rép_instance_DS*`/idsslapd-`*nom_instance*`/etc/logmgmt`.
8. Ajoutez l'entrée `systemqueue.on=false` à la fin du fichier *rép_instance_DS*`/idsslapd-`*nom_instance*`/etc/logmgmt/solutions.properties`.
9. Si le chemin d'installation d'IBM Security Directory Integrator version 7.1 est différent du chemin par défaut, définissez-le dans la variable *IDS_LDAP_TDI_HOME*.
10. Exécutez la solution de gestion de journaux.

Migration de la solution SNMP

Vous pouvez migrer la solution SNMP (Simple Network Management Protocol) qui est configurée avec une instance d'une version précédente vers une instance à la version 6.3.1.

Avant de commencer

Vous devez effectuer les tâches suivantes avant de migrer la solution SNMP d'une instance d'une version précédente vers une instance à la version 6.3.1 :

- Installez IBM Security Directory Server version 6.3.1. Voir «Démarrage de l'installation», à la page 28.
- Installez IBM Security Directory Integrator version 7.1 sur l'ordinateur s'il n'y est pas.
- Connectez-vous en tant qu'utilisateur root sur les systèmes d'exploitation AIX, Linux ou Solaris, et en tant que membre du groupe des administrateurs sur le système d'exploitation Windows.

Procédure

1. Sauvegardez le répertoire `snmp` qui se trouve dans le répertoire d'installation d'IBM Security Directory Server installation associé à l'instance existante de la version précédente.
2. Mettez à niveau la version précédente de l'instance vers la version 6.3.1. Voir Chapitre 14, «Mise à niveau d'une instance d'une version précédente», à la page 91.
3. Remplacez le fichier `/idstools/snmp/idssnmp.conf` qui se trouve dans le chemin d'installation d'IBM Security Directory Server version 6.3.1 par le fichier `/idstools/snmp/idssnmp.conf` qui se trouve dans le chemin d'installation de la version précédente d'IBM Security Directory Server.
4. Remplacez le fichier `/idstools/snmp/idssnmp.properties` qui se trouve dans le chemin d'installation d'IBM Security Directory Server version 6.3.1 par le fichier `/idstools/snmp/idssnmp.properties` qui se trouve dans le chemin d'installation de la version précédente d'IBM Security Directory Server.
5. Remplacez le fichier `/idstools/snmp/IBM-DIRECTORYSERVER-MIB` qui se trouve dans le chemin d'installation d'IBM Security Directory Server version 6.3.1 par le fichier `/idstools/snmp/IBM-DIRECTORYSERVER-MIB` qui se trouve dans le chemin d'installation de la version précédente d'IBM Security Directory Server.
6. Remplacez le fichier `/idstools/snmp/INET-ADDRESS-MIB` qui se trouve dans le chemin d'installation d'IBM Security Directory Server version 6.3.1 par le fichier `/idstools/snmp/INET-ADDRESS-MIB` qui se trouve dans le chemin d'installation de la version précédente d'IBM Security Directory Server.
7. Si le chemin d'installation d'IBM Security Directory Integrator version 7.1 est différent du chemin par défaut, définissez-le dans la variable *IDS_LDAP_TDI_HOME*.
8. Exécutez la solution SNMP.

Migration de la solution de synchronisation Active Directory

Vous pouvez migrer la solution de gestion Active Directory qui est configurée avec une instance d'une version précédente vers une instance de la version 6.3.1.

Avant de commencer

Vous devez effectuer les tâches suivantes avant de migrer la solution de synchronisation Active Directory d'une instance d'une version précédente vers une instance de la version 6.3.1 :

- Installez IBM Security Directory Server version 6.3.1. Voir «Démarrage de l'installation», à la page 28.
- Installez IBM Security Directory Integrator version 7.1 sur l'ordinateur s'il n'y est pas.
- Connectez-vous en tant qu'utilisateur root sur les systèmes d'exploitation AIX, Linux ou Solaris, et en tant que membre du groupe des administrateurs sur le système d'exploitation Windows.

Dans IBM Security Directory Server version 6.3.1, la solution de synchronisation d'Active Directory est obsolète. Utilisez la solution LDAPSync à la place.

Procédure

1. Mettez à niveau la version précédente de l'instance vers la version 6.3.1. Voir Chapitre 14, «Mise à niveau d'une instance d'une version précédente», à la page 91.
2. Créez une instance de serveur d'annuaire. Voir «Création d'une instance à l'aide de l'outil d'administration d'instance», à la page 138.
3. Configurez l'instance de serveur d'annuaire pour la synchronisation avec Active Directory. Voir «Synchronisation Active Directory», à la page 221.
4. Restaurez les modifications apportés au fichier *rép_principal_instance_DS*`/idsslapd-`*nom_instance*`/etc/tdisoldir/solution.properties` avant la mise à niveau de l'instance.

   Remarque : Si vous remplacez le nouveau fichier `solution.properties` par le fichier précédent, la synchronisation avec Active Directory risque d'échouer. Le format du fichier `solution.properties` qui est créé lorsque vous exécutez la commande **idsadscfg** est en effet différent de celui de l'ancien fichier.
5. Exécutez la solution de synchronisation avec Active Directory. Pour plus d'informations sur la commande **idsadsrun**, consultez le manuel *Guide des commandes*.

Migration d'une version précédente de la configuration de l'outil d'administration Web

La migration d'une version précédente de l'outil d'administration Web vous permet de continuer à utiliser les mêmes paramètres avec une version plus récente de l'outil.

Pour migrer la configuration existante d'une version précédente de l'outil d'administration Web à l'aide de la commande **idswmigr**, vous devez vérifier que les conditions ci-après sont réunies.

1. La version précédente de l'outil d'administration Web est installée sur l'ordinateur.
2. La version précédente d'Embedded WebSphere Application Server est installée sur l'ordinateur.
3. La version précédente de l'outil d'administration Web est déployée sur la version précédente d'Embedded WebSphere Application Server.

4. Installez l'outil d'administration Web qui est fourni avec IBM Security Directory Server version 6.3.1.
5. Installez la version d'Embedded WebSphere Application Server qui est fournie avec IBM Security Directory Server version 6.3.1.
6. Ne déployez pas l'outil d'administration Web qui est fourni avec la version 6.3.1 dans Embedded WebSphere Application Server.

L'outil d'administration Web des versions suivantes d'IBM Security Directory Server, déployé sur les version suivantes d'Embedded WebSphere Application Server, est pris en charge pour la migration :

- IBM Security Directory Server version 6.1 et Embedded WebSphere Application Server version 6.1.0.7 ou versions suivantes
- IBM Security Directory Server version 6.2 et Embedded WebSphere Application Server version 6.1.0.13 ou versions suivantes (sous UNIX) ou Embedded WebSphere Application Server version 6.1.0.17 (sous Windows) ou versions suivantes
- IBM Security Directory Server version 6.3 et Embedded WebSphere Application Server version 7.0.0.7 ou versions suivantes

Lorsque vous utilisez la commande **idswmigr** pour migrer les paramètres de configuration d'une version précédente de l'outil d'administration Web, la commande réalise les opérations ci-après.

1. Elle enregistre les fichiers de configuration de la version précédente de l'outil d'administration Web.
2. Elle annule le déploiement de la version précédente de l'outil d'administration Web dans la version précédente d'Embedded WebSphere Application Server.
3. Elle sauvegarde la configuration de la version précédente d'Embedded WebSphere Application Server dans un emplacement temporaire défini.
4. Elle restaure la configuration de la version précédente d'Embedded WebSphere Application Server.
5. Elle déploie l'outil d'administration Web dans la version en cours d'Embedded WebSphere Application Server qui est fournie avec IBM Security Directory Server version 6.3.1.
6. Elle migre les fichiers de la configuration précédente de l'outil d'administration Web et les restaure dans la version récente d'Embedded WebSphere Application Server.

Remarque : La migration de l'outil d'administration Web n'est possible avec IBM Installation Manager que si la version majeure de l'instance d'Embedded WebSphere Application Server à migrer est inférieure à celle de l'instance d'Embedded WebSphere Application Server qui vient d'être installée.

idswmigr

Utilisez la commande **idswmigr** pour migrer la configuration existante d'une version précédente de l'outil d'administration Web vers une version plus récente de l'outil.

Description

Pour migrer la configuration existante d'une version précédente de l'outil d'administration Web à l'aide de la commande **idswmigr**, vous devez vérifier que les conditions ci-après sont réunies.

1. La version précédente de l'outil d'administration Web est installée sur l'ordinateur.
2. La version précédente d'Embedded WebSphere Application Server est installée sur l'ordinateur.
3. La version précédente de l'outil d'administration Web est déployées sur la version précédente d'Embedded WebSphere Application Server.
4. Installez la version récente de l'outil d'administration Web.
5. Installez la version récente d'Embedded WebSphere Application Server.
6. Ne déployez pas un outil d'administration Web d'une version supérieure à celle d'Embedded WebSphere Application Server.

Syntaxe

```
idswmigr -l chemin_temp [-s chemin_source -t chemin_cible
          -r nom_profil -a nom_appli -v -o chemin_ports ]
```

Options

La commande **idswmigr** accepte les paramètres suivants :

-a *app_name*
Indique le nom de l'application. En l'absence de ce paramètre, la valeur par défaut est `IDSWebApp.war`.

-l *temp_path*
Indique l'emplacement des fichiers temporaires.

-o *ports_path*
Indique le chemin d'accès complet du fichier de définition de ports. En l'absence de ce paramètre, le chemin par défaut suivant est utilisé :

Windows
`C:\Program Files\IBM\ldap\V6.3.1\idstools\TDSWEBPortDef.props`

AIX et Solaris
`/opt/IBM/ldap/V6.3.1/idstools/TDSWEBPortDef.props`

Linux `/opt/ibm/ldap/V6.3.1/idstools/TDSWEBPortDef.props`

-r *profile_name*
Indique le nom du profil associé à l'application. Si celui-ci n'est pas indiqué, la valeur par défaut est `TDSWebAdminProfile`.

-s *source_path*
Indique l'emplacement source de la version précédente d'Embedded WebSphere Application Server.

-t *target_path*
Indique l'emplacement d'installation de la version plus récente d'Embedded WebSphere Application Server.

-v
Affiche la version.

Exemples

Exemple 1
Pour migrer une configuration existante de l'outil d'administration Web de la version 6.2 vers la version 6.3.1, entrez la commande ci-après.

```
idswmigr -l /tmp/web_migr -s /opt/ibm/ldap/V6.2/appsrv \
-t /opt/ibm/ldap/V6.3.1/appsrv -r TDSWebAdminProfile \
-a IDSWebApp.war
```

Migration manuelle de l'Outil d'administration Web

Vous pouvez migrer manuellement l'Outil d'administration Web.

Avant de commencer

Pour migrer manuellement l'Outil d'administration Web, vous devez installer d'abord l'Outil d'administration Web. Effectuez la procédure de migration manuelle de l'Outil d'administration Web. Dans l'exemple indiqué, l'Outil d'administration Web de IBM Security Directory Server V6.3 est migré vers IBM Security Directory Server V6.3.1.

Sous AIX, les commandes de migration sont semblables aux commandes de Linux, sauf que le chemin `/opt/ibm/ldap` doit être remplacé par `/opt/IBM/ldap`.

Procédure

1. Pour Windows, ajoutez le service WebSphere Application Server avec la commande ci-après.

   ```
   "C:\Program Files\IBM\ldap\V6.3.1\appsrv\bin\WASService.exe" -add
   TDSWebAdmin-V6.3.1 -serverName server1 -profilePath
   "C:\Program Files\IBM\ldap\V6.3.1\appsrv\profiles\TDSWebAdminProfile"
   -startType automatic
   ```

2. Sauvegardez les fichiers de l'Outil d'administration Web de l'édition précédente.
   - Sous Windows, recherchez ces fichiers dans le répertoire suivant :

     ```
     C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\
      installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\
      WEB-INF\classes\
     ```

     ou

     ```
     C:\Program Files\IBM\LDAP\V6.3\appsrv\installedApps\DefaultNode
     \IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\classes
     ```

   - Sous Linux, recherchez ces fichiers dans le répertoire suivant :

     ```
     /opt/ibm/ldap/V6.3/appsrv/profiles/TDSWebAdminProfile/installedApps
     /DefaultNode/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes
     ```

     ou

     ```
     /opt/ibm/ldap/V6.3/appsrv/installedApps/DefaultNode
     /IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes
     ```

   Copiez uniquement les cinq fichiers suivants à partir des répertoires :

   ```
   security\console_passwd
   IDSConfig\IDSSessionConfig\IDSSessionMgmt.xml
   IDSConfig\IDSServersConfig\IDSServersInfo.xml
   IDSConfig\IDSAppReg\IDSAppReg.xml
   IDSConfig\IDSSearchSettings\IDSSearchMgmt.xml
   ```

   Par exemple :

   ```
     copy "C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\
   installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\classes\
   security\console_passwd" c:\BackUp
     copy "C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\
   installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\classes\
   ```

```
IDSConfig\IDSSessionConfig\IDSSessionMgmt.xml" c:\BackUp
  copy "C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\
installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\classes\
IDSConfig\IDSServersConfig\IDSServersInfo.xml" c:\BackUp
  copy "C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\
installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\classes\
IDSConfig\IDSAppReg\IDSAppReg.xml" c:\BackUp
  copy "C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\
installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\classes\
IDSConfig\IDSSearchSettings\IDSSearchMgmt.xml" c:\BackUp
```

3. Désinstallez le fichier WAR de l'édition précédente.
   - Sous Windows, la commande se trouve dans le répertoire suivant :

     ```
     C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\bin\wsadmin.bat
     ```

     ou

     ```
     C:\Program Files\IBM\LDAP\V6.3\appsrv\bin\wsadmin.bat
     ```

   - Sous Linux, la commande se trouve dans le répertoire suivant :

     ```
     /opt/ibm/ldap/V6.3/appsrv/profiles/TDSWebAdminProfile/bin/wsadmin.sh
     ```

     ou

     ```
     /opt/ibm/ldap/V6.3/appsrv/bin/wsadmin.sh
     ```

   ```
   wsadmin.bat -conntype NONE -c "$AdminApp uninstall IDSWebApp.war"
   ```

   Par exemple :

   ```
   "C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\bin\wsadmin.bat"
    -conntype NONE -c "$AdminApp uninstall IDSWebApp.war"
   ```

4. Si le serveur de la version intégrée précédente de WebSphere Application Server est en cours d'exécution, arrêtez le serveur d'application.
   - Sous Windows, la commande se trouve dans le répertoire suivant :

     ```
     C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\bin\
     stopServer.bat
     ```

     ou

     ```
     C:\Program Files\IBM\LDAP\V6.3\appsrv\bin\stopServer.bat
     ```

   - Sous Linux, la commande se trouve dans le répertoire suivant :

     ```
     /opt/ibm/ldap/V6.3/appsrv/profiles/TDSWebAdminProfile/bin/stopServer.sh
     ```

     ou

     ```
     /opt/ibm/ldap/V6.3/appsrv/bin/stopServer.sh
     ```

   Par exemple :

   ```
   "C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\bin\
   stopServer.bat" server1
   ```

5. Recherchez l'existence du profil dans la nouvelle version intégrée de WebSphere Application Server. Si le profil n'existe pas, créez-le.
   - Sous Windows, exécutez la commande ci-après pour créer un profil.

     ```
     "C:\Program Files\IBM\LDAP\V6.3.1\appsrv\bin\manageprofiles.bat" -create
      -profileName TDSWebAdminProfile -profilePath "C:\Program Files\IBM\
      LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile" -templatePath
      "C:\Program Files\IBM\LDAP\V6.3.1\appsrv\ profileTemplates\default"
      -nodeName DefaultNode -hostName localhost -cellName
      DefaultNode -isDefault -portsFile "C:\Program Files\IBM\LDAP\V6.3.1\idstools
      \TDSWEBPortDef.props"
     ```

   - Sous Linux, exécutez la commande ci-après pour créer un profil.

```
/opt/ibm/ldap/V6.3.1/appsrv/bin/manageprofiles.sh -create -profileName
 TDSWebAdminProfile -profilePath "/opt/ibm/ldap/V6.3.1/appsrv/profiles/
 TDSWebAdminProfile" -templatePath "/opt/ibm/ldap/V6.3.1/appsrv/
 profileTemplates/default" -nodeName DefaultNode -hostName localhost
 -cellName DefaultNode -isDefault -portsFile "/opt/ibm/ldap/V6.3.1/idstools
 /TDSWEBPortDef.props"
```

6. Copiez le nouveau fichier WAR dans le nouveau répertoire WebSphere Application Server.
   - Sous Windows, exécutez la commande ci-après.

     ```
     copy "C:\Program Files\IBM\LDAP\V6.3.1\idstools\IDSWebApp.war"
      "C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\
      installableApps"
     ```

   - Sous Linux, exécutez la commande ci-après.

     ```
     cp "/opt/ibm/ldap/V6.3.1/idstools/IDSWebApp.war"
      "/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/installableApps"
     ```

7. Installez le nouveau fichier WAR dans le nouveau WebSphere Application Server.
   - Sous Windows, exécutez la commande ci-après.

     ```
     "C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\bin
      \wsadmin.bat" -conntype NONE -c "$AdminApp install {C:\Program Files\
      IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\installableApps\
      IDSWebApp.war} {-configroot \"C:\Program Files\IBM\LDAP\V6.3.1\
      appsrv\config\" -node DefaultNode -usedefaultbindings -nodeployejb
      -appname IDSWebApp.war -contextroot \"IDSWebApp\"}"
     ```

   - Sous Linux, exécutez la commande ci-après.

     ```
     "/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/bin/wsadmin.sh"
      -conntype NONE -c "\$AdminApp install {/opt/ibm/ldap/V6.3.1/appsrv/
      profiles/TDSWebAdminProfile/installableApps/IDSWebApp.war}
      {-configroot \"/opt/ibm/ldap/V6.3.1/appsrv/config\"
      -node DefaultNode -usedefaultbindings -nodeployejb -appname IDSWebApp.war
      -contextroot \"IDSWebApp\"}"
     ```

8. Restaurez les fichiers de configuration de l'Outil d'administration Web que vous aviez sauvegardés.
   - Sous Windows, remplacez les fichiers suivants par les fichiers de copie de sauvegarde suivants :

     ```
     C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\
      installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\
      classes\security\console_passwd
      C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\
      installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\
      classes\IDSConfig\IDSSessionConfig\IDSSessionMgmt.xml
      C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\
      installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\
      classes\IDSConfig\IDSServersConfig\IDSServersInfo.xml
      C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\
      installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\
      classes\IDSConfig\IDSAppReg\IDSAppReg.xml
      C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\
      installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\
      classes\IDSConfig\IDSSearchSettings\IDSSearchMgmt.xml
     ```

   - Sous Linux, remplacez les fichiers suivants par les fichiers de copie de sauvegarde suivants :

     ```
     /opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/installedApps/
      DefaultNode/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes/security/
      console_passwd
      /opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/installedApps/
      DefaultNode/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes/IDSConfig/
      IDSSessionConfig/IDSSessionMgmt.xml
      /opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/installedApps/
     ```

```
DefaultNode/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes/IDSConfig/
IDSServersConfig/IDSServersInfo.xml
/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/installedApps/
DefaultNode/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes/IDSConfig/
IDSAppReg/IDSAppReg.xml
/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/installedApps/
DefaultNode/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes/IDSConfig/
IDSSearchSettings/IDSSearchMgmt.xml
```

9. Sous Windows, démarrez le service qui a été ajouté.

```
"C:\Program Files\IBM\ldap\V6.3.1\appsrv\bin\WASService.exe"
 -start TDSWebAdmin-V6.3.1
```

10. Sous Linux, démarrez le serveur.

```
/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/bin/startServer.sh server1
```

Chapitre 16. Déploiement manuel de l'outil d'administration Web

Pour gérer et administrer les instances de serveur d'annuaire avec l'outil d'administration Web, vous devez déployer l'outil sur un serveur d'applications Web compatible.

L'outil d'administration Web peut être déployé si l'ordinateur contient une version compatible du serveur d'application Web. Le support d'installation d'IBM Security Directory Server contient Embedded WebSphere Application Server version 7.0.0.25. Vous pouvez utiliser IBM Installation Manager pour installer l'outil d'administration Web, et le déployer sur Embedded WebSphere Application Server.

Si votre système d'exploitation ne prend pas en charge l'installation d'IBM Security Directory Server à l'aide d'IBM Installation Manager, installez Embedded WebSphere Application Server manuellement. Après avoir installé Embedded WebSphere Application Server, vous devez déployer l'outil d'administration Web dans Embedded WebSphere Application Server.

Si votre ordinateur contient une version compatible de WebSphere Application Server, vous pouvez y déployer l'outil d'administration Web.

WebSphere Application Server est l'environnement d'exécution d'IBM pour les applications Java. Pour plus d'informations, voir la documentation du produit WebSphere Application Server à l'adresse http://www-01.ibm.com/support/knowledgecenter/SSEQTP/welcome.

Installation manuelle d'Embedded WebSphere Application Server

Avant de déployer l'outil d'administration Web, vous devez installer Embedded WebSphere Application Server sur l'ordinateur.

Avant de commencer

Pour l'installation d'Embedded WebSphere Application Server, procédez de la manière suivante :

1. Accédez au support d'installation d'IBM Security Directory Server qui contient l'installable d'Embedded WebSphere Application Server. Voir «Préparation du support d'installation», à la page 6.

Pourquoi et quand exécuter cette tâche

Pour déployer l'outil d'administration Web à l'aide de la commande `deploy_IDSWebApp` sans utiliser de paramètres, vous devez définir les valeurs ci-après.

1. Entrez le répertoire `appsrv` du chemin d'installation d'IBM Security Directory Server comme emplacement d'installation d'Embedded WebSphere Application Server. Pour plus d'informations sur le chemin d'installation par défaut d'IBM Security Directory Server, voir «Emplacements d'installation par défaut», à la page 27.

Vous pouvez choisir un autre emplacement pour l'installation d'Embedded WebSphere Application Server. Dans ce cas, vous devez utiliser les paramètres **-w**, **-p**, **-r** et **-o** et leurs valeurs avec la commande`deploy_IDSWebApp` pour le déploiement de l'outil d'administration Web.

Procédure

1. Connectez-vous avec les privilèges d'administrateur.
2. Accédez à l'invite de commande.
3. Le répertoire de travail en cours doit être celui qui contient l'installable d'Embedded WebSphere Application Server.
4. Pour installer Embedded WebSphere Application Server dans le chemin d'installation par défaut d'IBM Security Directory Server, exécutez la commande ci-après.

Systèmes d'exploitation	Commande à exécuter :
Microsoft Windows	`install.bat -installRoot c:\Program Files\IBM\ldap\V6.3.1\appsrv`
AIX et Solaris	`install.sh -installRoot /opt/IBM/ldap/V6.3.1\appsrv`
Linux	`install.sh -installRoot /opt/ibm/ldap/V6.3.1\appsrv`

Que faire ensuite

Si l'outil d'administration Web n'est pas installé sur l'ordinateur, installez-le. Voir Chapitre 12, «Installation avec les utilitaires de ligne de commande du système d'exploitation», à la page 69.

Si l'outil d'administration Web est installé sur l'ordinateur, déployez-le. Voir «Déploiement de l'outil d'administration Web dans la version intégrée de WebSphere Application Server», à la page 115.

Ports par défaut de l'outil d'administration Web

Pour éviter les conflits de ports entre l'outil d'administration Web et d'autres applications, vous devez connaître les ports utilisés par défaut par l'outil d'administration Web.

Embedded WebSphere Application Server utilise le paramétrage par défaut des ports pour l'outil d'administration Web :

- Transport HTTP (port 1) : 12100
- Transport HTTPS (port 2) : 12101
- Port de la console d'administration (permettant d'administrer WebSphere Application Server) : 12104
- Port sécurisé de la console d'administration (permettant d'administrer WebSphere Application Server) : 12105

Embedded WebSphere Application Server utilise le paramétrage suivant pour les ports des autres applications :

- Port RMI/d'amorçage : 12102
- Port de connexion SOAP : 12103

Autres numéros de port susceptibles d'être utilisés par Embedded WebSphere Application Server : 9405, 9406, 9407, 9375, 9105, 7276, 7286, 5558, 5577, 5075, 5076.

En cas de conflit de port avec une autre application qui utiliserait l'un des ports par défaut, appliquez l'une des solutions suivantes en fonction de votre environnement :

- Remplacez le port par défaut par un port inutilisé, et démarrez l'application sur ce port.
- Si l'application qui utilise le port par défaut n'est un un service ou un serveur important, modifiez son numéro de port et libérez le port par défaut.

Vous pouvez redéfinir le numéro de port par défaut initialisé par Embedded WebSphere Application Server pour une application dans le fichier `portdef.props`. Le fichier `portdef.props` se trouve dans le répertoire `\appsrv\profiles\TDSWebAdminProfile\properties\` de l'emplacement d'installation d'IBM Security Directory Server. Pour plus d'informations sur l'emplacement par défaut d'IBM Security Directory Server, voir «Emplacements d'installation par défaut», à la page 27.

Port 1 de transport HTTP
Pour modifier le numéro du port 1 de transport HTTP, remplacez, dans l'entrée contenant le numéro 12100, ce numéro par celui d'un port inutilisé.

Port 2 de transport HTTPS
Pour modifier le numéro du port 2 de transport HTTPS, remplacez, dans l'entrée contenant le numéro 12101, ce numéro par celui d'un port inutilisé.

Port RMI/d'amorçage
Pour modifier le numéro du port RMI/d'amorçage, remplacez, dans l'entrée contenant le numéro 12102, ce numéro par celui d'un port inutilisé.

Port de connexion SOAP
Pour modifier le numéro du port de connexion SOAP, remplacez, dans l'entrée contenant le numéro 12103, ce numéro par celui d'un port inutilisé.

Port de la console d'administration
Pour modifier le numéro du port de la console d'administration, remplacez, dans l'entrée contenant le numéro 12104, ce numéro par celui d'un port inutilisé.

Port sécurisé de la console d'administration
Pour modifier le numéro du port sécurisé de la console d'administration, remplacez, dans l'entrée contenant le numéro 12105, ce numéro par celui d'un port inutilisé.

Déploiement de l'outil d'administration Web dans la version intégrée de WebSphere Application Server

Pour utiliser l'outil d'administration Web, vous devez le déployer sur un serveur d'applications Web.

Avant de commencer

Vous devez effectuer les opérations suivantes avant de déployer l'outil d'administration Web :

1. Installez le package de l'outil d'administration Web pour votre système d'exploitation.

2. Exécutez l'installation d'une version prise en charge du serveur d'applications Web.
3. Si vous prévoyez de faire migrer une configuration existante de l'outil d'administration Web provenant d'une version précédente, vous ne devez pas déployer de version ultérieure de l'outil d'administration Web.

Pourquoi et quand exécuter cette tâche

Lorsque vous déployez l'outil d'administration Web, la commande exécute les opérations ci-après.

1. Elle supprime la version précédente de l'outil d'administration Web, le cas échéant.
2. Elle déploie l'outil d'administration Web dans un serveur d'applications Web.
3. Elle démarre le serveur d'applications Web.

Procédure

1. Connectez-vous avec les privilèges d'administrateur.
2. Accédez au répertoire *rép_installation_DS*/idstools. *rép_installation_DS* est l'emplacement d'installation d'IBM Security Directory Server0 Les emplacements suivants sont les emplacements par défaut pour différents systèmes d'exploitation :

Systèmes d'exploitation	Emplacement d'installation par défaut
Microsoft Windows	c:\Program Files\IBM\ldap\V6.3.1
AIX et Solaris	/opt/IBM/ldap/V6.3.1
Linux	/opt/ibm/ldap/V6.3.1

3. Exécutez la commande ci-après.

   Remarque : Si vous avez installé la version intégrée de WebSphere Application Server dans le chemin d'installation par défaut d'IBM Security Directory Server, n'indiquez pas de paramètres pour la commande deploy_IDSWebApp. Pour plus d'informations sur la commande deploy_IDSWebApp, consultez la syntaxe de la commande deploy_IDSWebApp -h.

Systèmes d'exploitation	Commande à exécuter :
Microsoft Windows	deploy_IDSWebApp.bat -w *path_to_war_file* -p *was_installation_path* -r *profile* -o ports_file
AIX, Linux et Solaris	deploy_IDSWebApp -w *path_to_war_file* -p *was_installation_path* -r *profile* -o ports_file

Résultats

La commande déploie l'Outil d'administration Web sur le serveur d'applications Web spécifié dans *was_installation_path*.

Que faire ensuite

Pour accéder à l'Outil d'administration Web, ouvrez un navigateur et entrez http://*host_name*:12100/IDSWebApp. La variable *host_name* indique le nom d'hôte

ou l'adresse IP de l'ordinateur sur lequel vous avez installé l'Outil d'administration Web.

Déploiement de l'outil d'administration Web dans WebSphere Application Server

Si vous voulez gérer les applications sur votre ordinateur dans WebSphere Application Server, vous pouvez déployer l'outil d'administration Web dans WebSphere Application Server.

Avant de commencer

Avant de déployer l'outil d'administration Web dans WebSphere Application Server, vous devez vérifier que les conditions ci-après sont remplies.

1. Installez le package de l'outil d'administration Web pour votre système d'exploitation. Voir «Installation à l'aide d'IBM Installation Manager», à la page 31.
2. L'ordinateur doit contenir une version prise en charge de WebSphere Application Server.

Pourquoi et quand exécuter cette tâche

Le support d'installation d'IBM Security Directory Server contient l'outil d'administration Web et Embedded WebSphere Application Server. Si votre ordinateur contient WebSphere Application Server, vous pouvez déployer l'outil d'administration Web dans WebSphere Application Server. Pour déployer l'outil d'administration Web, vous devez déployer le fichier `IDSWebApp.war` qui se trouve dans le répertoire `idstools` de l'emplacement d'installation d'IBM Security Directory Server.

Procédure

1. Utilisez l'URL `http://`*`nom_hôte_serveur_WAS`*`:9060/ibm/console` pour vous connecter à la console d'administration WebSphere. Remplacez la variable *nom_hôte_serveur_WAS* par le nom d'hôte ou l'adresse IP de l'ordinateur sur lequel WebSphere Application Server est installé. Si vous définissez un port personnalisé pour accéder à la console d'administration de WebSphere, remplacez le port par défaut, `9060`, par votre numéro de port.
2. Entrez l'ID et le mot de passe de l'utilisateur. L'utilisateur doit disposer du droit d'exécuter des opérations sur WebSphere Application Server.
3. Dans le panneau de navigation de gauche, cliquez sur **Application** > **Nouvelle application**.
4. Dans la page **Nouvelle application**, cliquez sur **Nouvelle application d'entreprise**.
5. Dans la page du chemin d'accès au panneau de la nouvelle application, sélectionnez l'une des options suivantes selon l'endroit à partir duquel la console d'administration WebSphere est lancée :
   - Si vous accédez la console d'administration WebSphere à partir de l'ordinateur local, sélectionnez **Système de fichiers local** et entrez le chemin du fichier `IDSWebApp.war` dans la zone **Chemin complet**. Vous pouvez également cliquer sur **Parcourir** pour entrer le chemin.
   - Si vous accédez la console d'administration WebSphere à partir de l'ordinateur distant, sélectionnez **Système de fichiers éloigné** et entrez le

chemin du fichier `IDSWebApp.war` dans la zone **Chemin complet**. Vous pouvez également cliquer sur **Parcourir** pour entrer le chemin.

6. Dans la page **Comment voulez-vous installer l'application ?**, sélectionnez l'option **Raccourci** et cliquez sur **Suivant**.
7. Dans la page **Sélection des options d'installation**, les options par défaut sont sélectionnées.
8. Cliquez sur **Suivant**.
9. Dans la page **Mappage des modules vers les serveurs**, l'utilisateur peut mapper les modules vers les serveurs de la zone **Clusters et serveurs**.
   a. Cochez la case du module requis, et cliquez sur **Appliquer**.
   b. Lorsque le mappage est établi, cliquez sur **Suivant**.
10. Dans la page **Mappage des hôtes virtuels pour les modules Web**, vous pouvez mapper l'application Web à des serveurs virtuels spécifiques. Si les hôtes virtuels sont plus nombreux, le serveur doit connaître l'environnement WebSphere pour sélectionner le module approprié. Dans cet exemple, l'option `default_host` peut être sélectionnée.
11. Cliquez sur **Suivant**.
12. Dans la page **Mappage des racines de contexte des modules Web**, entrez la racine de contexte `/IDSWebApp` dans la zone.
13. Un récapitulatif de votre sélection s'affiche.
14. Cliquez sur **Terminer**. L'installation de votre application est lancée. Un récapitulatif de l'installation d'affiche.
15. Pour sauvegarder les modifications apportées à la configuration principale, cliquez sur **Enregistrer**.
16. Dans le panneau de navigation de gauche, cliquez sur **Applications** > **Types d'application** > **Applications d'entreprise WebSphere**.
17. Dans la page **Applications d'entreprise**, cochez la case située en regard d'`IDSWebApp_war`, et cliquez sur **Démarrer**.
18. Démarrez l'outil d'administration Web.
19. Pour accéder à l'outil d'administration Web, ouvrez un navigateur et entrez l'adresse suivante :
    - Pour un accès non sécurisé (HTTP), entrez `http://nom_hôte_serveur_WAS:9080/IDSWebApp`.
    - Pour un accès sécurisé (HTTPS), entrez `https://nom_hôte_serveur_WAS:9443/IDSWebApp`

    Le port 9080 est le port HTTP par défaut de WebSphere Application Server, et le port 9443 est le port HTTPS par défaut. Si ces ports ne sont pas configurés pour votre serveur WAS, entrez les numéros de port appropriés. Si la sécurité globale ou administrative est configurée pour WebSphere Application Server, vous devez vérifier que les conditions ci-après sont remplies.
    a. Déployez l'outil d'administration Web dans WebSphere Application Server en tant que nouveau profil.
    b. Configurez SSL pour l'outil d'administration Web.
    c. S'il est impossible de déployer l'outil d'administration Web dans un profil, ajoutez le certificat du serveur d'annuaire au magasin de clés de confiance du profil. Pour l'authentification client-serveur, ajoutez le certificat du profil de WebSphere Application Server au magasin de clés de confiance du serveur d'annuaire.

Démarrage de la version intégrée de WebSphere Application Server en vue d'utiliser l'Outil d'administration Web

Démarrez le serveur d'applications Web associé à l'Outil d'administration Web afin d'ajouter, de gérer et d'administrer les instances du serveur d'annuaire.

Avant de commencer

Vous devez effectuer les tâches suivantes avant de pouvoir arrêter le serveur d'applications Web qui est associé à l'Outil d'administration Web :

1. Installez l'outil d'administration Web.
2. Déployez l'outil d'administration Web sur un serveur d'applications Web compatible.

Remarque : Si vous utilisez IBM Installation Manager pour l'installation et le déploiement de l'Outil d'administration Web dans la version intégrée de WebSphere Application Server, le serveur d'application démarre lorsque vous avez terminé le déploiement de l'Outil d'administration Web.

Procédure

1. Pour démarrer le serveur d'applications associé à l'Outil d'administration Web, exécutez la commande ci-après sur les différents systèmes d'exploitation.

   Windows
   Si le serveur d'application n'est pas démarré, exécutez la commande suivant e:

   installation_path\idstools\bin\startWebadminApp.bat

   Le chemin d'installation par défaut est `C:\Program Files\IBM\ldap\V6.3.1`.

   AIX et Solaris
   `/opt/IBM/ldap/V6.3.1/idstools/bin/startWebadminApp`

   Linux
   `/opt/ibm/ldap/V6.3.1/idstools/bin/startWebadminApp`
2. Ouvrez un navigateur Web.
3. Entrez l'URL suivante dans la barre d'adresse du navigateur Web :

   Remarque : Si vous avez installé et déployé l'Outil d'administration Web sur un système distant, indiquez le nom d'hôte ou l'adresse IP du système à la place de `localhost`.

   `http://localhost:12100/IDSWebApp`

Que faire ensuite

Pour gérer et administrer les instances de serveur d'annuaire, ajoutez des serveurs dans la console de l'Outil d'administration Web. Voir «Accès à l'outil d'administration Web».

Accès à l'outil d'administration Web

Pour gérer le instances de serveur d'annuaire à distance, ouvrez l'outil d'administration Web et configurez l'instance de serveur d'annuaire pour la gestion à distance.

Avant de commencer

Vous devez effectuer les tâches suivantes avant de pouvoir accéder à l'outil d'administration Web :

1. Installez l'outil d'administration Web.
2. Déployez l'outil d'administration Web sur un serveur d'applications Web compatible.
3. Démarrez le serveur d'applications Web associé à l'outil d'administration Web.

Procédure

1. Pour accéder à l'outil d'administration Web, choisissez l'une des méthodes suivantes :
   - Ouvrez un navigateur Web et entrez l'URL suivante :
     - Pour un accès non sécurisé, entrez `http://nom_hôte:12100/IDSWebApp`.
     - Pour un accès sécurisé, entrez `https://nom_hôte:12101/IDSWebApp`.
   - Ouvrez le fichier suivant dans un navigateur Web :

     Windows

     Pour un accès non sécurisé, ouvrez *chemin_installation_ds*`\idstools\bin\idswebadmin.html`. Vous pouvez aussi cliquer sur **Démarrer** > **Tous les programmes** > **IBM Security Directory Server 6.3.1** > **Outil d'administration Web**.

     Pour un accès sécurisé, ouvrez *chemin_installation_ds*`\idstools\bin\idswebadminssl.html`. Vous pouvez aussi cliquer sur **Démarrer** > **Tous les programmes** > **IBM Security Directory Server 6.3.1** > **Outil d'administration Web(sécurisé)**.

     AIX, Linux et Solaris

     Pour un accès non sécurisé, ouvrez *chemin_installation_ds*`/idstools/bin/idswebadmin.html`.

     Pour un accès sécurisé, ouvrez *chemin_installation_ds*`/idstools/bin/idswebadminssl.html`.

     La variable *chemin_installation_ds* représente l'emplacement d'installation d'IBM Security Directory Server. Pour plus d'informations sur l'emplacement par défaut, voir «Emplacements d'installation par défaut», à la page 27.
2. Connectez-vous à la console de l'outil d'administration Web en tant qu'administrateur.
   a. Dans la zone **ID utilisateur**, entrez `superadmin`.
   b. Dans la zone **Mot de passe**, entrez **secret**.

      Remarque : Après la première connexion, vous devez changer le mot de passe de l'administrateur de la console.
   c. Cliquez sur **Connexion**.
3. Pour ajouter un serveur d'annuaire à la console, procédez de la façon suivante :
   a. Dans la page **Introduction**, cliquez sur **Gérer les serveurs de la console**.
   b. Dans la page **Gérer les serveurs de la console**, cliquez sur **Ajouter**.
   c. Dans la zone **Nom du serveur**, entrez un nom unique pour identifier le serveur. Si vous n'entrez pas de valeur, l'application lui affecte une valeur, du type `nom_hôte:port` ou `adresse_IP:port`.
   d. Dans la zone **Nom d'hôte**, entrez le nom d'hôte ou l'adresse IP du serveur d'annuaire.

e. Dans la zone **Port**, entrez le numéro de port du serveur.
f. Si la console doit communiquer avec le serveur de façon sécurisée, sélectionnez **Activer le chiffrement SSL**.
g. Pour activer le contrôle du port d'administration, sélectionnez **Serveur d'administration pris en charge**.
h. Dans la zone **Port d'administration**, entrez le numéro de port du serveur d'administration.
i. Pour appliquer les modifications, cliquez sur **OK**.

4. Pour vous déconnecter de la console de l'outil d'administration Web, cliquez sur **Déconnexion**.

Arrêt du serveur d'applications Web

Avant de désinstaller l'outil d'administration Web, vous devez vous en déconnecter et arrêter le serveur d'applications Web qui lui est associé.

Avant de commencer

Vous devez effectuer les tâches suivantes avant de pouvoir arrêter le serveur d'applications Web qui est associé à l'outil d'administration Web :

1. Déployez l'outil d'administration Web sur un serveur d'applications Web compatible.
2. Démarrez le serveur d'applications Web associé à l'outil d'administration Web.

Procédure

1. Connectez-vous en tant que root sur les systèmes UNIX, et en tant que membre du groupe des administrateurs sous Windows.
2. Accédez à l'invite de commande.
3. Accédez au sous-répertoire `bin` du profil de l'outil d'administration Web. L'emplacement suivant est le chemin d'installation par défaut su serveur Embedded WebSphere Application Server sur lequel l'outil d'administration Web est déployé. Si vous avez défini un chemin d'installation personnalisé pour Embedded WebSphere Application Server, faites les modifications correspondantes.

Système d'exploitation	Chemin
Windows	`C:\Program Files\IBM\ldap\V6.3.1\appsrv\profiles\TDSWebAdminProfile\bin`
AIX et Solaris	`/opt/IBM/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/bin`
Linux	`/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/bin`

4. Pour arrêter le serveur d'applications Web associé à l'outil d'administration Web, exécutez la commande ci-après.

Système d'exploitation	Commande à exécuter :
Windows	`stopServer.bat server1`
AIX, Linux et Solaris	`./stopServer server1`

Remarque : Sous Windows, vous pouvez également arrêter le service associé au serveur d'applications Web dans la fenêtre **Services**.

HTTPS et Embedded WebSphere Application Server

Pour sécuriser l'accès Web à vos applications, vous pouvez configurer le mode HTTPS et démarrer les applications dans ce mode.

Après avoir déployé l'outil d'administration Web sur Embedded WebSphere Application Server, vous pouvez démarrer votre application. Pour vous connecter à l'outil d'administration Web en mode sécurisé, définissez l'adresse Web HTTPS et le port sécurisé.

Pour utiliser HTTPS, utilisez l'adresse suivante pour accéder à l'outil d'administration Web :

`https://`*`nom_hôte`*`:12101/IDSWebApp`

Pour utiliser une connexion non-HTTPS, accédez à l'outil d'administration Web avec l'adresse suivante :

`http://`*`nom_hôte`*`:12100/IDSWebApp`

Vous pouvez également modifier les fichiers JKS par défaut en y ajoutant des certificats fournis par le serveur d'applications Web et destinés aux communications sécurisées SSL/TLS. Vous pouvez créer de nouveaux fichiers de clés et de magasin de clés de confiance destinés aux applications déployées sur Embedded WebSphere Application Server. Les fichiers de clés et de magasin de clés de confiance par défaut sont des fichiers distincts stockés dans le répertoire *RACINE_WAS*/profiles/TDSWebAdminProfile/etc/. La variable *RACINE_WAS* est dans le répertoire d'installation d'Embedded WebSphere Application Server. Le fichier de la base de données de clés par défaut est DummyServerKeyFile.jks, et le fichier du magasin de clés de confiance par défaut est DummyServerTrustFile.jks.

Si vous avez créé les fichiers JKS, vous pouvez modifier les fichiers de clés et de magasin de clés de confiance. Pour configurer les fichiers JKS, les mots de passe et le format des fichiers, ajoutez ou modifiez les entrées suivantes (en **gras**) dans le fichier *RACINE_WAS*/profiles/TDSWebAdminProfile/config/cells/DefaultNode/security.xml :

```
<keyStores xmi:id="KeyStore_DefaultNode_10"
 name="DummyServerKeyFile"
 password="{xor}CDo9Hgw="
 provider="IBMJCE"
 location="${RACINE_WAS}/profiles/TDSWebAdminProfile/etc/DummyServerKeyFile.jks"
 type="JKS"
 fileBased="true"
 hostList=""
 managementScope="ManagementScope_DefaultNode_1"/>
<keyStores xmi:id="KeyStore_DefaultNode_11"
 name="DummyServerTrustFile"
 password="{xor}CDo9Hgw="
 provider="IBMJCE"
 location="${RACINE_WAS}/profiles/TDSWebAdminProfile/etc/DummyServerTrustFile.jks"
 type="JKS"
 fileBased="true"
 hostList=""
 managementScope="ManagementScope_DefaultNode_1"/>
```

Annulation du déploiement de l'outil d'administration Web dans la version intégrée de WebSphere Application Server

Pour remplacer un Outil d'administration Web (fichier `IDSWebApp.war`) par une version ultérieure, vous devez annuler le déploiement de l'Outil d'administration Web.

Procédure

1. Démarrez le serveur d'applications Web associé à l'outil d'administration Web, s'il est arrêté . Voir «Démarrage de la version intégrée de WebSphere Application Server en vue d'utiliser l'Outil d'administration Web», à la page 119.
2. Accédez au répertoire *rép_installation_DS*`/idstools`. *rép_installation_DS* est l'emplacement d'installation d'IBM Security Directory Server0 Les emplacements suivants sont les emplacements par défaut pour différents systèmes d'exploitation :

Systèmes d'exploitation	Emplacement d'installation par défaut
Microsoft Windows	`c:\Program Files\IBM\ldap\V6.3.1`
AIX et Solaris	`/opt/IBM/ldap/V6.3.1`
Linux	`/opt/ibm/ldap/V6.3.1`

3. Exécutez la commande ci-après.

   Remarque : Si vous avez installé la version intégrée de WebSphere Application Server dans un emplacement personnalisé, vous devez aussi fournir les paramètres **`-a`**, **`-w`**, **`-p`** et **`-r`** à la commande `deploy_IDSWebApp`. Pour plus d'informations sur la commande `deploy_IDSWebApp`, consultez la syntaxe de la commande `deploy_IDSWebApp -h`.

Systèmes d'exploitation	Commande à exécuter :
Microsoft Windows	`deploy_IDSWebApp.bat -u`
AIX, Linux et Solaris	`deploy_IDSWebApp -u`

Chapitre 17. Planification de la configuration d'une instance

Vous devez choisir les paramètres de configuration de votre ordinateur avent de créer et de configurer un environnement LDAP.

Avant de créer une instance de serveur d'annuaire ou de serveur proxy, vous devez créer un ID utilisateur système qui est propriétaire de l'instance. Pour stocker les données d'annuaire dans une instance de serveur d'annuaire, vous devez choisir la page de code à utiliser.

L'installation d'IBM Security Directory Server et des produits logiciels corequis, et la création d'une instance de serveur d'annuaire, nécessite la création d'un utilisateur et d'un groupe sur l'ordinateur. L'installation des logiciels corequis d'IBM Security Directory Server, par exemple IBM DB2, nécessite la création d'un ID utilisateur système pour l'administrateur DB2.

Utilisateurs et groupes associés à une instance de serveur d'annuaire

Avant de créer une instance de serveur d'annuaire ou de serveur proxy, vous devez créer un utilisateur et un groupe disposant des droits requis.

Si vous voulez créer une instance sur votre ordinateur, vous devez lui associer un ID utilisateur système. Cet ID utilisateur est le propriétaire de l'instance de serveur d'annuaire. S'il n'existe pas d'ID utilisateur pour l'instance, vous devez en créer un sur l'ordinateur. Pour créer un ID utilisateur pour le propriétaire de l'instance de serveur d'annuaire, celui de l'instance de base de données et celui de la base de données, vous devez suivre les règles d'attribution de nom. Pour plus d'informations sur les règles d'attribution de nom, voir «Règles d'attribution de nom», à la page 126.

Pour un serveur d'annuaire complet, vous devez également associer des ID utilisateur système en tant que propriétaires de l'instance de base de données et de la base de données. Vous pouvez utiliser le même ID utilisateur pour ces trois rôles. Dans ce cas, l'instance de serveur d'annuaire , l'instance de base de données et le propriétaire de base de données contiennent le même nom de propriétaire.

Si vous créez une instance de serveur d'annuaire à l'aide de l'outil d'administration d'instance, l'outil vous permet de créer l'ID utilisateur du propriétaire de l'instance de serveur d'annuaire. Vous pouvez aussi utiliser la commande **idsadduser** pour créer l'ID utilisateur du propriétaire de l'instance de serveur d'annuaire. La commande crée un ID utilisateur qui répond à tous les critères.

L'ID utilisateur que vous associez au propriétaire de l'instance de serveur d'annuaire, à celui de l'instance de base de données et à celui de la base de données contient les rôles suivants :

Propriétaire de l'instance de serveur d'annuaire
Un ID utilisateur système doit exister sur l'ordinateur qui sert de propriétaire de l'instance de serveur d'annuaire. L'ID du propriétaire d'instance de serveur d'annuaire est également le nom de l'instance de serveur d'annuaire. Cet utilisateur est autorisé à gérer l'instance de serveur d'annuaire.

Sous Windows, tous les membres du groupe Administrateurs sont également autorisés à gérer l'instance de serveur d'annuaire. Sous AIX, Linux et Solaris, le groupe primaire du propriétaire de l'instance de serveur d'annuaire est également autorisé à gérer l'instance de serveur d'annuaire.

Remarque : Sous AIX, Linux et Solaris, les noms des propriétaires d'instance sont sensibles à la casse. Vous devez toujours spécifier le nom et le propriétaire de l'instance de serveur d'annuaire exactement comme l'ID utilisateur. L'exemple suivant contient deux noms de propriétaire différents, `JoeSmith` et `joesmith`.

Propriétaire de l'instance de base de données
L'ID utilisateur qui est propriétaire de l'instance de base de données est aussi propriétaire de l'instance de base de données qui est configurée pour l'instance de serveur d'annuaire. Le nom de l'instance de base de données et le nom du propriétaire de l'instance de base de données sont les mêmes. Cet utilisateur gère l'instance de base de données. Le propriétaire de l'instance de serveur d'annuaire peut également gérer l'instance de base de données. Par défaut, cet ID utilisateur est le même que l'ID utilisateur du propriétaire de l'instance de serveur d'annuaire.

Propriétaire de la base de données
Cet ID utilisateur possède la base de données utilisée par l'instance de serveur d'annuaire et y stocke les données d'annuaire. La base de données est stockée sur l'instance de base de données que possède le propriétaire de l'instance de base de données. L'instance de serveur d'annuaire utilise l'ID utilisateur du propriétaire de la base de données et son mot de passe pour la connexion à la base de données.

Règles d'attribution de nom

Les ID utilisateur et le groupe primaire d'une instance de serveur d'annuaire doivent respecter les règles d'attribution de nom.

Les règles d'attribution de nom s'appliquent aux utilisateurs suivants :

- Nom de l'instance de serveur d'annuaire (ID utilisateur qui possède l'instance de serveur d'annuaire).
- Nom de l'instance de base de données (ID utilisateur qui possède l'instance de base de données). Généralement, cet ID utilisateur est le même que le nom de l'instance de serveur d'annuaire.
- Sur les systèmes AIX, Linux et Solaris, il s'agit des groupes principaux d'ID utilisateur du propriétaire d'instance de serveur d'annuaire et de l'ID utilisateur du propriétaire de l'instance de base de données.

Remarque : Lorsque vous créez un ID utilisateur et un groupe, vous devez leur affecter des droits. Voir «Conditions requises pour la création des utilisateurs et des groupes», à la page 127.

Les ID utilisateur et de groupe doivent respecter les conditions ci-après.

- Ils ne doivent pas comporter plus de 8 caractères.
- Ils ne doivent pas porter l'un des noms suivants :
  - `USERS`
  - `ADMINS`
  - `GUESTS`
  - `PUBLIC`

  - LOCAL
  - idsldap
- Ils ne peuvent pas commencer par l'un des préfixes suivants :
  - IBM
  - SQL
  - SYS
- Ils ne doivent pas contenir de caractères accentués
- Il peuvent contenir les caractères suivants :
  - De A à Z
  - De a à z
  - De 0 à 9
  - _ (trait de soulignement)
- Ils doivent commencer par l'un des caractères suivants :
  - De A à Z
  - De a à z

Conditions requises pour la création des utilisateurs et des groupes

Lorsque vous créez des utilisateurs et des groupes pour une instance, vous devez leur affecter des droits, et définir les utilisateurs en tant que membres des groupes adéquats.

Lorsque vous avez créé les utilisateurs et les groupes requis pour une instance, vous devez leur affecter des droits appropriés et ajouter les utilisateurs aux groupes. Les conditions ci-après doivent être respectées pour les ID des utilisateurs et des groupes.

Windows

- Définissez le propriétaire de l'instance de serveur d'annuaire et le propriétaire de l'instance de base de données en tant que membres du groupe d'administrateurs.
- Définissez, comme valeur de l'environnement local du propriétaire de l'instance de la base de données, la langue dans laquelle le serveur doit générer les messages. Si nécessaire, connectez-vous en tant qu'utilisateur et corrigez l'environnement local.

AIX, Linux et Solaris

- Définissez l'ID root en tant que membre du groupe primaire du propriétaire de l'instance du serveur d'annuaire et du propriétaire de l'instance de base de données.
- Ajoutez l'ID root en tant que membre du groupe idsldap.
- Définissez le propriétaire de l'instance de serveur d'annuaire et le propriétaire de l'instance de base de données en tant que membres du groupe idsldap.
- Créez les répertoires de base du propriétaire de l'instance de serveur d'annuaire et celui du propriétaire de l'instance de base de données.
- Affectez les droits appropriés au répertoire de base du propriétaire de l'instance de serveur d'annuaire.
  - L'utilisateur propriétaire de l'instance est le propriétaire de l'instance du serveur d'annuaire.

  - Le groupe propriétaire de l'instance est le groupe primaire du propriétaire de l'instance de serveur d'annuaire.
  - Vous devez affecter les droits en lecture, écriture et exécution sur le répertoire de base au propriétaire de l'instance de serveur d'annuaire et à son groupe primaire.
- Affectez les droits en lecture, écriture et exécution sur l'emplacement dans lequel la base de données est créée pour le propriétaire de l'instance de serveur d'annuaire et son groupe primaire.
- Le propriétaire de l'instance de serveur d'annuaire et le propriétaire de l'instance de base de données pour l'instance d'annuaire peuvent être des utilisateurs différents. Dans ce cas, le propriétaire de l'instance de serveur d'annuaire doit faire partie du groupe primaire du propriétaire de l'instance de base de données.
- Si le propriétaire de l'instance de serveur d'annuaire, le propriétaire de l'instance DB2 et le propriétaire de la base de données sont différents, ils doivent tous être membres du même groupe.
- Définissez le script de shell Korn (`/usr/bin/ksh`) comme shell de connexion du propriétaire de l'instance de serveur d'annuaire, du propriétaire de l'instance de base de données et du propriétaire de la base de données.

Vous devez définir le mot de passe du propriétaire de l'instance de serveur d'annuaire, du propriétaire de l'instance de base de données et du propriétaire de la base de données, qui doivent avoir été prêts à être utilisés. Le mot de passe ne doit pas arriver à expiration, ni être en attente d'une validation quelconque. Vous pouvez vérifier si le mot de passe est correctement défini en accédant à telnet sur l'ordinateur et en vous connectant avec l'ID utilisateur et le mot de passe.

Lors de la configuration de la base de données, il est d'usage d'indiquer le répertoire de base du propriétaire de l'instance base de données comme emplacement de la base de données, bien que cela ne soit pas obligatoire. Si vous indiquez un autre emplacement, 3 à 4 Mo d'espace doivent être disponibles dans le répertoire de base du propriétaire de l'instance de base de données. DB2 crée des liens et ajoute des fichiers dans le répertoire de base du propriétaire de l'instance de base de données, même si la base de données elle-même est située à un autre emplacement. Si le répertoire de base du propriétaire de l'instance ne contient pas suffisamment d'espace, vous pouvez en ajouter, ou changer de répertoire de base.

Exemples

Pour créer un propriétaire d'instance qui remplisse les conditions d'un propriétaire d'instance de serveur d'annuaire, vous pouvez utiliser la commande **idsadduser**. La commande **idsadduser** est dans le sous-répertoire `sbin` du répertoire d'installation d'IBM Security Directory Server.

Exemple 1 :

Pour créer un compte utilisateur sous AIX, Linux ou Solaris avec les valeurs ci-après, lancez la commande **idsadduser**.

- Nom d'utilisateur : `JoeSmith`
- Groupe primaire : `employees`
- Répertoire de base : `/home/joe` (Sous Solaris, utilisez `/export/home/joe`)
- Mot de passe : `joespw`

```
idsadduser –u JoeSmith –g employees –l /home/joe –w joespw
```

Exemple 2 :

Pour créer un compte utilisateur en que membre du groupe des administrateurs sous Windows avec les valeurs ci-après, lancez la commande **idsadduser**.

- Nom d'utilisateur : `JoeSmith`
- Mot de passe : `joespw`

```
idsadduser –u JoeSmith –w joespw
```

Planification de la configuration

Pour votre environnement de serveur d'annuaire, vous devez déterminer le type de données que vous allez stocker, leur structure et la sécurité à leur appliquer.

Vous devez prendre les décisions suivantes avant de configurer et de remplir votre base de données :

Le type de données que vous voulez stocker dans le serveur d'annuaire

Vous devez choisir le schéma à utiliser pour votre serveur d'annuaire, et le type de données que vous allez y stocker. Le serveur d'annuaire intègre un ensemble standard de définitions de types d'attribut et de classes d'objet. Pour personnaliser vos données, vous voudrez peut-être ajouter vos propres définitions de type d'attribut et de classes d'objet avant d'ajouter des données au serveur d'annuaire.

Vous pourrez apporter des ajouts ou des modifications au schéma après le chargement de vos données dans l'annuaire. Dans certains cas, la modification du schéma peut nécessiter le déchargement/rechargement des données.

La page de code à utiliser

Déterminez si la création de votre base de données s'effectue à l'aide de la page de codes locale ou du jeu de caractères universel (UTF-8). Dans le premier cas, les applications et les utilisateurs d'IBM Security Directory Server obtiennent les résultats de recherche dans l'ordre de tri attendu dans la langue nationale. Cependant, si vous utilisez une page de code locale, les données sont stockées dans l'annuaire dans cette page de code. Le choix d'UTF-8 permet de stocker dans la base de données des caractères codés sous UTF-8. Pour plus d'informations sur le format UTF-8, voir «Prise en charge d'UTF-8», à la page 130.

Remarque : Si vous souhaitez utiliser des balises de langue, la page de code de la base de données doit UTF-8.

La structure hiérarchique pour le stockage de vos données d'annuaire

IBM Security Directory Server stocke les données d'annuaire dans une arborescence hiérarchique. Le nom des entrées d'annuaire est basé sur leur position relative au sein de l'arborescence. Il est donc important de définir une organisation logique de votre annuaire qui corresponde à votre environnement LDAP. Une organisation logique facilite la localisation des informations par les clients.

Les modalités de sécurisation de vos données

Pour empêcher l'accès aux données sur un port non sécurisé, vous pouvez configurer des communications sécurisées pour le serveur d'annuaire. Pour plus d'informations sur la sécurisation des données, voir la section Administration de la documentation IBM Security Directory Server.

Droits d'accès aux données d'annuaire
Pour plus d'informations sur l'utilisation des droits d'accès, consultez les informations relatives aux listes de contrôle d'accès, dans la section Administration de la documentation IBM Security Directory Server.

Conditions d'utilisation d'un serveur proxy
Si les données du répertoire sont volumineuses et si l'environnement nécessite beaucoup d'opérations d'écriture, vous devez réfléchir à la mise en place d'un serveur proxy. Il est possible d'effectuer une mise à l'échelle appropriée des environnements de répertoire volumineux nécessitant de nombreuses opérations de lecture par la configuration de la réplication. Consultez la liste des fonctions prises en charge dans un serveur proxy dans la section Administration de la documentation IBM Security Directory Server, avant de décider d'utiliser un serveur proxy.

Prise en charge d'UTF-8

Le serveur d'annuaire peut être configuré pour gérer tous les caractères nationaux susceptibles d'être représentés en UTF-8.

IBM Security Directory Server prend en charge un grand nombre de jeux de caractères nationaux via le jeu de caractères UTF-8 (UCS Transformation Format). Dans le protocole LDAP version 3, tous les caractères échangés entre le client LDAP et le serveur LDAP sont codées au format UTF-8.

En fonction de la page de code utilisée pour configurer la base de données, le serveur détermine les types de caractères qui peuvent être stockés et sur lesquels des recherches peuvent être effectuées. Le jeu de caractères de la base de données peut être UTF-8, ou le jeu de caractères local du système sur lequel le serveur est installé. Le jeu de caractères local dépend des paramètres régionaux, de la langue et de la page de codes du système.

L'option UTF-8 permet de stocker dans la base de données des caractères codés sous UTF-8. Les clients LDAP installés sur un système qui prend en charge toutes les langues compatibles avec UTF-8 peuvent accéder à l'annuaire et y faire des recherches dont les résultats s'affichent correctement. Les client LDAP installés sur un système avec un jeu de caractères local peuvent avoir des difficultés à afficher des résultats extraits du serveur dans un autre jeu de caractères.

L'utilisation d'une base de données UTF-8 présente des avantages en termes de performances car aucune conversion de données n'est nécessaire lors de l'enregistrement de données dans la base de données ou lors de la récupération de données à partir de cette base.

Remarque : Si vous souhaitez utiliser des balises de langue, la base de données doit être une base de données UTF-8.

Utilisation d'UTF-8 dans un serveur d'annuaire

Avant de choisir la page de code à utiliser, vous devez comprendre comment un serveur d'annuaire utilise la page de code pour stocker les données d'annuaire et y accéder.

Dans une base de données UTF-8, l'ordre de tri des caractères est fixe. Il s'agit de l'ordre des valeurs binaires des caractères UTF-8. Il n'est donc pas possible d'effectuer des tris adaptés à telle ou telle langue dans une base de données UTF-8.

Le choix de la page de code UTF-8 n'est donc pas forcément le meilleur pour votre base de données si vous souhaitez obtenir les résultats suivants :

- Une recherche avec un filtre de tri, par exemple `"name >= SMITH"`, si l'ordre de tri de l'environnement local doit être respecté.
- Une recherche avec une commande de tri des résultats, si l'ordre de tri de l'environnement local doit être respecté.

Pour ces cas de figure, le système du serveur LDAP et tous les systèmes client doivent utiliser le même jeu de caractères et le même environnement local.

Par exemple, la base de données d'un serveur LDAP configurée avec l'environnement local espagnol renvoie des résultats qui sont triés dans l'ordre des caractères attendu par les clients espagnols. Cette configuration oblige l'ensemble de la communauté d'utilisateurs d'annuaire à utiliser le même jeu de caractères dans l'environnement local et le même ordre de tri.

Création d'un fichier LDIF contenant des valeurs en UTF-8 à l'aide des utilitaires du serveur

L'extension `charset` vous permet de créer un format LDIF avec des valeurs en UTF-8.

La création manuelle d'un fichier LDIF contenant des valeurs en UTF-8 est compliquée. Dans l'en-tête de fichier LDIF, vous pouvez spécifier une extension prenant en charge un jeu de caractères IANA (Internet Assigned Numbers Authority) et son numéro de version. Pour plus d'informations sur les jeux de caractères IANA pris en charge, voir «Jeux de caractères IANA pris en charge», à la page 132.

Exemples

Exemple 1 :

La balise `charset` permet aux utilitaires du serveur d'effectuer une conversion automatique entre le jeu de caractères défini et UTF-8.

```
version: 1
charset: ISO-8859-1

dn: cn=Juan Griego, ou=University of New Mexico, o=sample
cn: Juan Griego
sn: Griego
description:: V2hhdCBhIGNhcmVmdWwgcmVhZGVyIHlvd
title: Associate Dean
title: [en espagnol]
jpegPhoto:< file:///usr/local/photos/jgriego.jpg
```

Dans l'exemple qui suit, tous les attributs dont la valeur est séparée du nom de l'attribut par un deux-points sont convertis du jeu de caractères `ISO-8859-1` en UTF-8. tous les attributs dont la valeur est séparée du nom de l'attribut par deux deux-points, par exemple `description:: V2hhdCBhIGNhcmVmdWwgcmVhZGVyIHlvd`, doivent être codés en `base 64` et être dans des chaînes de caractères en binaire ou en UTF-8. Les valeurs extraites d'un fichier, telles que l'attribut `jpegPhoto` qui est défini par une adresse Web, doivent également être en binaires ou UTF-8. Pour ces valeurs, aucune conversion n'est réalisée entre le jeu de caractère (`charset`) défini et UTF-8.

Exemple 2 :

Dans cet exemple de fichier LDIF sans la balise `charset`, le contenu doit être au format UTF-8 :

```
# IBM Directorysample LDIF file
#
# The suffix "o=sample" should be defined before attempting to load
# this data.

 version: 1

 dn: o=sample
 objectclass: top
 objectclass: organization
 o: sample

 dn: ou=Austin, o=sample
 ou: Austin
 objectclass: organizationalUnit
 seealso: cn=Mary Smith, ou=Austin, o=sample
```

Dans IBM Security Directory Server, le fichier LDIF avec le contenu suivant peut être utilisé sans l'information d'en-tête `version: 1` :

```
# IBM Directorysample LDIF file
#
# Le suffixe "o=sample" doit être défini avant de charger
# ces données.

 dn: o=sample
 objectclass: top
 objectclass: organization
 o: sample

 dn: ou=Austin, o=sample
 ou: Austin
 objectclass: organizationalUnit
 seealso: cn=Linda Carlesberg, ou=Austin, o=sample
```

Jeux de caractères IANA pris en charge

Vous pouvez utiliser le jeu de caractères IANA (Internet Assigned Number Authority) dans un fichier LDIF ou avec l'interface du client C pour identifier le jeu de caractères des données d'annuaire.

IBM Security Directory Server prend en charge les jeux de caractères IANA (Internet Assigned Number Authority) par systèmes d'exploitation.

Pour plus d'informations sur les jeux de caractères enregistrés par IANA, voir le site Web Character Sets à l'adresse www.iana.org/assignments/character-sets.

Tableau 38. Jeux de caractères définis par IANA

Nom du	Environnement local					Page de code DB2	
jeu de caractères	HP-UX	Linux, Linux_390,	Windows	AIX	Solaris	UNIX	Windows
ISO-8859-1	X	X	X	X	X	819	1252
ISO-8859-2	X	X	X	X	X	912	1250
ISO-8859-5	X	X	X	X	X	915	1251
ISO-8859-6	X	X	X	X	X	1089	1256
ISO-8859-7	X	X	X	X	X	813	1253

Tableau 38. Jeux de caractères définis par IANA (suite)

Nom du	Environnement local					Page de code DB2	
jeu de caractères	HP-UX	Linux, Linux_390,	Windows	AIX	Solaris	UNIX	Windows
ISO-8859-8	X	X	X	X	X	916	1255
ISO-8859-9	X	X	X	X	X	920	1254
ISO-8859–15	X	n/a	X	X	X		
IBM437	n/a	n/a	X	n/a	n/a	437	437
IBM850	n/a	n/a	X	X	n/a	850	850
IBM852	n/a	n/a	X	n/a	n/a	852	852
IBM857	n/a	n/a	X	n/a	n/a	857	857
IBM862	n/a	n/a	X	n/a	n/a	862	862
IBM864	n/a	n/a	X	n/a	n/a	864	864
IBM866	n/a	n/a	X	n/a	n/a	866	866
IBM869	n/a	n/a	X	n/a	n/a	869	869
IBM1250	n/a	n/a	X	n/a	n/a		
IBM1251	n/a	n/a	X	n/a	n/a		
IBM1253	n/a	n/a	X	n/a	n/a		
IBM1254	n/a	n/a	X	n/a	n/a		
IBM1255	n/a	n/a	X	n/a	n/a		
IBM1256	n/a	n/a	X	n/a	n/a		
TIS-620	n/a	n/a	X	X	n/a	874	874
EUC-JP	X	X	n/a	X	X	954	n/a
EUC-KR	n/a	n/a	n/a	X	X	970	n/a
EUC-CN	n/a	n/a	n/a	X	X	1383	n/a
EUC-TW	X	n/a	n/a	X	X	964	n/a
Shift-JIS	n/a	X	X	X	X	932	943
KSC	n/a	n/a	X	n/a	n/a	n/a	949
GBK	n/a	n/a	X	X	n/a	1386	1386
Big5	X	n/a	X	X	X	950	950
GB18030	n/a	X	X	X	X		
HP15CN	X (avec des caractères non-GB18030)						

Remarque :

- Le jeu de caractères chinois standard, GB18030, est pris en charge par les correctifs disponibles sur les sites www.oracle.com et www.microsoft.com.
- Sous Windows, vous devez définir la valeur TRUE pour la variable d'environnement *zhCNGB18030*.

Caractères ASCII de 33 à 126

Utilisez la table de caractères ASCII pour déterminer les caractères à utiliser pour les valeurs de départ et de sel du chiffrement de l'instance de serveur d'annuaire.

Vous pouvez utiliser les caractères ASCII de 33 à 126 dans la chaîne de valeurs de départ de chiffrement et dans la valeur de sel de chiffrement.

Tableau 39. Caractères ASCII de 33 à 126

Code ASCII	Nom du	Code ASCII	Nom du	Code ASCII	Nom du
33	! point d'exclamation	34	" guillemets doubles	35	# symbole dièse
36	$ signe dollar	37	% symbole pourcentage	38	& symbole perluète
39	' apostrophe	40	(parenthèse gauche	41	) parenthèse droite
42	* astérisque	43	+ signe plus	44	, virgule
45	- tiret	46	. point	47	/ barre oblique
48	0	49	1	50	2
51	3	52	4	53	5
54	6	55	7	56	8
57	9	58	: deux points	59	; point virgule
60	< signe inférieur à	61	= signe égal	62	> signe supérieur à
63	? point d'interrogation	64	@ signe arobas	65	A a majuscule
66	B b majuscule	67	C c majuscule	68	D d majuscule
69	E e majuscule	70	F f majuscule	71	G g majuscule
72	H h majuscule	73	I i majuscule	74	J j majuscule
75	K k majuscule	76	L l majuscule	77	M m majuscule
78	N n majuscule	79	O o majuscule	80	P p majuscule
81	Q q majuscule	82	R r majuscule	83	S s majuscule
84	T t majuscule	85	U u majuscule	86	V v majuscule
87	W w majuscule	88	X x majuscule	89	Y y majuscule
90	Z z majuscule	91	[crochet gauche	92	\ barre oblique inversée
93	] crochet droit	94	^ caret	95	_ trait de soulignement
96	` accent grave	97	a a minuscule	98	b b minuscule
99	c c minuscule	100	d d minuscule	101	e e minuscule
102	f f minuscule	103	g g minuscule	104	h h minuscule
105	i i minuscule	106	j j minuscule	107	k k minuscule
108	l l minuscule	109	m m minuscule	110	n n minuscule
111	o o minuscule	112	p p minuscule	113	q q minuscule
114	r r minuscule	115	s s minuscule	116	t t minuscule
117	u u minuscule	118	v v minuscule	119	w w minuscule
120	x x minuscule	121	y y minuscule	122	z z minuscule
123	{ accolade gauche	124	| barre verticale	125	} accolade droite
126	~ tilde				

Chapitre 18. Création et administration d'instance

Pour utiliser un serveur d'annuaire dans une infrastructure d'identité, vous devez créer une instance de serveur d'annuaire qui correspond à vos besoins.

Après l'installation d'IBM Security Directory Server, vous devez créer une instance de serveur d'annuaire puis définir le nom distinctif et le mot de passe administrateur de l'instance. Vous pouvez créer un serveur d'annuaire complet ou un serveur proxy. Avant de créer une instance de serveur d'annuaire ou de serveur proxy, vous devez créer un ID utilisateur système sur l'ordinateur. Cet ID utilisateur est le propriétaire de l'instance de serveur d'annuaire ou de serveur proxy.

Dans le cas d'un serveur d'annuaire complet, vous devez créer une base de données DB2 et la configurer dans l'instance de serveur d'annuaire. Pour créer une base de données DB2, vous devez installer sur l'ordinateur une version de DB2 prise en charge. Vous devez vérifier si le fichier `ldapdb.properties` contient le chemin d'installation et la version de DB2. Pour plus d'informations, voir Annexe C, «Mise à jour manuelle du fichier `ldapdb.properties`», à la page 257.

Remarque : Lorsque vous utilisez l'outil d'administration d'instance (**idsxinst**) d'IBM Security Directory Server pour créer une instance de serveur d'annuaire complet, l'outil crée aussi le fichier `ldapdb.properties` dans le répertoire de base de l'instance. Sous Windows, le fichier `ldapdb.properties` est dans le répertoire *rép_base_instance*\idsslapd-*nom_instance*\etc. Sous AIX, Linux ou Solaris, le fichier est dans le répertoire *rép_base_instance*/idsslapd-*nom_instance*/etc.

Dans le cas d'une instance de serveur proxy, ne créez pas et ne configurez pas une base de données DB2.

L'outil d'administration d'instance est une interface graphique que vous pouvez utiliser pour créer et gérer des instances de serveur d'annuaire. IBM Java Development Kit est requis pour l'utilisation de l'outil d'administration d'instance. Lorsque vous l'utilisez, l'outil fournit un assistant qui vous guide dans la réalisation des tâches.

Vous pouvez utiliser l'outil d'administration d'instance pour créer, afficher, copier et supprimer des instances, ainsi que pour modifier les informations les concernant. Vous pouvez également employer cet outil pour créer ou éditer des utilisateurs qui possèdent des instances de serveur d'annuaire et mettre à niveau des instances à partir de versions précédentes d'IBM Security Directory Server. Vous pouvez utiliser l'outil d'administration d'instance pour démarrer ou arrêter le serveur ou le serveur d'administration de vos instances. En outre, vous pouvez ouvrir l'outil de configuration à partir de l'outil d'administration d'instance.

Vous pouvez également vous servir des utilitaires de ligne de commande pour créer et gérer les instances de serveur d'annuaire.

Démarrage de l'outil d'administration d'instance

Démarrez l'outil d'administration d'instance pour créer et administrer une instance de serveur d'annuaire ou une instance de serveur proxy.

Avant de commencer

Pour utiliser l'outil d'administration d'instance, vous devez installer IBM Security Directory Server avec la fonction serveur et/ou la fonction serveur proxy. Pour exécuter l'outil d'administration d'instance, connectez-vous avec les données d'identification suivantes :

AIX, Linux et Solaris
Connectez-vous en tant qu'utilisateur root.

Windows
Connectez-vous en tant que membre du groupe des administrateurs.

IBM Java Development Kit doit exister dans le chemin d'installation d'IBM Security Directory Server. Pour le chemin d'installation par défaut d'IBM Security Directory Server, voir «Emplacements d'installation par défaut», à la page 27.

Procédure

Pour utiliser l'outil d'administration d'instance, choisissez l'une des méthodes suivantes :

Méthodes d'ouverture de l'outil d'administration d'instance	**Commande à exécuter :**
Installation de la fonction serveur d'IBM Security Directory Server	Dans la page **Récapitulatif**, cliquez sur **Outil d'administration d'instance (idsxinst)**. Pour plus d'informations, voir «Installation à l'aide d'IBM Installation Manager», à la page 31.
Commande `idsxinst`	**Windows** 1. Le répertoire en cours doit être le sous-répertoire `sbin` du répertoire d'installation d'IBM Security Directory Server. 2. Lancez la commande **`idsxinst`**. **Remarque :** Vous pouvez aussi cliquer sur **Démarrer** > **Tous les programmes** > **IBM Security Directory Server 6.3.1** > **Outil d'administration d'instance**. **AIX, Linux et Solaris** 1. Le répertoire en cours doit être le sous-répertoire `sbin` du répertoire d'installation d'IBM Security Directory Server. 2. Lancez la commande **`idsxinst`**. Pour plus d'informations sur le chemin d'installation d'IBM Security Directory Server, voir «Emplacements d'installation par défaut», à la page 27.

Démarrage de l'outil d'administration d'instance pour la mise à niveau d'une instance

Exécutez l'outil d'administration d'instance avec ses paramètres pour mettre à niveau une instance distante contenant des données de sauvegarde.

Avant de commencer

Avant de mettre à niveau une instance distante, vous devez vérifier que les conditions ci-après sont remplies.

- L'ordinateur doit contenir les données de sauvegarde de l'instance, créées avec la commande **migbkup**. Vous devez utiliser la commande **migbkup** de la version à laquelle vous voulez mettre à niveau l'instance distante.
- Connectez-vous en tant qu'utilisateur root sur les systèmes AIX, Linux et Solaris. Sous Windows, connectez-vous en tant que membre du groupe des administrateurs.

Procédure

1. Accédez à l'invite de commande.
2. Le répertoire de travail en cours doit être le sous-répertoire `sbin` du répertoire d'installation d'IBM Security Directory Server. Pour plus d'informations sur le chemin d'installation par défaut, voir «Emplacements d'installation par défaut», à la page 27.
3. Exécutez la commande **idsxinst** avec la syntaxe ci-après.

   ```
   idsxinst -migrate rép_sauvegarde
   ```

   Remplacez la variable *rép_sauvegarde* par le répertoire dans lequel vous avez stocké les données de sauvegarde de l'instance, créées avec la commande **migbkup**.

Création d'une instance de serveur d'annuaire

Pour utiliser une instance de serveur d'annuaire dans un environnement LDAP avec les meilleures performances, créez une instance dont le chiffrement est synchronisé avec l'instance existante.

Si vous créez une instance de serveur d'annuaire en tant que copie d'une instance existante, le chiffrement des deux instances est synchronisé. Vous n'avez pas à le synchroniser vous-même.

Si vous créez une instance qui n'est pas une copie d'une instance existante, synchronisez le chiffrement de la nouvelle instance avec celui de l'instance existante. Vous devez synchroniser le chiffrement des instances de serveur pour obtenir les meilleures performances dans les environnements suivants :

- La réplication
- Un annuaire distribué
- L'importation et l'exportation de données LDIF entre les instances du serveur

Vous devez synchroniser les instances de serveur avant d'effectuer les opérations ci-après.

- Démarrez la nouvelle instance du serveur.
- Exécuter la commande **idsbulkload** sur l'instance du serveur

- Exécuter la commande **idsldif2db** sur l'instance du serveur

Pour plus d'informations sur la synchronisation des serveurs d'annuaire, consultez la section *Administration* de la documentation IBM Security Directory Server.

Lorsque vous avez créé une instance de serveur d'annuaire et que vous l'avez configurée avec une base de données DB2, sauvegardez-la. Vous devez sauvegarder la configuration, le schéma, la base de données DB2 et les fichiers de dissimulation de clés de l'annuaire. Vous pouvez utiliser la commande **idsdbback** pour créer une sauvegarde de l'instance de serveur d'annuaire. La commande **idsdbrestore** permet de restaurer les fichiers de dissimulation de clés de l'annuaire, si nécessaire. Pour plus d'informations sur les commandes de sauvegarde et de restauration, voir le manuel *Command Reference*.

Création d'une instance à l'aide de l'outil d'administration d'instance

Vous devez évaluer les besoins de votre environnement avant de créer une instance de serveur d'annuaire qui y réponde.

Vous pouvez utiliser l'outil d'administration d'instance pour créer une instance de différentes manières :

- Créez une instance par défaut en indiquant un nom et d'autres paramètres par défaut. Voir «Création de l'instance de serveur d'annuaire par défaut».
- Créez une instance avec des paramètres personnalisés. Voir «Création d'une instance de serveur d'annuaire avec des paramètres personnalisés», à la page 140.
- Mettez à niveau une instance à partir d'une version précédente d'IBM Security Directory Server. Voir «Mise à niveau d'une instance d'une version précédente à l'aide de la commande **idsimigr**», à la page 94 ou «Mise à niveau d'une instance d'une version précédente à l'aide de l'outil d'administration d'instance», à la page 153.
- Créez la copie d'une instance qui existe sur cet ordinateur ou sur un autre ordinateur. Voir «Création d'une copie d'une instance existante à l'aide de l'outil d'administration d'instance», à la page 159.

Création de l'instance de serveur d'annuaire par défaut

Utilisez l'option de création d'instance par défaut pour créer une instance de serveur d'annuaire avec un nom d'instance prédéfini et des paramètres par défaut.

Avant de commencer

Pour créer une instance par défaut, vous devez effectuer les tâches ci-après.

1. Installez IBM Security Directory Server avec la fonction serveur. Voir «Installation à l'aide d'IBM Installation Manager», à la page 31.
2. Installez IBM DB2. Voir «Installation à l'aide d'IBM Installation Manager», à la page 31.
3. Vérifiez si le fichier `ldapdb.properties` contient le chemin d'installation et la version de DB2. Voir Annexe C, «Mise à jour manuelle du fichier `ldapdb.properties`», à la page 257.

Pourquoi et quand exécuter cette tâche

Si votre ordinateur contient une instance de serveur d'annuaire ayant le nom d'instance par défaut, vous ne pouvez pas créer l'instance de serveur d'annuaire par défaut.

L'instance de serveur d'annuaire par défaut possède les paramètres suivants, qui ne peuvent être modifiés :

Tableau 40. Paramètres d'une instance de serveur par défaut

Paramètres	Microsoft Windows	AIX et Linux	Solaris
Nom	`dsrdbm01`	`dsrdbm01`	`dsrdbm01`
Emplacement de l'instance	`c:\idsslapd-dsrdbm01`	`/home/dsrdbm01`	`/export/home/dsrdbm01`
Nom du groupe	`Administrators`	`grrdbm01`	`grrdbm01`
Nom distinctif de l'administrateur	`cn=root`	`cn=root`	`cn=root`
Nom de base de données	`dsrdbm01`	`dsrdbm01`	`dsrdbm01`

Les espaces table DB2 de l'instance de serveur d'annuaire par défaut sont de type DMS (Database Managed Storage).

Pour l'instance de serveur d'annuaire par défaut, l'Outil d'administration d'instance crée le suffixe `o=sample`. Vous pouvez ajouter des suffixes par la suite avec l'Outil de configuration ou la commande **idscfgsuf**. Pour plus d'informations, voir «Configuration des suffixes», à la page 209.

Procédure

1. Démarrez l'outil d'administration d'instance. Voir «Démarrage de l'outil d'administration d'instance», à la page 135.
2. Cliquez sur **Créer une instance**.
3. Dans la fenêtre **Créer une instance de serveur d'annuaire**, procédez comme suit.
   a. Cliquez sur **Créer une instance par défaut**.
   b. Cliquez sur **Suivant**.
   c. Dans la zone **Mot de passe de l'utilisateur**, entrez le mot de passe du compte utilisateur qui possède l'instance de serveur d'annuaire.
   d. Dans la zone **Confirmer le mot de passe**, entrez de nouveau le mot de passe du compte utilisateur qui possède l'instance de serveur d'annuaire.
   e. Dans la zone **Valeur de départ de chiffrement**, entrez la valeur de départ de chiffrement de l'instance du serveur d'annuaire.

      A faire : Vous devez noter la valeur de départ de chiffrement de l'instance de serveur d'annuaire, car vous pouvez en avoir besoin pour d'autres tâches de configuration.
      La valeur de départ du chiffrement ne doit contenir que des caractères `ISO-8859-1 ASCII` imprimables dont la valeur est comprise entre 33 et 126. Elle doit comporter entre 12 et 1016 caractères. Pour des informations sur les caractères à utiliser, voir «Caractères ASCII de 33 à 126», à la page 134.
      Le serveur d'annuaire utilise la valeur de départ de chiffrement pour générer des valeurs de clés secrètes AES (Advanced Encryption Standard).

Les fichiers de dissimulation de clés d'une instance de serveur d'annuaire stocke les valeurs des clés et sont utilisés pour chiffrer et déchiffrer le mot de passe et les attributs.

f. Dans la zone **Confirmer le chiffrement initial**, entrez la valeur de départ de chiffrement de l'instance du serveur d'annuaire.

g. Dans la zone **Mot de passe du nom distinctif de l'administrateur**, entrez le mot de passe administrateur de l'instance de serveur d'annuaire.

h. Dans la zone **Confirmer le mot de passe**, entrez le mot de passe de l'administrateur de l'instance du serveur d'annuaire.

i. Cliquez sur **Suivant**.

j. Vérifiez les information de l'instance de serveur d'annuaire par défaut et

k. Pour démarrer la création de l'instance de serveur d'annuaire par défaut, cliquez sur **Terminer**. La fenêtre Résultats contenant les informations de journal s'affiche.

4. Vérifiez les informations de journal dans la fenêtre **Résultats**.
5. Pour fermer la fenêtre **Résultats**, cliquez sur **Fermer**.
6. Pour fermer l'outil d'administration d'instance, cliquez sur **Fermer**.

Résultats

L'Outil d'administration d'instance crée l'instance de serveur d'annuaire par défaut, `dsrdbm01`, sur l'ordinateur.

Que faire ensuite

Vous devez démarrer le processus `ibmslapd` et le serveur d'administration associé à l'instance de serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration», à la page 162.

Création d'une instance de serveur d'annuaire avec des paramètres personnalisés

Utilisation du serveur d'administration d'instance pour créer une instance de serveur d'annuaire avec des valeurs personnalisées conformes à vos besoins.

Avant de commencer

Pour créer une instance de serveur d'annuaire, vous devez effectuer les tâches ci-après.

1. Installez IBM Security Directory Server avec la fonction serveur. Voir «Installation à l'aide d'IBM Installation Manager», à la page 31.
2. Pour créer un serveur d'annuaire complet avec un programme dorsal RDBM, installez IBM DB2. Voir «Installation à l'aide d'IBM Installation Manager», à la page 31.
3. Vérifiez si le fichier `ldapdb.properties` contient le chemin d'installation et la version de DB2. Voir Annexe C, «Mise à jour manuelle du fichier `ldapdb.properties`», à la page 257.

Procédure

1. Démarrez l'outil d'administration d'instance. Voir «Démarrage de l'outil d'administration d'instance», à la page 135.
2. Cliquez sur **Créer une instance**.

3. Dans le panneau **Création ou migration** de la fenêtre **Créer une instance de serveur d'annuaire**, cliquez sur **Créer une instance de serveur d'annuaire**.
4. Cliquez sur **Suivant**.
5. Dans le panneau **Détails de l'instance** de la fenêtre **Créer une instance de serveur d'annuaire**, entrez les valeurs ci-après.
   a. Dans la liste **Nom d'utilisateur**, sélectionnez le nom de l'utilisateur qui est propriétaire de l'instance du serveur d'annuaire. L'instance de serveur d'annuaire prend le même nom que l'utilisateur.
   b. Si vous voulez associer un nouveau compte d'utilisateur à l'instance, cliquez sur **Créer un utilisateur**. Dans la fenêtre **Créer un utilisateur pour l'instance de serveur d'annuaire**, procédez de la manière suivante :
      1) Dans la zone **Nom d'utilisateur**, entrez le nom de l'utilisateur.
      2) Dans la zone **Mot de passe**, entrez le mot de passe associé au compte utilisateur.
      3) Dans la zone **Confirmation du mot de passe**, entrez le mot de passe du compte utilisateur.
      4) Dans la zone **Répertoire de base**, entrez le répertoire de base à configurer pour le compte utilisateur. Vous pouvez cliquer sur **Parcourir** pour localiser le répertoire de base.
      5) Dans la zone **Groupe primaire**, entrez le nom du groupe primaire de l'utilisateur.
      6) Pour créer le compte utilisateur, cliquez sur **Créer**.
   c. Pour modifier un compte utilisateur existant, sélectionnez le nom d'utilisateur dans la liste **Nom d'utilisateur** et cliquez sur **Modifier un utilisateur**. Dans la fenêtre **Editer l'utilisateur de l'instance de serveur d'annuaire**, procédez de la manière suivante :
      1) Le nom d'utilisateur figure dans la zone **Nom d'utilisateur**.
      2) Dans la zone **Mot de passe**, entrez le mot de passe associé au compte utilisateur.
      3) Dans la zone **Confirmation du mot de passe**, entrez le mot de passe du compte utilisateur.
      4) Dans la zone **Répertoire de base**, entrez le répertoire de base à configurer pour le compte utilisateur. Vous pouvez cliquer sur **Parcourir** pour localiser le répertoire de base.
      5) Dans la zone **Groupe primaire**, entrez le nom du groupe primaire de l'utilisateur.
      6) Pour éditer le compte utilisateur, cliquez sur **Modifier**.
6. Dans la zone **Emplacement de l'instance**, entrez l'emplacement de l'instance de serveur d'annuaire. Vous pouvez cliquer sur **Parcourir** pour localiser le répertoire de base de l'instance. L'emplacement doit contenir au moins 30 Mo d'espace disponible. Sous Windows, cet emplacement est une unité de disque, par exemple `C:`. Les fichiers de l'instance d'annuaire sont stockés dans le répertoire `\idsslapd-`*`nom_instance`* sur l'unité de disque de votre choix. La variable *nom_instance* est le nom de l'instance de serveur d'annuaire. Sur les systèmes AIX, Linux et Solaris, le répertoire de base du propriétaire de l'instance de serveur d'annuaire est l'emplacement de l'instance par défaut, mais vous pouvez définir un autre chemin.
7. Dans la zone **Chaîne de valeur de départ de chiffrement**, entrez la valeur de départ de chiffrement de l'instance du serveur d'annuaire.

A faire : Vous devez noter la valeur de départ de chiffrement de l'instance de serveur d'annuaire, car vous pouvez en avoir besoin pour d'autres tâches de configuration.
La valeur de départ du chiffrement ne doit contenir que des caractères ISO-8859-1 ASCII imprimables dont la valeur est comprise entre 33 et 126. Elle doit comporter entre 12 et 1016 caractères. Pour des informations sur les caractères à utiliser, voir «Caractères ASCII de 33 à 126», à la page 134. Le serveur d'annuaire utilise la valeur de départ de chiffrement pour générer des valeurs de clés secrètes AES (Advanced Encryption Standard). Les fichiers de dissimulation de clés d'une instance de serveur d'annuaire stocke les valeurs des clés et sont utilisés pour chiffrer et déchiffrer le mot de passe et les attributs.

8. Dans la zone **Confirmer le chiffrement initial**, entrez la valeur de départ de chiffrement de l'instance du serveur d'annuaire.
9. Si vous souhaitez indiquer une chaîne de sel de chiffrement, cliquez sur **Utiliser la valeur de sel de chiffrement**.
   a. Dans la zone **Chaîne de sel de chiffrement**, entrez la valeur de sel de chiffrement de l'instance du serveur d'annuaire. Le sel de chiffrement ne doit contenir que des caractères ISO-8859-1 ASCII imprimables dont la valeur est comprise entre 33 et 126. Le sel de chiffrement doit contenir 12 caractères. Pour des informations sur les caractères à utiliser, voir «Caractères ASCII de 33 à 126», à la page 134. Pour synchroniser le chiffrement d'un serveur d'annuaire avec une autre instance de serveur d'annuaire, vous devez utiliser les mêmes valeurs de départ et de sel de chiffrement.
   b. Dans la zone **Confirmer le sel de chiffrement**, entrez la valeur de sel de chiffrement de l'instance du serveur d'annuaire.
10. Facultatif : Dans la zone **Description de l'instance**, entrez la description de l'instance de serveur d'annuaire. La description permet d'identifier l'instance plus facilement.
11. Cliquez sur **Suivant**.
12. Dans la zone **Nom de l'instance DB2** du panneau **Détails de l'instance DB2**, entrez le nom de l'instance DB2 de l'instance du serveur d'annuaire.

    Remarque : L'instance DB2 de l'instance du serveur d'annuaire ne doit pas être configurée ni utilisée par d'autres programmes ou produits.

    Par défaut, le nom de l'instance DB2 est le même que celui du serveur d'annuaire. Cependant, vous pouvez entrer un autre nom pour l'instance DB2. Si vous entrez un nom différent, un ID utilisateur système portant le même nom doit exister sur l'ordinateur. Ce nom de compte utilisateur ne doit pas être associé à une autre instance de serveur d'annuaire.
13. Cliquez sur **Suivant**.
14. Dans le panneau **Paramètres TCP/IP pour les hôtes multiréseau**, sélectionnez l'une des options ci-après.
    - Si vous souhaitez que l'instance de serveur d'annuaires écoute sur toutes les adresses IP, sélectionnez **Intercepter toutes les adresses IP configurées**.
    - Si vous souhaitez que l'instance écoute sur un ensemble spécifique d'adresses IP configurées sur l'ordinateur, effectuez les opérations ci-après.
      a. Désélectionnez **Ecouter toutes les adresses IP configurées**.
      b. Dans la liste **Sélectionner les adresses IP spécifiques à écouter**, sélectionnez les adresses qui doivent être écoutées par l'instance.
15. Cliquez sur **Suivant**.

16. Dans le panneau **Paramètres de port TCP/IP**, entrez les valeurs ci-après.

    Remarque : Vous devez affecter des numéros de port uniques aux ports de serveur d'annuaire, car ils ne doivent pas entrer en conflit avec des ports déjà utilisés sur l'ordinateur. Sur les systèmes AIX, Linux et Solaris, les numéros de port de 1 à 1000 ne peuvent être utilisés que par l'utilisateur root.

    a. Dans la zone **Port du serveur**, entrez le numéro du port destiné à être le port non sécurisé du serveur. Vous pouvez entrer un nombre entre 1 et 65535.
    b. Dans la zone **Port sécurisé du serveur**, entrez le numéro du port destiné à être le port sécurisé du serveur. Vous pouvez entrer un nombre entre 1 et 65535.
    c. Dans la zone **Port du serveur d'administration**, entrez le numéro du port destiné à être le port non sécurisé du serveur d'administration. Vous pouvez entrer un nombre entre 1 et 65535.
    d. Dans la zone **Port sécurisé du serveur d'administration**, entrez le numéro du port destiné à être le port sécurisé du serveur d'administration. Vous pouvez entrer un nombre entre 1 et 65535.
    e. Cliquez sur **Suivant**.

17. Dans le panneau **Etapes facultatives**, effectuez les opérations ci-après.
    a. Pour configurer le nom distinctif et le mot de passe de l'administrateur de l'instance de serveur d'annuaire, sélectionnez **Configurer le DN et le mot de passe de l'administrateur**. Vous devez définir le nom distinctif et le mot de passe de l'administrateur des serveurs proxy et des serveurs d'annuaire complets.
    b. Pour configurer la base de données de l'instance du serveur d'annuaire, sélectionnez **Configurer la base de données**.
    c. Cliquez sur **Suivant**.

18. Dans le panneau **Configurer le DN et le mot de passe de l'administrateur**, effectuez les opérations ci-après.
    a. Dans la zone **DN de l'administrateur**, entrez un nom distinctif valide ou acceptez le nom distinctif par défaut, `cn=root`. Le nom distinctif de l'administrateur n'est pas sensible à la casse. Le nom distinctif de l'administrateur a accès à toutes les données de l'instance de serveur d'annuaire.
    b. Dans la zone **Mot de passe de l'administrateur**, entrez le mot de passe associé au nom distinctif de l'administrateur. Les mots de passe sont sensibles à la casse. Les caractères DBCS ne sont pas valides dans le mot de passe.
    c. Dans la zone **Confirmation du mot de passe**, entrez le mot de passe du nom distinctif de l'administrateur. Vous devez noter le mot de passe, car vous pourrez en avoir besoin ultérieurement.
    d. Cliquez sur **Suivant**.

19. Dans le panneau **Configurer la base de données**, effectuez les tâches suivantes pour configurer la base de données de l'instance du serveur d'annuaire : L'outil d'administration d'instance ajoute les informations sur la base de données dans le fichier de configuration de l'instance du serveur d'annuaire, `ibmslapd.conf`. Si la base de données n'existe pas, l'outil d'administration d'instance la crée.

a. Dans la zone **Nom utilisateur de base de données**, entrez un ID d'administrateur DB2 valide. Avant de configurer la base de données, vous devez vérifier que l'ID d'administrateur DB2 existe sur l'ordinateur et possède les droits d'accès requis.

   Remarque : Avant le démarrage du serveur, l'ID d'administrateur DB2 doit définir l'environnement local correspondant à la langue dans laquelle les messages du serveur doivent s'afficher.

b. Dans la zone **Mot de passe**, entrez le mot de passe de l'administrateur DB2. Le mot de passe est sensible à la casse.

   Remarque : Si vous modifiez le mot de passe système de l'administrateur DB2, vous ne pouvez pas le mettre à jour à l'aide de l'outil d'administration d'instance. Vous devez utiliser l'outil de configuration ou la commande **idscfgdb** avec le paramètre **-w**. Pour plus d'informations, voir «Gestion du mot de passe de l'administrateur de la base de données DB2», à la page 186.

c. Dans la zone **Nom de base de données**, entrez le nom d'une base de données DB2. Le nom doit contenir de 1 à 8 caractères.

d. Facultatif : Si vous voulez définir les paramètres de configuration suivants, sélectionnez **Affichage des options d'espace table avancées**.

   Remarque : DB2 peut créer des espaces table en utilisant le type de stockage de données SMS (System Managed Storage) ou DMS (Database Managed Storage). Le choix par défaut pour IBM Security Directory Server est DMS (Database Managed Storage). Les versions d'IBM Security Directory Server antérieures à 6.2 utilisent SMS pour toutes les bases de données. Si vous désélectionnez **Affichage des options d'espace table avancées**, les espaces table USERSPACE1 et LDAPSPACE sont créées au type DMS avec les tailles et les emplacements par défaut. Sous AIX, Linux et Solaris, le chemin et le nom de fichier par défaut de l'espace table USERSPACE1 est *emplacement_basededonnées*/*nom_instance*/NODE0000/SQL00001/USPACE. Sous Windows, le chemin et le nom de fichier par défaut de l'espace table USERSPACE1 est *emplacement_basededonnées**nom_instance*\NODE0000\SQL00001\USPACE. Sous AIX, Linux et Solaris, le chemin et le nom de fichier par défaut de l'espace table LDAPSPACE est *emplacement_basededonnées*/ldap32kcont_*nom_instance*/ldapspace. On Windows, le chemin et le nom de fichier par défaut de l'espace table LDAPSPACE est *emplacement_basededonnées*\ldap32kcont_*nom_instance*\ldapspace.

   - Vous souhaitez que la base de données utilise le stockage de données SMS (System Managed Storage) pour les espaces table DB2. Lorsque le type SMS est utilisé, le gestionnaire de système de fichiers du système d'exploitation alloue et gère l'espace dans lequel les tables DB2 sont stockées.
   - Vous souhaitez que la base de données utilise le stockage de données DMS (Database Managed Storage) pour les espaces table DB2. Vous voulez également configurer les espaces table USERSPACE1 et LDAPSPACE de la base de données, leur taille et leur emplacement. Lorsque le type DMS est utilisé, les espaces table sont gérés par le gestionnaire de la base de données. L'administrateur de base de données détermine les unités et les fichiers à utiliser. DB2 gère l'espace situé sur ces unités et dans ces fichiers.

e. Cliquez sur **Suivant**.

20. Dans le panneau **Options de base de données**, effectuez les opérations ci-après.
    a. Dans la zone **Emplacement d'installation de la base de données**, entrez le chemin du répertoire de la base de données. Vous pouvez cliquer sur **Parcourir** pour localiser le répertoire. Sous Windows, cet emplacement est une unité de disque, par exemple `C:`. Sous AIX, Linux et Solaris, il doit s'agir d'un nom de répertoire, par exemple `/home/ldapdb`.

       Remarque : L'espace disque minimal requis pour une base de données DMS est 1 Go. Une base de données SMS nécessite 150 Mo d'espace disque au minimum. Ces exigences s'appliquent à une base de données vide. Lorsque vous stockez des données dans la base de données, vous avez besoin d'un espace disque supplémentaire.
    b. Pour configurer la sauvegarde en ligne d'un serveur d'annuaire associé à une base de données, effectuez les opérations ci-après.
       1) Sélectionnez **Configuration pour la sauvegarde en ligne**.
       2) Dans la zone **Emplacement de sauvegarde de base de données**, indiquez l'emplacement dans lequel vous voulez stocker l'image de sauvegarde. Vous pouvez cliquer sur **Parcourir** pour rechercher cet emplacement.

       Remarque : Ne quittez pas l'outil d'administration d'instance tant que l'opération de sauvegarde est en cours.
       Lorsque vous configurez la sauvegarde en ligne de la base de données après avoir configuré la base de données elle-même, une sauvegarde initiale hors ligne est effectuée. Après la sauvegarde hors ligne, le serveur d'administration est redémarré. Vous pouvez également configurer la sauvegarde en ligne d'une instance de serveur d'annuaire à l'aide de la commande **idscfgdb**. Cependant, la configuration de la sauvegarde en ligne ne peut pas être annulée avec la commande **idscfgdb** et le paramètre **-c**. Si vous configurez la sauvegarde en ligne d'une instance à l'aide de l'outil d'administration d'instance ou de l'outil de configuration, vous pouvez annuler la configuration avec l'outil de configuration ou la commande **idscfgdb**.
    c. Dans la zone **Option de jeu de caractères**, choisissez l'une des options suivantes pour créer un type de base de données :

       Remarque : Créez une base de données DB2 universelle si vous envisagez de stocker des données dans plusieurs langues dans le serveur d'annuaire. Une base de données DB2 Universal très efficace aussi parce qu'elle nécessite moins de traduction de données. Si vous souhaitez utiliser des balises de langue, la base de donnée doit être une base de données UTF-8. Pour plus d'informations sur le format UTF-8, consultez l'«Prise en charge d'UTF-8», à la page 130.
       - Pour créer une base de données au format UTF-8 (UCS Transformation Format) dans laquelle les clients LDAP peuvent stocker des données UTF-8, cliquez sur **Créer une base de données DB2 universelle**.
       - Pour créer une base de données dans la page de code locale, cliquez sur **Créer une base de données DB2 dans la page de codes locale**.
    d. Cliquez sur **Suivant**.
21. Si vous sélectionnez **Affichage des options d'espace table avancées** dans le panneau **Configurer la base de données**, vous devez entrer les valeurs ci-après dans le panneau **Configuration des espaces table de base de données**.

a. Dans la liste **Sélectionnez le type d'espace table de base de données**, sélectionnez un type de base de données. DMS est le type d'espace table par défaut. Si vous sélectionnez le type d'espace table SMS, toutes les autres zones sont désactivées. Le support d'espace table DMS est applicable uniquement pour les espaces table USERSPACE1 et LDAPSPACE. Tous les autres espaces table, tels que les espaces table de catalogue et temporaires, sont de type SMS.

a. Sous la zone **Détails de l'espace table USERSPACE1**, entrez les détails suivants :

1) Dans la liste **Conteneur d'espace table**, sélectionnez le type de conteneur. Si l'emplacement de l'espace table USERSPACE1 doit être dans le système de fichiers, sélectionnez **Fichier**. Si le conteneur d'espace table de la base de données se trouve dans un système de fichiers, un espace table préparé DMS est créé. Vous pouvez définir la taille initiale de l'espace table, ainsi qu'une taille d'unité personnalisable pour l'extension automatique de cet espace table lorsqu'elle est nécessaire. Si vous voulez créer l'espace table USERSPACE1 sur une unité brute, sélectionnez **Disque dur**. Ce disque dur est de type "unité brute", c'est-à-dire une unité sur laquelle aucun système de fichiers n'est installé. Si le conteneur d'espace table de base de données se trouve sur une unité brute, un espace table brut DMS est créé. Dans ce cas, la taille du conteneur d'espace table de la base de données est fixe et non extensible. Si vous sélectionnez **Disque dur**, indiquez la taille et l'emplacement du conteneur, plutôt que d'accepter les valeurs par défaut.

2) Si vous avez sélectionné **Fichier** dans la liste **Conteneur d'espace table**, entrez les détails suivants :

a) Dans la zone **Chemin de répertoire**, entrez le chemin du répertoire dans lequel vous voulez créer l'espace table USERSPACE1. Vous pouvez cliquer sur **Parcourir** pour sélectionner le répertoire.

b) Dans la zone **Nom de fichier**, entrez le nom du fichier de l'espace table que vous voulez créer, ou acceptez le nom de fichier par défaut, USPACE.

c) Dans la zone **Taille initiale**, entrez la taille initiale de l'espace table USERSPACE1, en pages, ou acceptez la valeur par défaut. Pour le type de conteneur d'espace table **Fichier**, le conteneur USERSPACE1 est à incrémentation automatique. Vous pouvez entrer sa taille initiale dans la zone **Taille initiale**, et une taille d'unité personnalisable dans la zone **Taille personnalisable**. La taille initiale par défaut est 16 K pages, et la taille d'unité personnalisable par défaut est 8 K pages. La taille de page du conteneur d'espace table USERSPACE1 est égale à 4 ko par page.

3) Si vous avez sélectionné **Disque dur** dans la liste **Conteneur d'espace table**, entrez les détails suivants :

a) Dans la zone **Chemin d'unité**, entrez l'emplacement de l'unité brute. Sous Windows, le chemin doit commencer par \\.\. Voici un exemple qui montre le chemin et le nom de l'unité : \\.*nom_unité*. Sous AIX, Linux et Solaris, le chemin de l'unité doit être un chemin valide.

b) Dans la zone **Taille initiale**, entrez la taille initiale de l'espace table USERSPACE1, ou acceptez la valeur par défaut. Pour le type de conteneur d'espace table **Disque dur**, la taille du conteneur USERSPACE1 est fixe. Sa taille par défaut est 16 K pages. Pour de meilleurs résultats, entrez une taille de votre choix.

b. Sous la zone **Détails de l'espace table LDAPSPACE**, entrez les détails suivants :
   1) Dans la liste **Conteneur d'espace table**, sélectionnez le type de conteneur. Si l'emplacement de l'espace table LDAPSPACE doit être dans le système de fichiers, sélectionnez **Fichier**. Si vous voulez créer l'espace table LDAPSPACE sur une unité brute, sélectionnez **Disque dur**. Ce disque dur est de type "unité brute", c'est-à-dire une unité sur laquelle aucun système de fichiers n'est installé.
   2) Si vous avez sélectionné **Fichier** dans la liste **Conteneur d'espace table**, entrez les détails suivants :
      a) Dans la zone **Chemin de répertoire**, entrez le chemin du répertoire dans lequel vous voulez créer l'espace table LDAPSPACE. Vous pouvez cliquer sur **Parcourir** pour sélectionner le répertoire.
      b) Dans la zone **Nom de fichier**, entrez le nom du fichier de l'espace table que vous voulez créer, ou acceptez le nom de fichier par défaut, `ldapspace`.
      c) Dans la zone **Taille initiale**, entrez la taille initiale de l'espace table LDAPSPACE, en pages, ou acceptez la valeur par défaut. Pour le type de conteneur d'espace table **Fichier**, le conteneur LDAPSPACE est à incrémentation automatique. Vous pouvez entrer sa taille initiale dans la zone **Taille initiale**, et une taille d'unité personnalisable dans la zone **Taille personnalisable**. La taille initiale par défaut est 16 K pages, et la taille d'unité personnalisable par défaut est 8 K pages. La taille de page du conteneur d'espace table LDAPSPACE est égale à 32 ko par page.
   3) Si vous avez sélectionné **Disque dur** dans la liste **Conteneur d'espace table**, entrez les détails suivants :
      a) Dans la zone **Chemin d'unité**, entrez l'emplacement de l'unité brute. Sous Windows, le chemin doit commencer par `\\.\`. Voici un exemple qui montre le chemin et le nom de l'unité : `\\.\`*`nom_unité`*. Sous AIX, Linux et Solaris, le chemin de l'unité doit être un chemin valide.
      b) Dans la zone **Taille initiale**, entrez la taille initiale de l'espace table LDAPSPACE, ou acceptez la valeur par défaut. Pour le type de conteneur d'espace table **Disque dur**, la taille du conteneur LDAPSPACE est fixe. Sa taille par défaut est 16 K pages. Pour de meilleurs résultats, entrez une taille de votre choix.

c. Si vous avez sélectionné **Fichier** dans au moins une des deux zones **Conteneur d'espace table**, dans la zone **Taille personnalisable**, indiquez le nombre de pages à utiliser pour l'extension des conteneurs d'espace table.

d. Cliquez sur **Suivant**.

22. Dans le panneau **Vérifier les paramètres**, vérifiez le récapitulatif qui est généré.
23. Pour lancer la création de l'instance de serveur d'annuaire, cliquez sur **Terminer**.
24. Dans la fenêtre **Résultats**, vérifiez les messages d'erreur qui ont été générés par les opérations de création de l'instance.
25. Pour fermer la fenêtre **Résultats**, cliquez sur **Fermer**.
26. Pour fermer l'outil d'administration d'instance, cliquez sur **Fermer**.

Résultats

L'outil d'administration d'instance crée une instance de serveur d'annuaire sur l'ordinateur.

Que faire ensuite

Vous devez démarrer le processus `ibmslapd` et le serveur d'administration associé à l'instance de serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration», à la page 162.

Création d'une instance de serveur proxy avec des paramètres personnalisés

Utilisation du serveur d'administration d'instance pour créer une instance de serveur proxy avec des valeurs personnalisées conformes à vos besoins.

Avant de commencer

Pour créer une instance de serveur proxy, vous devez effectuer les tâches ci-après.

1. Installez IBM Security Directory Server avec la fonction serveur proxy. Voir «Installation à l'aide d'IBM Installation Manager», à la page 31.

Procédure

1. Démarrez l'outil d'administration d'instance. Voir «Démarrage de l'outil d'administration d'instance», à la page 135.
2. Cliquez sur **Créer une instance**.
3. Dans le panneau **Création ou migration** de la fenêtre **Créer une instance de serveur d'annuaire**, procédez de la façon suivante pour créer une instance de serveur proxy.
   a. Cliquez sur **Créer une instance de serveur d'annuaire**.
   b. Cliquez sur **Configurer en tant que proxy**.
4. Cliquez sur **Suivant**.
5. Dans le panneau **Détails de l'instance** de la fenêtre **Créer une instance de serveur d'annuaire**, entrez les valeurs ci-après.
   a. Dans la liste **Nom d'utilisateur**, sélectionnez le nom de l'utilisateur qui est propriétaire de l'instance. L'instance prend le même nom que l'utilisateur.
   b. Si vous voulez associer un nouveau compte d'utilisateur à l'instance, cliquez sur **Créer un utilisateur**. Dans la fenêtre **Créer un utilisateur pour l'instance de serveur d'annuaire**, procédez de la manière suivante :
      1) Dans la zone **Nom d'utilisateur**, entrez le nom de l'utilisateur.
      2) Dans la zone **Mot de passe**, entrez le mot de passe associé au compte utilisateur.
      3) Dans la zone **Confirmation du mot de passe**, entrez le mot de passe du compte utilisateur.
      4) Dans la zone **Répertoire de base**, entrez le répertoire de base à configurer pour le compte utilisateur. Vous pouvez cliquer sur **Parcourir** pour localiser le répertoire de base.
      5) Dans la zone **Groupe primaire**, entrez le nom du groupe primaire de l'utilisateur.
      6) Pour créer le compte utilisateur, cliquez sur **Créer**.

c. Pour modifier un compte utilisateur existant, sélectionnez le nom d'utilisateur dans la liste **Nom d'utilisateur** et cliquez sur **Modifier un utilisateur**. Dans la fenêtre **Editer l'utilisateur de l'instance de serveur d'annuaire**, procédez de la manière suivante :
   1) Le nom d'utilisateur figure dans la zone **Nom d'utilisateur**.
   2) Dans la zone **Mot de passe**, entrez le mot de passe associé au compte utilisateur.
   3) Dans la zone **Confirmation du mot de passe**, entrez le mot de passe du compte utilisateur.
   4) Dans la zone **Répertoire de base**, entrez le répertoire de base à configurer pour le compte utilisateur. Vous pouvez cliquer sur **Parcourir** pour localiser le répertoire de base.
   5) Dans la zone **Groupe primaire**, entrez le nom du groupe primaire de l'utilisateur.
   6) Pour éditer le compte utilisateur, cliquez sur **Modifier**.
   7) Dans la fenêtre de confirmation **Editer l'utilisateur de l'instance de serveur d'annuaire**, cliquez sur **Oui**.

6. Dans la zone **Emplacement de l'instance**, entrez l'emplacement de l'instance de serveur proxy. Vous pouvez cliquer sur **Parcourir** pour localiser le répertoire de base de l'instance. L'emplacement doit contenir au moins 30 Mo d'espace disponible. Sous Windows, cet emplacement est une unité de disque, par exemple `C:`. Les fichiers de l'instance d'annuaire sont stockés dans le répertoire `\idsslapd-`*`nom_instance`* sur l'unité de disque de votre choix. La variable *nom_instance* est le nom de l'instance de serveur proxy. Sur les systèmes AIX, Linux et Solaris, le répertoire de base du propriétaire de l'instance de serveur proxy est l'emplacement par défaut de l'instance, mais vous pouvez définir un autre chemin.
7. Dans la zone **Chaîne de valeur de départ de chiffrement**, entrez la valeur de départ de chiffrement de l'instance.

   A faire : Vous devez noter la valeur de départ de chiffrement de l'instance, car vous pouvez en avoir besoin pour d'autres tâches de configuration.
   La valeur de départ du chiffrement ne doit contenir que des caractères `ISO-8859-1 ASCII` imprimables dont la valeur est comprise entre 33 et 126. Elle doit comporter entre 12 et 1016 caractères. Pour des informations sur les caractères à utiliser, voir «Caractères ASCII de 33 à 126», à la page 134. Le serveur d'annuaire utilise la valeur de départ de chiffrement pour générer des valeurs de clés secrètes AES (Advanced Encryption Standard). Les fichiers de dissimulation de clés d'une instance de serveur d'annuaire stocke les valeurs des clés et sont utilisés pour chiffrer et déchiffrer le mot de passe et les attributs.
8. Dans la zone **Confirmer le chiffrement initial**, entrez la valeur de départ de chiffrement de l'instance.
9. Si vous souhaitez indiquer une chaîne de sel de chiffrement, cliquez sur **Utiliser la valeur de sel de chiffrement**.
   a. Dans la zone **Chaîne de sel de chiffrement**, entrez la valeur de sel de chiffrement de l'instance. Le sel de chiffrement ne doit contenir que des caractères `ISO-8859-1 ASCII` imprimables dont la valeur est comprise entre 33 et 126. Le sel de chiffrement doit contenir 12 caractères. Pour des informations sur les caractères à utiliser, voir «Caractères ASCII de 33 à 126», à la page 134.
   b. Dans la zone **Confirmer le sel de chiffrement**, entrez la valeur de sel de chiffrement de l'instance.

10. Facultatif : Dans la zone **Description de l'instance**, entrez la description de l'instance. La description permet d'identifier l'instance plus facilement.
11. Cliquez sur **Suivant**.
12. Dans le panneau **Paramètres TCP/IP pour les hôtes multiréseau**, sélectionnez l'une des options ci-après.
    - Si vous souhaitez que l'instance écoute sur toutes les adresses IP, sélectionnez **Intercepter toutes les adresses IP configurées**.
    - Si vous souhaitez que l'instance écoute sur un ensemble spécifique d'adresses IP configurées sur l'ordinateur, effectuez les opérations ci-après.
      a. Désélectionnez **Ecouter toutes les adresses IP configurées**.
      b. Dans la liste **Sélectionner les adresses IP spécifiques à écouter**, sélectionnez les adresses qui doivent être écoutées par l'instance.
13. Cliquez sur **Suivant**.
14. Dans le panneau **Paramètres de port TCP/IP**, entrez les valeurs ci-après.

    Remarque : Vous devez affecter des numéros de port uniques aux ports de serveur d'annuaire, car ils ne doivent pas entrer en conflit avec des ports déjà utilisés sur l'ordinateur. Sur les systèmes AIX, Linux et Solaris, les numéros de port de 1 à 1000 ne peuvent être utilisés que par l'utilisateur root.
    a. Dans la zone **Port du serveur**, entrez le numéro du port destiné à être le port non sécurisé du serveur. Vous pouvez entrer un nombre entre 1 et 65535.
    b. Dans la zone **Port sécurisé du serveur**, entrez le numéro du port destiné à être le port sécurisé du serveur. Vous pouvez entrer un nombre entre 1 et 65535.
    c. Dans la zone **Port du serveur d'administration**, entrez le numéro du port destiné à être le port non sécurisé du serveur d'administration. Vous pouvez entrer un nombre entre 1 et 65535.
    d. Dans la zone **Port sécurisé du serveur d'administration**, entrez le numéro du port destiné à être le port sécurisé du serveur d'administration. Vous pouvez entrer un nombre entre 1 et 65535.
    e. Cliquez sur **Suivant**.
15. Dans le panneau **Etapes facultatives**, effectuez les opérations ci-après.
    a. Pour configurer le nom distinctif et le mot de passe de l'administrateur de l'instance, sélectionnez **Configurer le DN et le mot de passe de l'administrateur**. Vous devez définir le nom distinctif et le mot de passe de l'administrateur de l'instance de serveur proxy.
    b. Cliquez sur **Suivant**.
16. Dans le panneau **Configurer le DN et le mot de passe de l'administrateur**, effectuez les opérations ci-après.
    a. Dans la zone **DN de l'administrateur**, entrez un nom distinctif valide ou acceptez le nom distinctif par défaut, `cn=root`. Le nom distinctif de l'administrateur n'est pas sensible à la casse. Le nom distinctif de l'administrateur a accès à toutes les données de l'instance.
    b. Dans la zone **Mot de passe de l'administrateur**, entrez le mot de passe associé au nom distinctif de l'administrateur. Les mots de passe sont sensibles à la casse. Les caractères DBCS ne sont pas valides dans le mot de passe.
    c. Dans la zone **Confirmation du mot de passe**, entrez le mot de passe du nom distinctif de l'administrateur. Vous devez noter le mot de passe, car vous pourrez en avoir besoin ultérieurement.

d. Cliquez sur **Suivant**.

17. Dans le panneau **Vérifier les paramètres**, vérifiez le récapitulatif qui est généré.
18. Pour lancer la création de l'instance de serveur proxy, cliquez sur **Terminer**.
19. Dans la fenêtre **Résultats**, vérifiez les messages d'erreur qui ont été générés par les opérations de création de l'instance.
20. Pour fermer la fenêtre **Résultats**, cliquez sur **Fermer**.
21. Pour fermer l'outil d'administration d'instance, cliquez sur **Fermer**.

Résultats

L'outil d'administration d'instance crée une instance de serveur proxy sur l'ordinateur.

Que faire ensuite

Vous devez démarrer le serveur d'administration et le processus `ibmslapd` en mode configuration uniquement et configurer les serveurs dorsaux. Consultez la section *Administration* de la documentation IBM Security Directory Server.

Création d'une instance à l'aide de l'utilitaire de ligne de commande

Utilisez l'utilitaire de ligne de commande, **`idsicrt`**, pour créer une instance.

Avant de commencer

Pour créer une instance avec l'utilitaire de ligne de commande, vous devez vérifier que les conditions ci-après sont remplies.

1. Installez IBM Security Directory Server avec le serveur, le serveur proxy, ou les deux. Voir «Installation à l'aide d'IBM Installation Manager», à la page 31.
2. Un ID utilisateur système propriétaire de l'instance doit exister. Pour plus d'informations sur la création d'un ID utilisateur système, voir «Utilisateurs et groupes associés à une instance de serveur d'annuaire», à la page 125.

Pourquoi et quand exécuter cette tâche

Lorsqu'elle est exécutée, la commande **`idsicrt`** crée une instance et une instance de base de données DB2 pour l'instance de serveur d'annuaire complet.

Procédure

1. Connectez-vous en tant qu'utilisateur root sous AIX, Linux ou Solaris, et en tant que membre du groupe des administrateurs sous Windows.
2. Le répertoire de travail en cours doit être le sous-répertoire `sbin` du répertoire d'installation d'IBM Security Directory Server.
3. Pour créer une instance, entrez la commande ci-après. Remplacez la variable *nom_instance* par un ID utilisateur système valide.

Tâche à effectuer	Commande à exécuter :
Créer une instance de serveur d'annuaire	`idsicrt -I nom_instance -e mysecretkey! -l rép_instance`
Créer une instance de serveur proxy	`idsicrt -I nom_instance -e mysecretkey! -l rép_base_instance -x`

Pour plus d'informations sur la commande **idsicrt**, consultez le manuel *Command Reference*.

Exemples

Exemple 1 :

Pour créer une instance de serveur d'annuaire avec les valeurs suivantes sous AIX, Linux ou Solaris, lancez la commande ci-après.

- Nom de l'instance : `myinst`
- Port non sécurisé : `389`
- Port sécurisé : `636`
- Valeur de départ de chiffrement : `mysecretkey!`
- Sel de chiffrement : `mysecretsalt`
- Répertoire de base de l'instance : `/home/myinst` sous AIX et Linux, et `/export/home/myinst` sous Solaris

```
idsicrt -I myinst -p 389 -s 636 -e mysecretkey!\
-g mysecretsalt -l /home/myinst
```

Pour créer une instance de serveur d'annuaire avec les valeurs suivantes sous Windows, lancez la commande ci-après.

- Nom de l'instance : `myinst`
- Port non sécurisé : `389`
- Port sécurisé : `636`
- Valeur de départ de chiffrement : `mysecretkey!`
- Sel de chiffrement : `mysecretsalt`
- Répertoire de base de l'instance : `C:`

```
idsicrt -I myinst -p 389 -s 636 -e mysecretkey!
-g mysecretsalt -l C:
```

Exemple 2 :

Pour créer une instance de serveur proxy avec les valeurs suivantes sous AIX, Linux ou Solaris, lancez la commande ci-après.

- Nom de l'instance : `myproxy`
- Port non sécurisé : `389`
- Port sécurisé : `636`
- Valeur de départ de chiffrement : `mysecretkey!`
- Sel de chiffrement : `mysecretsalt`
- Répertoire de base de l'instance : `/home/myproxy` sous AIX et Linux, et `/export/home/myproxy` sous Solaris

```
idsicrt -I myproxy -p 389 -s 636 -e mysecretkey!\
-g mysecretsalt -l /home/myproxy -x
```

Pour créer une instance de serveur proxy avec les valeurs suivantes sous Windows, lancez la commande ci-après.

- Nom de l'instance : `myproxy`
- Port non sécurisé : `389`
- Port sécurisé : `636`
- Valeur de départ de chiffrement : `mysecretkey!`
- Sel de chiffrement : `mysecretsalt`
- Répertoire de base de l'instance : `C:`

```
idsicrt -I myproxy -p 389 -s 636 -e mysecretkey!
-g mysecretsalt -l C: -x
```

Que faire ensuite

Effectuez les opérations de configuration suivantes pour créer une instance fonctionnelle :

1. Configurez une instance de base de données DB2 pour une instance de serveur d'annuaire complet.
2. Configurez le nom distinctif et le mot de passe de l'administrateur de l'instance.
3. Configurez les suffixes de l'instance.

Mise à niveau d'une instance d'une version précédente à l'aide de l'outil d'administration d'instance

Utilisez l'outil d'administration d'instance pour mettre à niveau vers la version 6.3.1 une instance de serveur d'annuaire ou de serveur proxy d'une version précédente.

Avant de commencer

Vous devez effectuer les tâches suivantes avant de mettre à niveau une instance à l'aide de l'outil d'administration d'instance :

- Installez IBM Security Directory Server version 6.3.1. Voir «Démarrage de l'installation», à la page 28.
- Avant de mettre à niveau une instance, configurez l'environnement. Voir «Configuration de l'environnement avant la mise à niveau d'une instance», à la page 92.
- Connectez-vous en tant qu'utilisateur root sur les systèmes d'exploitation AIX, Linux ou Solaris, et en tant que membre du groupe des administrateurs sur le système d'exploitation Windows.

Pourquoi et quand exécuter cette tâche

Une instance mise à niveau à partir d'une version précédente devient une instance parfaitement fonctionnelle d'IBM Security Directory Server version 6.3.1.

Procédure

1. Accédez à l'invite de commande.
2. Accédez au répertoire `sbin`. Voici le répertoire d'installation par défaut sur différents systèmes d'exploitation :

   Microsoft Windows
   `C:\Program Files\IBM\ldap\V6.3.1\sbin`

   AIX et Solaris
   `/opt/IBM/ldap/V6.3.1/sbin`

   Linux `/opt/ibm/ldap/V6.3.1/sbin`
3. Pour utiliser l'outil d'administration d'instance, lancez la commande ci-après.

   Remarque : Sous Windows, vous pouvez le lancer à partir du menu **Démarrer**. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Security Directory Server 6.3.1** > **Outil d'administration d'instance**.

   ```
   idsxinst
   ```
4. Sélectionnez l'instance à la version précédente que vous voulez migrer.

5. Cliquez sur **Migrer**.
6. Dans la fenêtre **Migrer une instance de serveur d'annuaire**, cliquez sur **Migrer**.
7. A l'invite de l'outil d'administration d'instance qui suit la mise à niveau, cliquez sur **OK**.
8. Vérifiez les informations récapitulatives.
9. Pour fermer la fenêtre **Migrer une instance de serveur d'annuaire**, cliquez sur **Fermer**.
10. Effectuez une sauvegarde hors ligne de l'instance. Pour plus d'informations, voir «Sauvegarde du serveur d'annuaire», à la page 194.
11. Pour fermer l'outil d'administration d'instance, cliquez sur **Fermer**.

Résultats

L'outil d'administration d'instance a mis à niveau une version précédente d'une instance de serveur d'annuaire vers la version 6.3.1.

Que faire ensuite

Vous devez démarrer le processus `ibmslapd` et le serveur d'administration associé à l'instance de serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration», à la page 162.

Mise à niveau d'une instance distante d'une version précédente à l'aide de l'outil d'administration d'instance

Utilisez l'outil d'administration d'instance pour mettre à niveau vers la version 6.3.1 une instance distante de serveur d'annuaire ou de serveur proxy d'une version précédente.

Avant de commencer

Vous devez effectuer les tâches suivantes avant de mettre à niveau une instance à l'aide de l'outil d'administration d'instance :

- Avant de mettre à niveau une instance, configurez l'environnement. Voir «Configuration de l'environnement avant la mise à niveau d'une instance», à la page 92.
- Connectez-vous en tant qu'utilisateur root sur les systèmes d'exploitation AIX, Linux ou Solaris, et en tant que membre du groupe des administrateurs sur le système d'exploitation Windows.

Pourquoi et quand exécuter cette tâche

Lorsque le processus de mise à niveau est terminé, l'outil d'administration d'instance crée sur le poste une instance à la version 6.3.1 en utilisant les informations de l'instance distante.

Procédure

1. A l'aide de la commande **idsdb2ldif**, sauvegardez la base de données de l'instance de serveur d'annuaire qui se trouve sur l'ordinateur distant.

   Important : Si vous mettez à niveau une instance de serveur proxy, ne sauvegardez pas la base de données. Aucune base de données n'est associée à un serveur proxy.

```
idsdb2ldif -I nom_instance -o sortie_instance.ldif
```

Pour plus d'informations sur la commande **idsdb2ldif**, consultez le manuel *Command Reference*.

2. Installez IBM Security Directory Server version 6.3.1 sur l'ordinateur sur lequel vous voulez mettre à jour l'instance distante. Voir «Démarrage de l'installation», à la page 28.
3. Pour sauvegarder les fichiers de schéma et de configuration de l'instance distante, exécutez la commande **migbkup** de la version 6.3.1 cible de la mise à niveau :

Système d'exploitation	Commande à exécuter :
Microsoft Windows	**migbkup.bat** unité\idsslapd-nom_instance rép_sauvegarde
AIX, Linux et Solaris	**migbkup** rép_base_utilisateur/idsslapd-nom_instance rép_sauvegarde

La commande **migbkup** est dans le sous-répertoire tools du support d'installation d'IBM Security Directory Server.

4. Copiez le répertoire de sauvegarde, rép_sauvegarde, que vous avez créé avec **migbkup**, de l'ordinateur distant vers l'ordinateur sur lequel IBM Security Directory Server version 6.3.1 est installé.
5. Facultatif : Copiez le fichier de sauvegarde de la base de données, sortie_instance.ldif, de l'ordinateur distant vers l'ordinateur sur lequel IBM Security Directory Server version 6.3.1 est installé.
6. Démarrez l'outil d'administration d'instance. Voir «Démarrage de l'outil d'administration d'instance», à la page 135.
7. Cliquez sur **Créer une instance**.
8. Sur le panneau **Création ou migration**, effectuez les opérations ci-après.
   a. Cliquez sur **Migrer à partir d'une version antérieure du serveur d'annuaire**.
   b. Dans la zone **Entrer le chemin des fichiers sauvegardés**, entrez le chemin dans lequel vous avez copié la sauvegarde des fichiers de configuration et de schéma de l'instance distante. Vous pouvez cliquer sur **Parcourir** pour rechercher l'emplacement de la sauvegarde.
   c. Cliquez sur **Suivant**.
9. Dans le panneau **Détails de l'instance** de la fenêtre **Créer une instance de serveur d'annuaire**, entrez les valeurs ci-après.

   Remarque : Si vous mettez à niveau une instance, vous ne pouvez pas modifier les informations existantes sur les utilisateurs.

   a. Dans la liste **Nom d'utilisateur**, sélectionnez le nom de l'utilisateur qui doit être propriétaire de l'instance du serveur d'annuaire. L'instance de serveur d'annuaire prend le même nom que l'utilisateur.
   b. Si vous voulez associer un nouveau compte d'utilisateur à l'instance, cliquez sur **Créer un utilisateur**. Dans la fenêtre **Créer un utilisateur pour l'instance de serveur d'annuaire**, procédez de la manière suivante :
      1) Dans la zone **Nom d'utilisateur**, entrez le nom de l'utilisateur.
      2) Dans la zone **Mot de passe**, entrez le mot de passe associé au compte utilisateur.
      3) Dans la zone **Confirmation du mot de passe**, entrez le mot de passe du compte utilisateur.

4) Dans la zone **Répertoire de base**, entrez le répertoire de base à configurer pour le compte utilisateur. Vous pouvez cliquer sur **Parcourir** pour localiser le répertoire de base.
5) Dans la zone **Groupe primaire**, entrez le nom du groupe primaire de l'utilisateur.
6) Pour créer le compte utilisateur, cliquez sur **Créer**.

10. Dans la zone **Emplacement de l'instance**, entrez l'emplacement de l'instance de serveur d'annuaire. Vous pouvez cliquer sur **Parcourir** pour localiser le répertoire de base de l'instance. L'emplacement doit contenir au moins 30 Mo d'espace disponible. Sous Windows, cet emplacement est une unité de disque, par exemple `C:`. Les fichiers de l'instance d'annuaire sont stockés dans le répertoire `\idsslapd-`*`nom_instance`* sur l'unité de disque de votre choix. La variable *nom_instance* est le nom de l'instance de serveur d'annuaire. Sur les systèmes AIX, Linux et Solaris, le répertoire de base du propriétaire de l'instance de serveur d'annuaire est l'instance par défaut, mais vous pouvez définir un autre chemin.
11. Facultatif : Dans la zone **Description de l'instance**, entrez la description de l'instance de serveur d'annuaire. La description permet d'identifier l'instance plus facilement.
12. Cliquez sur **Suivant**.
13. Si vous mettez à niveau les détails de la base de données DB2 dans une instance de serveur d'annuaire, cliquez sur **Suivant** dans le panneau **Détails de l'instance DB2**. Si les fichiers de sauvegarde sont ceux d'une instance de serveur proxy distante, le panneau **Détails de l'instance DB2** ne s'affiche pas forcément.
14. Dans le panneau **Paramètres TCP/IP pour les hôtes multiréseau**, sélectionnez l'une des options ci-après.
    - Si vous souhaitez que l'instance de serveur d'annuaires écoute sur toutes les adresses IP, sélectionnez **Intercepter toutes les adresses IP configurées**.
    - Si vous souhaitez que l'instance de serveur d'annuaire écoute sur un ensemble spécifique d'adresses IP configurées sur l'ordinateur, désélectionnez l'option **Intercepter toutes les adresses IP configurées**. Sélectionnez dans la liste les adresses IP sur lesquelles vous souhaitez que l'instance de serveur d'annuaires écoute.
15. Cliquez sur **Suivant**.
16. Dans le panneau **Paramètres de port TCP/IP**, entrez les valeurs ci-après.

    Remarque : Vous devez affecter des numéros de port uniques aux ports de serveur d'annuaire, car ils ne doivent pas entrer en conflit avec des ports déjà utilisés sur l'ordinateur. Sur les systèmes AIX, Linux et Solaris, les numéros de port de 1 à 1000 ne peuvent être utilisés que par l'utilisateur root.
    a. Dans la zone **Port du serveur**, entrez le numéro du port destiné à être le port non sécurisé du serveur. Vous pouvez entrer un nombre entre 1 et 65535.
    b. Dans la zone **Port sécurisé du serveur**, entrez le numéro du port destiné à être le port sécurisé du serveur. Vous pouvez entrer un nombre entre 1 et 65535.
    c. Dans la zone **Port du serveur d'administration**, entrez le numéro du port destiné à être le port non sécurisé du serveur d'administration. Vous pouvez entrer un nombre entre 1 et 65535.

d. Dans la zone **Port sécurisé du serveur d'administration**, entrez le numéro du port destiné à être le port sécurisé du serveur d'administration. Vous pouvez entrer un nombre entre 1 et 65535.
e. Cliquez sur **Suivant**.

17. Dans le panneau **Vérifier les paramètres**, vérifiez le récapitulatif qui est généré.
18. Pour lancer la création de l'instance de serveur d'annuaire avec les fichiers de configuration et de schéma sauvegardez, cliquez sur **Terminer**.
19. Dans la fenêtre **Résultats**, vérifiez les messages d'erreur qui ont été générés par les opérations de création de l'instance.
20. Pour fermer la fenêtre **Résultats**, cliquez sur **Fermer**.
21. Pour fermer l'outil d'administration d'instance, cliquez sur **Fermer**.

Résultats

L'outil d'administration d'instance crée une instance de serveur d'annuaire sur l'ordinateur.

Que faire ensuite

Vous devez démarrer le processus `ibmslapd` et le serveur d'administration associé à l'instance de serveur d'annuaire. Voir «Démarrage ou arrêt d'un serveur d'annuaire et d'un serveur d'administration», à la page 163.

Sauvegardez l'instance. Pour obtenir des informations sur la sauvegarde d'une instance de serveur d'annuaire, voir «Sauvegarde du serveur d'annuaire», à la page 194.

Création d'une instance à partir d'une instance existante

L'outil d'administration d'instance vous permet de créer une instance de serveur d'annuaire à partir d'une instance existante située sur un ordinateur local ou un distant. Le serveur d'annuaire source sert de modèle pour l'instance de serveur d'annuaire cible.

L'outil d'administration d'instance d'IBM Security Directory Server ne prend en charge la copie d'une instance de serveur d'annuaire source que si l'outil et l'instance sont à la même version. Le serveur d'annuaire cible est créé sur l'ordinateur sur lequel l'outil d'administration d'instance est exécuté. Si le serveur d'annuaire source se trouve sur un autre ordinateur, il n'est pas nécessaire que les systèmes d'exploitation des deux ordinateurs soient identiques. Par exemple, vous pouvez créer sur un système Windows une instance de serveur d'annuaire qui est la copie d'une instance sur un système Linux.

Lorsque vous utilisez l'outil pour copier une instance source, les opérations suivantes peuvent être réalisées :

- Vous pouvez créer un serveur d'annuaire cible avec les mêmes paramètres de configuration et fichiers de schéma que l'instance de serveur d'annuaire source. L'outil synchronise également les fichiers de dissimulation de l'annuaire du serveur cible avec ceux du serveur source.
- Si l'instance de serveur d'annuaire source est un serveur d'annuaire complet, l'instance de serveur d'annuaire cible qui est créée est aussi un serveur d'annuaire complet. Vous pouvez choisir de copier les données de l'instance de serveur d'annuaire existante. Si le serveur d'annuaire source est configuré pour

la sauvegarde en ligne, vous pouvez créer un serveur d'annuaire cible fonctionnel avec des entrées dans sa base de données.

- Si l'instance de serveur d'annuaire source est un serveur proxy, l'instance de serveur d'annuaire cible qui est créée est aussi un serveur proxy.
- Si le serveur d'annuaire source est un environnement de réplication, vous pouvez configurer l'instance cible en tant que serveur réplique ou serveur homologue du serveur source.
- Si le serveur d'annuaire source est un environnement distribué, vous pouvez configurer l'instance de serveur d'annuaire cible en tant que serveur proxy.
- Si l'instance du serveur d'annuaire source est configurée pour des communications sécurisées, l'outil d'administration d'instance copie les fichiers de la base de données de clés sur le serveur d'annuaire cible.

Vous devez vérifier que le serveur d'annuaire source remplit les conditions ci-après avant de l'utiliser pour créer un autre serveur d'annuaire.

- Le serveur d'annuaire source IBM Security Directory Server doit être à la version 6.3.1. L'instance du serveur d'annuaire source ne doit pas être à une version antérieure.
- Le serveur d'annuaire source doit fonctionner en mode normal. La copie d'une instance qui fonctionne en mode de configuration n'est pas prise en charge.
- Le serveur d'annuaire source doit être accessible à partir de l'ordinateur sur lequel vous exécutez l'outil d'administration d'instance.
- Vous ne pouvez créer le serveur d'annuaire cible en tant que réplique ou paire que si l'instance du serveur d'annuaire source contient un contexte de réplication. Vous ne pouvez pas utiliser l'outil d'administration d'instance pour configurer le premier serveur réplique ou homologue d'une topologie de réplication. L'instance de serveur d'annuaire source doit contenir au moins un contexte de réplication, un groupe de réplication et une sous-entrée de réplication définis. Si vous voulez configurer l'instance en tant que réplique, l'instance source doit contenir la topologie de réplication initiale, et notamment un accord vers au moins un autre serveur. Si vous voulez configurer l'instance en tant qu'homologue, définissez le serveur source en tant que serveur maître pour une ou plusieurs des sous-entrées de la configuration de réplication.
- Si vous voulez créer l'instance en tant qu'homologue ou que réplique, une nouvelle sous-entrée est créée sous le nom distinctif `ibm-replicaGroup=default,`*`contexteRéplication`*. Si vous omettez d'indiquer le nom distinctif, l'instance ne peut pas être copiée.

Si vous voulez copier les données de l'instance de serveur d'annuaire source à l'instance de serveur d'annuaire cible, les conditions ci-après doivent être remplies.

- La version de DB2 peut être différente dans les deux instances de serveur d'annuaire. Une base de données sauvegardée sur un système d'exploitation peut être restaurée sur tout poste fonctionnant avec le même type de système d'exploitation. Par exemple, vous pouvez restaurer, sur un système doté de DB2 version 10, une base de données créée sur DB2 UDB version 9 sur un système Windows. Sur les systèmes AIX, Linux et Solaris, vous pouvez restaurer, sur DB2 version 10, des sauvegardes générées sur DB2 UDB version 9 si le type endian (big endian ou little endian) des systèmes d'exploitation de sauvegarde et de restauration est identique.
- Vous devez configurer l'instance de serveur d'annuaire source pour une sauvegarde en ligne. Vous pouvez configurer la sauvegarde en ligne au cours de

la configuration initiale de la base de données. L'outil d'administration d'instance ou l'outil de configuration peuvent être utilisés pour configurer la sauvegarde en ligne.

- Vous devez effectuer une sauvegarde hors connexion initiale de l'instance de serveur d'annuaire source avant d'utiliser l'outil d'administration d'instance pour copier l'instance de serveur d'annuaire. Le chemin que vous indiquez pour la sauvegarde ne doit contenir qu'une seule image de sauvegarde.
- Le chemin de l'image de sauvegarde doit être accessible aussi bien par l'instance de serveur d'annuaire source que par l'instance de serveur d'annuaire cible.

Création d'une copie d'une instance existante à l'aide de l'outil d'administration d'instance

L'outil d'administration d'instance vous permet de créer une copie d'une instance existante.

Avant de commencer

Avant de copier une instance existante, vous devez vérifier que les conditions ci-après sont remplies.

- Démarrez le processus `ibmslapd` et le serveur d'administration de l'instance en mode normal.
- Vérifiez que le serveur d'annuaire source est accessible à partir de l'outil d'administration d'instance.

Procédure

1. Démarrez l'outil d'administration d'instance. Voir «Démarrage de l'outil d'administration d'instance», à la page 135.
2. Choisissez l'une des options suivantes pour créer une copie d'une instance existante :
   - Pour créer une copie d'une instance existante qui se trouve sur un ordinateur local, cliquez sur **Copier l'instance locale**.
   - Pour créer une copie d'une instance existante qui se trouve sur un ordinateur distant, cliquez sur **Copier l'instance distante**.
3. Dans le panneau **Copier l'instance de serveur d'annuaire**, entrez les valeurs ci-après.
   a. Dans la zone **Hôte**, entrez l'adresse IP ou le nom d'hôte si le serveur d'annuaire source est sur un ordinateur distant. Si le serveur d'annuaire source se trouve sur un ordinateur local, la zone contient `localhost` et cette valeur n'est pas modifiable.
   b. Dans la zone **Port**, entrez le numéro de port du serveur d'annuaire si celui qui y figure n'est pas valide. Si vous voulez utiliser une connexion sécurisée, vous devez entrer le numéro de port sécurisé de l'instance de serveur d'annuaire source.
   c. Dans la zone **DN de l'administrateur**, indiquez le nom distinctif de l'administrateur du serveur d'annuaire source si l'instance est sur un ordinateur distant. Si le serveur d'annuaire source se trouve sur un ordinateur local, la zone contient le nom distinctif de l'administrateur et cette valeur n'est pas modifiable.
   d. Dans la zone **Mot de passe**, entrez le mot de passe associé au nom distinctif de l'administrateur.
   e. Dans la zone **Valeur de départ de chiffrement**, entrez la valeur de départ de chiffrement de l'instance de serveur d'annuaire source.

f. Si les communications sécurisées sont configurées sur le serveur d'annuaire source, et si vous voulez les configurer sur le serveur d'annuaire cible, cliquez sur **Utiliser la connexion SSL**.
   1) Dans la zone **Fichier de clés**, entrez le nom et le chemin du fichier de la base de données de clés. Vous pouvez cliquer sur **Parcourir** pour rechercher cet emplacement.
   2) Dans la zone **Nom de clé**, entrez le nom de la clé privée à utiliser. La clé doit figurer dans le fichier de clés du serveur d'annuaire source.
   3) Dans la zone **Mot de passe de clé**, entrez le mot de passe de la base de données de clés du fichier de clés.

g. Cliquez sur **Suivant**.

4. Dans le panneau **Configuration de l'instance - étape 1**, effectuez les opérations ci-après.
   a. Vérifiez les informations relatives au serveur d'annuaire source dans les zones **URL source** et **Type d'instance source**. Le **Type d'instance source** peut être une instance de serveur d'annuaire complet ou de serveur proxy.
   b. Pour configurer le serveur d'annuaire cible en tant qu'homologue ou réplique dans une topologie de réplication existante, sélectionnez **Configurer en tant que serveur homologue ou réplique** et sélectionnez l'une des options ci-après.
      - Pour configurer le serveur d'annuaire cible en tant que réplique, cliquez sur **Réplique**.
      - Pour configurer le serveur d'annuaire cible en tant qu'homologue, cliquez sur **Homologue**.

   c. Dans la zone **Nom d'utilisateur**, entrez l'ID utilisateur système qui doit être propriétaire de l'instance de serveur d'annuaire cible. Il ne doit pas comporter plus de 8 caractères. Le même nom est également défini comme nom de l'instance du serveur d'annuaire, ID de l'administrateur DB2, le nom de l'instance de base de données et le nom de la base de données. L'ID utilisateur doit exister sur l'ordinateur et ne doit pas être associé à une autre instance de serveur d'annuaire de l'ordinateur. Pour plus d'informations sur cet ID utilisateur, voir «Utilisateurs et groupes associés à une instance de serveur d'annuaire», à la page 125.
   d. Dans la zone **Mot de passe**, entrez le mot de passe associé à l'ID utilisateur.
   e. Dans la zone **Emplacement de l'instance**, entrez l'emplacement de l'instance de serveur d'annuaire. Vous pouvez cliquer sur **Parcourir** pour localiser le répertoire de base de l'instance. L'emplacement doit contenir au moins 30 Mo d'espace disponible. Sous Windows, cet emplacement est une unité de disque, par exemple `C:`. Les fichiers de l'instance d'annuaire sont stockés dans le répertoire `\idsslapd-`*`nom_instance`* sur l'unité de disque de votre choix. La variable *nom_instance* est le nom de l'instance de serveur d'annuaire. Sur les systèmes AIX, Linux et Solaris, le répertoire de base du propriétaire de l'instance de serveur d'annuaire est l'instance par défaut, mais vous pouvez définir un autre chemin.
   f. Cliquez sur **Suivant**.

5. Dans le panneau **Configuration de l'instance - étape 2**, effectuez les opérations ci-après.
   a. Dans la zone **DN de l'administrateur**, entrez un nom distinctif valide pour l'instance de serveur d'annuaire cible. Le nom distinctif de l'administrateur n'est pas sensible à la casse. Le nom distinctif de l'administrateur a accès à toutes les données de l'instance de serveur d'annuaire.

b. Dans la zone **Mot de passe**, entrez le mot de passe associé au nom distinctif de l'administrateur. Les mots de passe sont sensibles à la casse. Les caractères DBCS ne sont pas valides dans le mot de passe.
c. Dans la zone **Confirmation du mot de passe**, entrez le mot de passe du nom distinctif de l'administrateur. Vous devez noter le mot de passe, car vous pourrez en avoir besoin ultérieurement.
d. Pour copier les données de la base de données du serveur source sur le serveur cible, sélectionnez **Copier les données de l'instance source vers la nouvelle instance** et effectuez les opérations ci-après.

   Remarque : Si vous avez choisi de créer le serveur d'annuaire cible en tant qu'homologue ou réplique, cette case est sélectionnée et vous ne pouvez pas la désélectionner.

   1) Dans la zone **Chemin des images de sauvegarde**, entrez le chemin de l'image de sauvegarde du serveur source. Vous pouvez cliquer sur **Parcourir** pour rechercher cet emplacement. Si l'instance source est sur un ordinateur distant, le chemin de sauvegarde doit être un chemin partagé, et doit être accessible des ordinateurs source et cible. Un exemple de chemin partagé est un système de fichier NFS en lecture/écriture.

e. Cliquez sur **Suivant**.

6. Dans le panneau **Vérifier les paramètres**, vérifiez le récapitulatif qui est généré.
7. Pour démarrer la création de la copie des serveurs d'annuaire source, cliquez sur **Terminer**.
8. Dans la fenêtre **Résultats**, vérifiez les messages d'erreur qui ont été générés par les opérations de création de l'instance.
9. Pour fermer la fenêtre **Résultats**, cliquez sur **Fermer**.
10. Pour fermer l'outil d'administration d'instance, cliquez sur **Fermer**.

Résultats

L'outil d'administration d'instance crée une copie de l'instance de serveur d'annuaire source sur l'ordinateur.

Que faire ensuite

Vous devez démarrer le processus `ibmslapd` et le serveur d'administration associé à l'instance de serveur d'annuaire. Voir «Démarrage ou arrêt d'un serveur d'annuaire et d'un serveur d'administration», à la page 163.

Sauvegardez l'instance. Pour obtenir des informations sur la sauvegarde d'une instance de serveur d'annuaire, voir «Sauvegarde du serveur d'annuaire», à la page 194.

Création d'une copie d'une instance existante à l'aide de l'utilitaire de ligne de commande

Utilisez l'utilitaire de ligne de commande **`idsideploy`** pour créer une copie d'instance.

Avant de commencer

Avant de copier une instance existante, vous devez vérifier que les conditions ci-après sont remplies.

- Démarrez le processus `ibmslapd` et le serveur d'administration de l'instance source en mode normal. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide des utilitaires de ligne de commande», à la page 163.
- Vérifiez que le serveur source est accessible à partir de l'ordinateur sur lequel vous voulez créer la copie d'instance.

Procédure

1. Connectez-vous en tant qu'utilisateur root sous AIX, Linux ou Solaris, et en tant que membre du groupe des administrateurs sous Windows.
2. Le répertoire de travail en cours doit être le sous-répertoire `sbin` du répertoire d'installation d'IBM Security Directory Server.
3. Pour créer une copie d'instance sans les données de l'instance de serveur d'annuaire existante, lancez la commande ci-après.

   ```
   idsideploy -sU ldap://hôte:port -sD DN_admin_src -sw mdp_admin_src
   -e départ_chiffrement -I nom_instance -a mdp_instance -D DN_admin
   -w mdp_admin -l emplacement_instance
   ```

   Pour plus d'informations sur la commande **idsideploy**, consultez le manuel *Command Reference*.

Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration

Pour utiliser une instance de serveur d'annuaire, vous devez démarrer le processus `ibmslapd` et le serveur d'administration associé à l'instance.

Si vous modifiez la configuration d'un serveur d'annuaire, vous devrez peut-être arrêter et redémarrer le serveur et le serveur d'administration pour appliquer les modifications. Vous ne pouvez redémarrer le serveur d'annuaire et le serveur d'administration que s'ils fonctionnent en mode normal ou en mode de configuration.

Pour démarrer ou arrêter les serveurs, vous pouvez utiliser le serveur d'administration d'instance ou les utilitaires serveurs, par exemple **ibmslapd** et **ibmdiradm**. Le processus `ibmslapd` est associé au serveur d'annuaire. Avec l'outil d'administration d'instance, vous ne pouvez démarrer l'instance de serveur d'annuaire qu'en mode normal. Pour démarrer le serveur d'annuaire en mode configuration uniquement, utilisez les options de la ligne de commande.

Un serveur d'annuaire peut être dans l'un des états suivants :

- Démarré
- Arrêté
- Démarré (Configuration uniquement)

Un serveur d'administration peut être dans l'un des états suivants :

- Démarré
- Arrêté

Démarrage ou arrêt d'un serveur d'annuaire et d'un serveur d'administration

Vous pouvez utiliser l'Outil d'administration d'instance pour démarrer ou arrêter le serveur d'annuaire et/ou le serveur d'administration associés à une instance.

Avant de commencer

Avant de démarrer ou d'arrêter le serveur d'annuaire et le serveur d'administration d'une instance, vous devez vérifier que les conditions ci-après sont remplies.

1. Une instance à la même version que l'outil d'administration d'instance doit exister.
2. Si l'instance n'existe pas, créez-la. Voir «Création de l'instance de serveur d'annuaire par défaut», à la page 138 ou «Création d'une instance de serveur d'annuaire avec des paramètres personnalisés», à la page 140.

Procédure

1. Démarrez l'outil d'administration d'instance. Voir «Démarrage de l'outil d'administration d'instance», à la page 135.
2. Dans la **Liste des instances de serveur d'annuaire installées sur l'ordinateur**, sélectionnez une instance dont la version est la même que celle de l'outil d'administration d'instance.
3. Pour démarrer ou arrêter le serveur d'annuaire et/ou le serveur d'administration, cliquez sur **Démarrer/Arrêter**.
4. Dans la fenêtre **Gérer l'état du serveur**, procédez comme suit.
   - Pour démarrer le serveur d'annuaire et/ou le serveur d'administration associés à une instance, procédez de la manière suivante :
     - Pour démarrer le serveur d'annuaire, cliquez sur **Démarrer le serveur**.
     - Pour démarrer le serveur d'administration, cliquez sur **Démarrer le serveur d'administration**.
     - Cliquez sur **OK**.
   - Pour arrêter le serveur d'annuaire et/ou le serveur d'administration, procédez de la manière suivante :
     - Pour arrêter le serveur d'annuaire, cliquez sur **Arrêter le serveur**.
     - Pour arrêter le serveur d'administration, cliquez sur **Arrêter le serveur d'administration**.
     - Cliquez sur **OK**.
5. Pour fermer la fenêtre **Gérer l'état du serveur**, cliquez sur **Fermer**.
6. Pour fermer l'outil d'administration d'instance, cliquez sur **Fermer**.

Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide des utilitaires de ligne de commande

Vous pouvez utiliser les utilitaires de ligne de commande pour démarrer ou arrêter le serveur d'annuaire et/ou le serveur d'administration associés à une instance.

Avant de commencer

Avant de démarrer ou d'arrêter le serveur d'annuaire et le serveur d'administration d'une instance, vous devez vérifier que les conditions ci-après sont remplies.

- Une instance à la même version que les utilitaires de ligne de commande doit exister. Si l'instance n'existe pas, créez-la. Voir «Création de l'instance de serveur

d'annuaire par défaut», à la page 138 ou «Création d'une instance de serveur d'annuaire avec des paramètres personnalisés», à la page 140.

Procédure

1. Connectez-vous à l'ordinateur avec les droits requis. Voir Chapitre 20, «Configuration d'instance», à la page 173.
2. Accédez à l'invite de commande.
3. Le répertoire de travail en cours doit être le sous-répertoire `sbin` du répertoire d'installation d'IBM Security Directory Server.
4. Pour démarrer le serveur d'annuaire et le serveur d'administration de l'instance *nom_instance*, exécutez les commandes suivantes : Remplacez la variable `nom_instance` par le nom de l'instance.

   ```
   ibmslapd -I nom_instance
   ibmdiradm -I nom_instance
   ```

5. Pour arrêter le serveur d'annuaire et le serveur d'administration d'une instance, exécutez les commandes suivantes : Remplacez la variable `nom_instance` par le nom de l'instance.

   ```
   ibmslapd -I nom_instance -k
   ibmdiradm -I nom_instance -k
   ```

Gestion de la configuration d'une instance de serveur d'annuaire

Vous pouvez utiliser l'outil de configuration pour vérifier le statut de la configuration d'une instance de serveur d'annuaire ou de serveur proxy, la gérer ou la modifier.

Vous pouvez utiliser l'outil de configuration pour gérer et modifier la configuration d'une instance de serveur d'annuaire ou de serveur proxy qui est à la même version. Vous ne pouvez pas utiliser l'outil de configuration qui est fourni avec une version d'IBM Security Directory Server pour gérer une instance de serveur d'annuaire ou de serveur proxy d'une version plus ancienne ou plus récente.

Vous disposez de deux possibilités pour ouvrir l'outil de configuration d'une instance :

- Utiliser l'outil d'administration d'instance.
- Exécuter la commande **idsxcfg** avec le nom de l'instance comme valeur de paramètre.

Pour plus d'informations sur l'outil de configuration, voir Chapitre 20, «Configuration d'instance», à la page 173.

Ouverture de l'outil de configuration depuis l'Outil d'administration d'instance

Ouvrez l'outil de configuration d'IBM Security Directory Server pour gérer ou modifier la configuration d'une instance de serveur d'annuaire ou une instance de serveur proxy.

Avant de commencer

Pour gérer une instance de l'outil de configuration, vous devez vérifier que les conditions ci-après sont remplies.

- Une instance de la même version que l'outil de configuration doit exister. Si l'instance n'existe pas, créez-la. Voir «Création de l'instance de serveur

d'annuaire par défaut», à la page 138 ou «Création d'une instance de serveur d'annuaire avec des paramètres personnalisés», à la page 140.

Procédure

1. Démarrez l'outil d'administration d'instance. Voir «Démarrage de l'outil d'administration d'instance», à la page 135.
2. Dans la **Liste des instances de serveur d'annuaire installées sur l'ordinateur**, sélectionnez une instance dont la version est la même que celle de l'outil d'administration d'instance.
3. Pour gérer l'instance avec l'outil de configuration, cliquez sur **Gérer**. La fenêtre de l'outil de configuration d'IBM Security Directory Server s'ouvre pour l'instance.
4. Pour fermer l'outil de configuration, cliquez sur **Fichier** > **Quitter**.
5. Dans la fenêtre de confirmation de l'outil de configuration, cliquez sur **Oui**.

Modification des paramètres TCP/IP d'une instance

Vous pouvez utiliser l'outil d'administration d'instance ou les utilitaires de ligne de commande pour modifier les paramètres TCP/IP d'une instance de serveur d'annuaire ou d'une instance de serveur proxy.

Vous ne pouvez modifier les paramètres TCP/IP d'une instance que si le version de l'instance et celle de l'outil d'administration d'instance sont les mêmes.

Modification des paramètres TCP/IP d'une instance avec l'Outil d'administration d'instance

Utilisez l'Outil d'administration d'instance pour modifier les paramètres TCP/IP d'une instance existante.

Avant de commencer

Avant de modifier les paramètres TCP/IP d'une instance à l'aide de l'outil d'administration d'instance, vous devez vérifier que les conditions ci-après sont respectées.

1. Une instance à la même version que l'outil d'administration d'instance doit exister.
2. Arrêtez le serveur d'annuaire et le serveur d'administration de l'instance. Voir «Démarrage ou arrêt d'un serveur d'annuaire et d'un serveur d'administration», à la page 163.

Procédure

1. Démarrez l'outil d'administration d'instance. Voir «Démarrage de l'outil d'administration d'instance», à la page 135.
2. Dans la **Liste des instances de serveur d'annuaire installées sur l'ordinateur**, sélectionnez une instance dont la version est la même que celle de l'outil d'administration d'instance.
3. Pour modifier les paramètres TCP/IP d'une instance existante, cliquez sur **Modifier les paramètres TCP/IP**. La fenêtre **Modifier les paramètres TCP/IP** de l'instance s'ouvre.
4. Dans la fenêtre **Modifier les paramètres TCP/IP**, sélectionnez l'une des options ci-après.

- Si vous souhaitez que l'instance écoute sur toutes les adresses IP configurées de l'ordinateur, sélectionnez **Intercepter toutes les adresses IP configurées**.
- Si vous souhaitez que l'instance écoute sur un ensemble spécifique d'adresses IP configurées sur l'ordinateur, effectuez les opérations ci-après.
  a. Désélectionnez **Ecouter toutes les adresses IP configurées**.
  b. Dans la liste **Sélectionner les adresses IP spécifiques à écouter**, sélectionnez les adresses qui doivent être écoutées par l'instance.

5. Cliquez sur **Suivant**.
6. Dans le panneau **Détails du port**, entrez les valeurs ci-après.

   Remarque : Vous devez affecter des numéros de port uniques aux ports de serveur d'annuaire, car ils ne doivent pas entrer en conflit avec des ports déjà utilisés sur l'ordinateur. Sur les systèmes AIX, Linux et Solaris, les numéros de port de 1 à 1000 ne peuvent être utilisés que par l'utilisateur root.
   a. Dans la zone **Port du serveur**, entrez le numéro du port destiné à être le port non sécurisé du serveur. Vous pouvez entrer un nombre entre 1 et 65535.
   b. Dans la zone **Port sécurisé du serveur**, entrez le numéro du port destiné à être le port sécurisé du serveur. Vous pouvez entrer un nombre entre 1 et 65535.
   c. Dans la zone **Port du serveur d'administration**, entrez le numéro du port destiné à être le port non sécurisé du serveur d'administration. Vous pouvez entrer un nombre entre 1 et 65535.
   d. Dans la zone **Port sécurisé du serveur d'administration**, entrez le numéro du port destiné à être le port sécurisé du serveur d'administration. Vous pouvez entrer un nombre entre 1 et 65535.
   e. Cliquez sur **Terminer**.
7. Dans la fenêtre **Modifier les résultats TCP/IP**, vérifiez les messages d'erreur qui ont été générés par les opérations de modification des paramètres TCP/IP.
8. Pour fermer la fenêtre **Modifier les résultats TCP/IP**, cliquez sur **Fermer**.
9. Pour fermer l'outil d'administration d'instance, cliquez sur **Fermer**.

Modification des paramètres TCP/IP d'une instance à l'aide des utilitaires de ligne de commande

Utilisez les commandes **idssethost** et **idssetport** pour modifier les paramètres TCP/IP et de port d'une instance existante.

Avant de commencer

Avant de modifier les paramètres TCP/IP d'une instance à l'aide des utilitaires de ligne de commande, vous devez vérifier que les conditions ci-après sont respectées.

1. Une instance à la même version que les utilitaires de ligne de commande doit exister.
2. Arrêtez le serveur d'annuaire et le serveur d'administration de l'instance. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide des utilitaires de ligne de commande», à la page 163.

Procédure

1. Connectez-vous en tant qu'utilisateur root sous AIX, Linux ou Solaris, et en tant que membre du groupe des administrateurs sous Windows.

2. Le répertoire de travail en cours doit être le sous-répertoire `sbin` du répertoire d'installation d'IBM Security Directory Server.
3. Pour mettre à jour les adresses IP du serveur d'annuaire *nom_instance*, choisissez l'une des options ci-après. Remplacez la variable *nom_instance* par le nom de l'instance.

Adresse IP pour la connexion	Commande à exécuter :
Une adresse spécifique, xx.xx.xx.xx, sur l'ordinateur	`idssethost -I nom_instance -i xx.xx.xx.xx`
Toutes les adresses IP configurées sur l'ordinateur	`idssethost -I nom_instance -i all`

4. Pour mettre à jour les numéros de port du serveur d'annuaire *nom_instance*, exécutez la commande ci-après. Remplacez la variable *nom_instance* par le nom de l'instance.

   Remarque : Vous devez affecter des numéros de port uniques aux ports de serveur d'annuaire, car ils ne doivent pas entrer en conflit avec des ports déjà utilisés sur l'ordinateur. Sur les systèmes AIX, Linux et Solaris, les numéros de port de 1 à 1000 ne peuvent être utilisés que par l'utilisateur root.

Port à configurer	Commande à exécuter :
Port du serveur	`idssetport -I nom_instance -p port_no`
Port sécurisé du serveur	`idssetport -I nom_instance -s port_sécurisé`
Port du serveur d'administration	`idssetport -I nom_instance -a port_adm`
Port sécurisé du serveur d'administration	`idssetport -I nom_instance -c port_sécurisé_adm`

   Pour plus d'informations sur les commandes **idssethost** et **idssetport**, voir le manuel *Command Reference*.
5. Démarrez le serveur d'annuaire et le serveur d'administration. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide des utilitaires de ligne de commande», à la page 163.

Affichage des informations relatives à une instance

Vous pouvez utiliser l'outil d'administration d'instance ou l'utilitaire de ligne de commande pour afficher les détails d'une instance, par exemple son répertoire de base, ses adresses IP et ses ports.

Vous pouvez affiche les informations de toutes les instance de l'ordinateur. Le statut de l'instance peut être Arrêté ou Démarré.

La commande **idsilist** fournit également des informations similaires pour une instances ou toutes les instances disponibles sur l'ordinateur. Pour plus d'informations sur la commande **idsilist**, consultez le manuel *Command Reference*.

Affichage des informations relatives à une instance à l'aide de l'Outil d'administration d'instance

L'Outil d'administration d'instance vous permet d'afficher les détails d'une instance existante.

Procédure

1. Démarrez l'outil d'administration d'instance. Voir «Démarrage de l'outil d'administration d'instance», à la page 135.
2. Dans la **Liste des instances de serveur d'annuaire installées sur l'ordinateur**, sélectionnez une instance dont vous souhaitez afficher les détails.
3. Cliquez sur **Afficher**. La fenêtre **Afficher les détails de l'instance** contenant les généralités et les détails TCP/IP de l'instance sélectionnée s'affiche.
4. Pour fermer la fenêtre **Afficher les détails de l'instance**, cliquez sur **Fermer**.
5. Pour fermer l'outil d'administration d'instance, cliquez sur **Fermer**.

Affichage des informations relatives à une instance à l'aide de l'utilitaire de ligne de commande

Utilisez la commande **idsilist** pour afficher des informations sur une instance existante.

Procédure

1. Connectez-vous en tant qu'utilisateur root sous AIX, Linux ou Solaris, et en tant que membre du groupe des administrateurs sous Windows.
2. Le répertoire de travail en cours doit être le sous-répertoire `sbin` du répertoire d'installation d'IBM Security Directory Server.
3. Pour afficher les informations relatives aux instances d'un ordinateur, lancez la commande **idsilist** appropriée :

Tâche à effectuer	Commande à exécuter :
Affiche la liste complète des instances	`idsilist`
Lister toutes les instances avec leurs informations complètes et leur description	`idsilist -a`
Lister toutes les instances avec leurs informations complètes au format brut	`idsilist -r`
Lister une instance spécifique	`idsilist -I` *`nom_instance`*
Lister une instance spécifique avec ses informations complètes et sa description	`idsilist -I` *`nom_instance`* `-a`
Lister une instance spécifique avec ses informations complètes au format brut	`idsilist -I` *`nom_instance`* `-r`

Pour plus d'informations sur la commande **idsilist**, consultez le manuel *Command Reference*.

Suppression d'une instance de serveur d'annuaire

Vous pouvez utiliser l'outil d'administration d'instance ou l'utilitaire de ligne de commande pour supprimer une instance de serveur d'annuaire ou une instance de serveur proxy.

Vous pouvez avoir besoin de supprimer une instance sur un poste, par exemple si vous avez migré l'instance vers un autre poste, ou si vous n'en avez plus besoin.

Si vous supprimez un serveur d'annuaire avec une base de données DB2, il est recommandé de réaliser une sauvegarde avant de supprimer l'instance. Si vous supprimez une instance de serveur proxy, il est recommandé de réaliser une sauvegarde de l'instance.

Remarque : Pour une instance de serveur proxy, la suppression de l'instance est la seule option valide.

Avec l'outil d'administration d'instance, vous disposez des possibilités suivantes :

- Supprimer l'instance de serveur d'annuaire et conserver l'instance de base de données
- Supprimer l'instance de serveur d'annuaire et supprimer l'instance de base de données DB2 associée

Avec la commande **idsidrop**, vous disposez des possibilités suivantes :

- Supprimer l'instance de serveur d'annuaire et conserver l'instance de base de données
- Supprimer l'instance de serveur d'annuaire et supprimer l'instance de base de données DB2 associée
- Annuler la configuration de l'instance du serveur d'annuaire dans l'instance de base de données DB2, et ne pas supprimer l'instance du serveur d'annuaire

Pour plus d'informations sur la commande **idsidrop**, consultez le manuel *Command Reference*.

Suppression d'une instance à l'aide de l'outil d'administration d'instance

Utilisez l'outil d'administration d'instance pour supprimer une instance de serveur d'annuaire ou une instance de serveur proxy.

Avant de commencer

Avant de modifier les paramètres TCP/IP d'une instance à l'aide de l'outil d'administration d'instance, vous devez vérifier que les conditions ci-après sont respectées.

1. Une instance à la même version que l'outil d'administration d'instance doit exister.
2. Arrêtez le serveur d'annuaire et le serveur d'administration de l'instance. Voir «Démarrage ou arrêt d'un serveur d'annuaire et d'un serveur d'administration», à la page 163.

Procédure

1. Démarrez l'outil d'administration d'instance. Voir «Démarrage de l'outil d'administration d'instance», à la page 135.
2. Dans la **Liste des instances de serveur d'annuaire installées sur l'ordinateur**, sélectionnez une instance dont la version est la même que celle de l'outil d'administration d'instance.
3. Pour lancer la suppression, cliquez sur **Supprimer**.
4. Dans la fenêtre **Supprimer l'instance de serveur d'annuaire**, procédez de la manière suivante :
   a. Sélectionnez l'une des méthodes de suppression ci-après.
      - Pour supprimer l'instance de serveur d'annuaire sans supprimer l'instance de base de données associée, cliquez sur **Supprimer l'instance de serveur d'annuaire uniquement**.

        Remarque : Pour une instance de serveur proxy, **Supprimer l'instance de serveur d'annuaire uniquement** est la seule option valide.

- Pour supprimer l'instance de serveur d'annuaire avec l'instance de base de données associée, cliquez sur **Supprimer l'instance de serveur d'annuaire et l'instance de base de données associée**.

b. Cliquez sur **Supprimer**.

c. Dans la fenêtre **Avertissement**, cliquez sur **Oui** pour confirmer la suppression de l'instance.

d. Dans la fenêtre **Information**, cliquez sur **OK**.

e. Pour fermer la fenêtre **Supprimer l'instance de serveur d'annuaire**, cliquez sur **Fermer**.

f. Pour fermer l'outil d'administration d'instance, cliquez sur **Fermer**.

Suppression d'une instance à l'aide de l'utilitaire de ligne de commande

Utilisez la commande **idsidrop** pour supprimer une instance existante.

Avant de commencer

Pour supprimer une instance avec l'utilitaire de ligne de commande, vous devez vérifier que les conditions ci-après sont remplies :

1. Une instance à la même version que l'utilitaire de ligne de commande doit exister.
2. Arrêtez le serveur d'annuaire et le serveur d'administration de l'instance. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide des utilitaires de ligne de commande», à la page 163.

Procédure

1. Connectez-vous en tant qu'utilisateur root sous AIX, Linux ou Solaris, et en tant que membre du groupe des administrateurs sous Windows.
2. Le répertoire de travail en cours doit être le sous-répertoire `sbin` du répertoire d'installation d'IBM Security Directory Server.
3. Pour supprimer l'instance *nom_instance*, choisissez l'une des options ci-après. Remplacez la variable *nom_instance* par le nom de l'instance.

Tâche à effectuer	Commande à exécuter :
Pour supprimer l'instance de serveur d'annuaire et conserver l'instance de base de données associée	`idsidrop -I nom_instance`
Pour supprimer l'instance de serveur d'annuaire et supprimer l'instance de base de données associée	`idsidrop -I nom_instance -r`
Pour annuler la configuration de l'instance de base de données associée sans supprimer l'instance de serveur d'annuaire	`idsidrop -I nom_instance -R`

Pour plus d'informations sur la commande **idsidrop**, consultez le manuel *Command Reference*.

Chapitre 19. Vérification de l'arborescence des fichiers

Après avoir installé IBM Security Directory Server, vous devez vérifier l'arborescence des fichiers.

Systèmes Windows 32 bits et 64 bits

Lorsqu'IBM Security Directory Server est installé sur le système d'exploitation Windows, les répertoires et les fichiers suivants figurent dans le répertoire d'installation, par exemple : `C:\Program Files\IBM\LDAP\V6.3.1` (le répertoire d'installation peut être modifié)

appsrv
etc
java
lib
messages
bin
examples
javalib
lib64
nls
var
codeset
idstools
jre
license
properties
config
include
ldapcfg.ico
logs
sbin

Systèmes Linux 64 bits

Lorsqu'IBM Security Directory Server est installé sur le système d'exploitation Linux, les répertoires et les fichiers suivants figurent dans le répertoire d'installation, par exemple : `/opt/ibm/ldap/V6.3.1` (le répertoire d'installation n'est pas modifiable)

bin
codeset
config
etc
examples
idstools
include
javalib
LAPID
lib
lib64
nls

properties
sbin
tmp
web

Chapitre 20. Configuration d'instance

Vous pouvez utiliser l'outil de configuration ou les utilitaires de ligne de commande pour configurer une instance de serveur d'annuaire ou une instance de serveur proxy selon vos besoins.

L'outil de configuration (**idsxcfg**) d'IBM Security Directory Server est une interface graphique que vous pouvez utiliser pour configurer une instance. IBM Java Development Kit est requis pour l'utilisation de l'outil de configuration.

Pour exécuter l'outil de configuration, connectez-vous avec les données d'identification suivantes :

AIX, Linux ou Solaris

- Utilisateur root
- Propriétaire de l'instance de serveur d'annuaire
- ID utilisateur membre du groupe primaire du propriétaire de l'instance de serveur d'annuaire

Windows

- ID utilisateur faisant partie du groupe d'administrateurs par défaut

Vous pouvez également utiliser l'outil de configuration pour modifier la configuration du serveur d'annuaire existant.

Vous pouvez utiliser l'outil de configuration pour les tâches suivantes sur une instance de serveur d'annuaire complet :

- Démarrez ou arrêter le serveur
- Gérer le nom distinctif et le mot de passe de l'administrateur principal
- Configurer une base de données DB2 pour une instance de serveur d'annuaire, et annuler sa configuration
- Optimiser la base de données associée à une instance
- Gérer une base de données DB2 avec organisation des index ou compression des lignes
- Sauvegarder et restaurer la base de données
- Optimiser les performances d'une instance de serveur d'annuaire
- Activer et désactiver le journal des modifications
- Ajouter ou supprimer des suffixes
- Ajouter ou supprimer des fichiers de schéma
- Importer ou exporter des données LDIF
- Configurer la synchronisation Active Directory

Vous pouvez utiliser l'outil de configuration pour les tâches suivantes sur une instance de serveur proxy :

- Démarrez ou arrêter le serveur
- Gérer le nom distinctif et le mot de passe de l'administrateur principal
- Ajouter ou supprimer des suffixes
- Ajouter ou supprimer des fichiers de schéma
- Sauvegarder et restaurer l'instance

Démarrage de l'outil de configuration

Démarrez l'IBM Security Directory Server outil de configuration pour l'instance, afin de configurer l'instance conformément aux exigences de votre environnement de répertoire.

Avant de commencer

Pour gérer une instance de l'outil de configuration, vous devez vérifier que les conditions ci-après sont remplies.

- Une instance de la même version que l'outil de configuration doit exister. Si l'instance n'existe pas, créez-la. Voir «Création d'une instance de serveur d'annuaire avec des paramètres personnalisés», à la page 140 ou «Création d'une instance de serveur proxy avec des paramètres personnalisés», à la page 148.
- IBM Java Development Kit doit exister dans le chemin d'installation d'IBM Security Directory Server. Pour le chemin d'installation par défaut d'IBM Security Directory Server, voir «Emplacements d'installation par défaut», à la page 27.

Procédure

1. Connectez-vous à l'ordinateur avec les droits requis. Voir Chapitre 20, «Configuration d'instance», à la page 173.
2. Ouvrez l'invite de commande.
3. A partir du répertoire de travail, accédez au sous-répertoire `sbin` dans l'emplacement d'installation d'IBM Security Directory Server.
4. Exécutez la commande **idsxcfg** avec la syntaxe ci-après. Remplacez la variable *nom_instance* par le nom de l'instance.

   ```
   idsxcfg -I nom_instance
   ```

   La fenêtre de l'outil de configuration d'IBM Security Directory Server s'ouvre pour l'instance indiquée.
5. Pour fermer la fenêtre Outil de configuration, cliquez sur **Fichier** > **Quitter**.
6. Dans la fenêtre de confirmation de l'outil de configuration, cliquez sur **Oui**.

Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide de l'outil de configuration

Vous pouvez utiliser l'outil de configuration pour démarrer le processus `ibmslapd` et le serveur d'administration associé à une instance.

Si vous modifiez la configuration d'un serveur d'annuaire, vous devrez peut-être arrêter et redémarrer le serveur et le serveur d'administration pour appliquer les modifications. Vous ne pouvez redémarrer le serveur d'annuaire et le serveur d'administration que s'ils fonctionnent en mode normal ou en mode de configuration.

Pour démarrer ou arrêter le serveur et le serveur d'administration, vous pouvez utiliser l'outil de configuration ou les utilitaires du serveur, par exemple **ibmslapd** et **ibmdiradm**. Le processus `ibmslapd` est associé au serveur d'annuaire. Avec l'outil de configuration, vous ne pouvez démarrer l'instance de serveur d'annuaire qu'en mode normal. Pour démarrer le serveur d'annuaire en mode configuration uniquement, utilisez les options de la ligne de commande.

Un serveur d'annuaire peut être dans l'un des états suivants :

- Démarré
- Arrêté
- Démarré (Configuration uniquement)

Un serveur d'administration peut être dans l'un des états suivants :

- Démarré
- Arrêté

Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide de l'outil de configuration

Vous pouvez utiliser l'outil de configuration pour démarrer ou arrêter le serveur d'annuaire et/ou le serveur d'administration associés à une instance.

Procédure

1. Démarrez l'outil de configuration pour l'instance. Voir «Démarrage de l'outil de configuration», à la page 174.
2. Dans la liste des tâches du panneau de navigation situé à gauche, cliquez sur **Gérer l'état du serveur**.
3. Dans la page **Etat en cours**, vérifiez l'état du serveur et du serveur d'administration.
4. Dans la page **Etat en cours**, effectuez les opérations ci-après.
   - Pour démarrer le serveur d'annuaire et/ou le serveur d'administration associés à une instance, procédez de la manière suivante :
     - Pour démarrer le serveur d'annuaire, cliquez sur **Démarrer le serveur**.
     - Pour démarrer le serveur d'administration, cliquez sur **Démarrer le serveur d'administration**.
     - Dans la fenêtre **Information**, cliquez sur **OK**.
   - Pour arrêter le serveur d'annuaire et/ou le serveur d'administration, procédez de la manière suivante :
     - Pour arrêter le serveur d'annuaire, cliquez sur **Arrêter le serveur**.
     - Pour arrêter le serveur d'administration, cliquez sur **Arrêter le serveur d'administration**.
     - Dans la fenêtre **Information**, cliquez sur **OK**.
5. Pour fermer la page **Etat en cours**, cliquez sur **Fermer**.
6. Pour fermer la fenêtre Outil de configuration, cliquez sur **Fichier** > **Quitter**.
7. Dans la fenêtre de confirmation de l'outil de configuration, cliquez sur **Oui**.

Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide des utilitaires de ligne de commande

Vous pouvez utiliser les utilitaires de ligne de commande pour démarrer ou arrêter le serveur d'annuaire et/ou le serveur d'administration associés à une instance.

Avant de commencer

Avant de démarrer ou d'arrêter le serveur d'annuaire et le serveur d'administration d'une instance, vous devez vérifier que les conditions ci-après sont remplies.

- Une instance à la même version que les utilitaires de ligne de commande doit exister. Si l'instance n'existe pas, créez-la. Voir «Création de l'instance de serveur

d'annuaire par défaut», à la page 138 ou «Création d'une instance de serveur d'annuaire avec des paramètres personnalisés», à la page 140.

Procédure

1. Connectez-vous à l'ordinateur avec les droits requis. Voir Chapitre 20, «Configuration d'instance», à la page 173.
2. Accédez à l'invite de commande.
3. Le répertoire de travail en cours doit être le sous-répertoire `sbin` du répertoire d'installation d'IBM Security Directory Server.
4. Pour démarrer le serveur d'annuaire et le serveur d'administration de l'instance *nom_instance*, exécutez les commandes suivantes : Remplacez la variable `nom_instance` par le nom de l'instance.

   ```
   ibmslapd -I nom_instance
   ibmdiradm -I nom_instance
   ```

5. Pour arrêter le serveur d'annuaire et le serveur d'administration d'une instance, exécutez les commandes suivantes : Remplacez la variable `nom_instance` par le nom de l'instance.

   ```
   ibmslapd -I nom_instance -k
   ibmdiradm -I nom_instance -k
   ```

Gestion du nom distinctif de l'administrateur principal d'une instance

Pour accéder à la configuration et à toutes les données d'annuaire d'une instance, vous devez créer et configurer un nom distinctif pour l'administrateur principal de l'instance.

Le nom distinctif de l'administrateur correspond au nom distinctif utilisé par l'administrateur principal de l'instance. Vous ne pouvez créer qu'un seul administrateur principal par instance.

Le nom distinctif par défaut est `cn=root`. Le nom distinctif n'est pas sensible à la casse.

Un nom distinctif est constitué de paires `attribut:valeur` séparées par des virgules. Voici un exemple de nom distinctif.

```
cn=Ben Gray,ou=dept_audit,o=sample
```

Vous pouvez utiliser l'outil de configuration ou l'utilitaire de ligne de commande **idsdnpw** pour définir ou modifier le nom distinctif de l'administrateur principal. Pour définir ou modifier le nom distinctif de l'administrateur, vous devez arrêter le processus `ibmslapd` associé à l'instance.

Gestion du nom distinctif de l'administrateur principal à l'aide de l'outil de configuration

Utilisez l'outil de configuration pour configurer le nom distinctif de l'administrateur principal d'une instance.

Avant de commencer

Pour configurer le nom distinctif de l'administrateur principal d'une instance, vous devez effectuer les tâches ci-après.

- Arrêtez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide de l'outil de configuration», à la page 175.

Procédure

1. Démarrez l'outil de configuration pour l'instance. Voir «Démarrage de l'outil de configuration», à la page 174.
2. Dans la liste des tâches du panneau de navigation situé à gauche, cliquez sur **Gérer le nom distinctif de l'administrateur**. .
3. Dans la zone **DN de l'administrateur**, entrez un nom distinctif valide pour l'administrateur principal ou acceptez le nom distinctif par défaut, `cn=root`.
4. Cliquez sur **OK**.
5. Pour confirmer l'action, cliquez sur **OK**.
6. Pour fermer la fenêtre Outil de configuration, cliquez sur **Fichier** > **Quitter**.
7. Pour confirmer, cliquez sur **Oui**.

Que faire ensuite

Démarrez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide de l'outil de configuration», à la page 175.

Gestion du nom distinctif de l'administrateur principal à l'aide de l'utilitaire de ligne de commande

Utilisez l'utilitaire de ligne de commande, **idsdnpw**, pour gérer le nom distinctif de l'administrateur principal d'une instance.

Avant de commencer

Pour configurer le nom distinctif de l'administrateur principal d'une instance, vous devez effectuer les tâches ci-après.

- Arrêtez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide des utilitaires de ligne de commande», à la page 163.

Pourquoi et quand exécuter cette tâche

Si vous ne définissez pas la valeur du nom distinctif de l'administrateur, la valeur par défaut, `cn=root`, est définie dans le fichier `ibmslapd.conf` de l'instance du serveur d'annuaire. Vous devez définir le mot de passe de l'administrateur principal de l'instance.

Si vous ne définissez pas le mot de passe, il vous est réclamé par la commande **idsdnpw**. Lorsque vous le saisissez, le mot de passe ne s'affiche pas dans l'invite.

Procédure

1. Connectez-vous en tant que propriétaire de l'instance de serveur d'annuaire.
2. Accédez à l'invite de commande.
3. Le répertoire de travail en cours doit être le sous-répertoire `sbin` du répertoire d'installation d'IBM Security Directory Server.
4. Pour définir le nom distinctif de l'administrateur d'une instance, exécutez la commande ci-après. Remplacez `nom_instance`, `DN_admin` et `mdp_admin` par vos valeurs.

```
idsdnpw -I nom_instance -u DN_admin -p mdp_admin
```

Pour plus d'informations sur la commande **idsdnpw**, consultez le manuel *Command Reference*.

Que faire ensuite

Démarrez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide des utilitaires de ligne de commande», à la page 163.

Gestion du mot de passe de l'administrateur principal d'une instance

Pour vous authentifier auprès d'une instance et accéder à la configuration et à toutes les données d'annuaire, vous devez créer et configurer le mot de passe de l'administrateur principal de l'instance.

Le mot de passe de l'administrateur est sensible à la casse. Vous ne devez pas utiliser les caractères DBCS dans les mots de passe car ils ne sont pas pris en charge. Vous devez enregistrer le mot de passe de l'administrateur, pour ne pas l'oublier.

Vous pouvez utiliser l'outil de configuration ou l'utilitaire de ligne de commande **idsdnpw** pour configurer le mot de passe de l'administrateur principal. Pour configurer le mot de passe de l'administrateur, vous devez arrêter le processus `ibmslapd` associé à l'instance.

Si les règles d'administration des mots de passe administrateur sont activées, le mot de passe de l'administrateur principal doit s'y conformer. Pour plus d'informations au sujet des règles sur les mots de passe, voir la section *Administration* de la documentation IBM Security Directory Server.

Gestion du mot de passe de l'administrateur principal à l'aide de l'outil de configuration

Utilisez l'outil de configuration pour configurer le mot de passe de l'administrateur principal d'une instance.

Avant de commencer

Pour configurer le mot de passe du nom distinctif de l'administrateur principal d'une instance, vous devez effectuer les tâches ci-après.

- Arrêtez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide de l'outil de configuration», à la page 175.

Procédure

1. Démarrez l'outil de configuration pour l'instance. Voir «Démarrage de l'outil de configuration», à la page 174.
2. Dans la liste des tâches du panneau de navigation situé à gauche, cliquez sur **Gérer le mot de passe de l'administrateur**.
3. Dans la zone **Mot de passe de l'administrateur**, entrez le mot de passe de l'administrateur principal.
4. Dans la zone **Confirmation du mot de passe**, entrez le mot de passe de l'administrateur principal.

5. Cliquez sur **OK**.
6. Pour confirmer l'action, cliquez sur **OK**.
7. Pour fermer la page **Gérer le mot de passe de l'administrateur**, cliquez sur **OK**.
8. Pour fermer la fenêtre Outil de configuration, cliquez sur **Fichier** > **Quitter**.
9. Pour confirmer, cliquez sur **Oui**.

Que faire ensuite

Démarrez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide de l'outil de configuration», à la page 175.

Gestion du mot de passe de l'administrateur principal à l'aide de l'utilitaire de ligne de commande

Utilisez l'utilitaire de ligne de commande, **idsdnpw**, pour gérer le mot de passe de l'administrateur principal d'une instance.

Avant de commencer

Pour configurer le mot de passe de l'administrateur principal d'une instance, vous devez effectuer les tâches ci-après.

- Arrêtez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide des utilitaires de ligne de commande», à la page 163.

Procédure

1. Connectez-vous en tant que propriétaire de l'instance de serveur d'annuaire.
2. Accédez à l'invite de commande.
3. Le répertoire de travail en cours doit être le sous-répertoire `sbin` du répertoire d'installation d'IBM Security Directory Server.
4. Pour définir le mot de passe de l'administrateur d'une instance, exécutez la commande ci-après. Remplacez `nom_instance`, `DN_admin` et `mdp_admin` par vos valeurs.

   ```
   idsdnpw -I nom_instance -u DN_admin -p mdp_admin
   ```

   Pour plus d'informations sur la commande **idsdnpw**, consultez le manuel *Command Reference*.

Que faire ensuite

Démarrez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide des utilitaires de ligne de commande», à la page 163.

Configuration de la base de données d'une instance de serveur d'annuaire

Pour utiliser une instance comme serveur d'annuaire et y stocker des données, vous devez configurer une base de données DB2 pour l'instance.

Vous pouvez utiliser l'outil d'administration d'instance, l'outil de configuration ou la commande **idscfgdb** pour créer et configurer une base de données DB2. Vous

devez arrêter le serveur d'annuaire avant de configurer la base de données ou d'annuler sa configuration. Pour plus d'informations sur la commande **idscfgdb**, consultez le manuel *Command Reference*.

Si vous choisissez de créer l'instance par défaut à l'aide de l'outil d'administration d'instance, l'instance de base de données DB2 est aussi créée et configurée pour elle. Dans le cas d'une instance de serveur proxy, il est inutile de configurer une base de données DB2.

Lorsque vous configurez une base de données DB2 pour une instance, les informations relatives à la base de données sont enregistrées dans le fichier de configuration de l'instance. L'outil crée également les paramètres de base de données et de bouclage local .

Les paramètres de base de données et de bouclage local sont créés, s'ils n'existent pas déjà. Vous pouvez spécifier la création de la base de données en tant que base de données de page de codes locale, ou en tant que base de données UTF-8. La page de code par défaut pour la création des bases de données DB2 est UTF-8.

Configuration d'une base de données d'instance à l'aide de l'outil de configuration

Utilisez l'outil de configuration pour configurer une base de données DB2 destinée à une instance de serveur d'annuaire.

Avant de commencer

Avant de configurer une base de données DB2 pour une instance de serveur d'annuaire, vous devez effectuer les tâches ci-après.

- Arrêtez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide de l'outil de configuration», à la page 175.
- Un ID utilisateur système susceptible d'être le propriétaire de l'instance de base de données DB2 doit exister. Pour plus d'informations sur les conditions associées aux ID utilisateur système, voir «Utilisateurs et groupes associés à une instance de serveur d'annuaire», à la page 125.

Procédure

1. Démarrez l'outil de configuration pour l'instance. Voir «Démarrage de l'outil de configuration», à la page 174.
2. Dans la liste des tâches du panneau de navigation situé à gauche, cliquez sur **Tâches de base de données** > **Configurer la base de données**.
3. sur la page **Configurer la base de données**, sélectionnez l'une des options ci-après.
   - Pour configurer une base de données pour une instance, effectuez les opérations ci-après.
     a. Dans la zone **Nom utilisateur de base de données**, entrez l'ID utilisateur système qui doit être propriétaire de la base de données. L'instance de serveur d'annuaire utilise cet ID utilisateur système pour la connexion à la base de données.
     b. Dans la zone **Mot de passe**, entrez le mot de passe de l'administrateur de la base de données.
     c. Dans la zone **Nom de base de données**, entrez le nom de la base de données.

d. Si vous voulez définir les paramètres de configuration suivants, sélectionnez **Affichage des options d'espace table avancées**.
   - Vous souhaitez que la base de données utilise le stockage de données SMS (System Managed Storage) pour les espaces table DB2. Lorsque le type SMS est utilisé, le gestionnaire de système de fichiers du système d'exploitation alloue et gère l'espace dans lequel les tables DB2 sont stockées.
   - Vous souhaitez que la base de données utilise le stockage de données DMS (Database Managed Storage) pour les espaces table DB2. Vous voulez également configurer les espaces table `USERSPACE1` et `LDAPSPACE` de la base de données, leur taille et leur emplacement. Lorsque le type DMS est utilisé, les espaces table sont gérés par le gestionnaire de la base de données. L'administrateur de base de données détermine les unités et les fichiers à utiliser. DB2 gère l'espace situé sur ces unités et dans ces fichiers.

   Si vous ne sélectionnez pas **Affichage des options d'espace table avancées**, une base de données DB2 avec les espaces table `USERSPACE1` et `LDAPSPACE` est créée à l'aide de DMS avec les tailles et les emplacements par défaut. Si vous configurez une instance avec une base de données existante, l'option **Affichage des options d'espace table avancées** est désactivée lorsque vous entrez le nom de la base de données existante dans la zone **Nom de base de données**.

e. Cliquez sur **Suivant**.

- Pour configurer à nouveau le mot de passe de l'administrateur de la base de données, effectuez les opérations ci-après.
  a. Cliquez sur **Redéfinir le mot de passe**.
  b. Dans la zone **Mot de passe**, entrez le mot de passe de l'administrateur de la base de données.
  c. Dans la zone **Confirmation du mot de passe**, entrez le mot de passe de l'administrateur de la base de données.
  d. Cliquez sur **Suivant**.

4. Si vous créez et configurez une base de données DB2, procédez de la façon suivante :
   a. Dans la zone **Emplacement d'installation de la base de données**, entrez le chemin du répertoire de la base de données. Vous pouvez cliquer sur **Parcourir** pour localiser le répertoire. Sous Windows, cet emplacement est une unité de disque, par exemple `C:`. Sous AIX, Linux et Solaris, il doit s'agir d'un nom de répertoire, par exemple `/home/ldapdb`.

      Remarque : L'espace disque minimal requis pour une base de données DMS est 1 Go. Une base de données SMS nécessite 150 Mo d'espace disque au minimum. Ces exigences s'appliquent à une base de données vide. Lorsque vous stockez des données dans la base de données, vous avez besoin d'un espace disque supplémentaire.

   b. Pour configurer la sauvegarde en ligne d'un serveur d'annuaire associé à une base de données, effectuez les opérations ci-après.
      1) Sélectionnez **Configuration pour la sauvegarde en ligne**.
      2) Dans la zone **Emplacement de sauvegarde de base de données**, indiquez l'emplacement dans lequel vous voulez stocker l'image de sauvegarde. Vous pouvez cliquer sur **Parcourir** pour rechercher cet emplacement.

Remarque : Ne quittez pas l'outil de configuration et n'annulez pas l'opération de sauvegarde tant qu'elles est en cours.
Lorsque vous configurez la sauvegarde en ligne de la base de données après avoir configuré la base de données elle-même, une sauvegarde initiale hors ligne est effectuée. Après la sauvegarde hors ligne, le serveur d'administration est redémarré. Vous pouvez également configurer la sauvegarde en ligne d'une instance de serveur d'annuaire à l'aide de la commande **idscfgdb**. Cependant, la configuration de la sauvegarde en ligne ne peut pas être annulée avec la commande **idscfgdb** et le paramètre **-c**. Si vous configurez la sauvegarde en ligne d'une instance à l'aide de l'outil d'administration d'instance ou de l'outil de configuration, vous pouvez annuler la configuration avec l'outil de configuration ou la commande **idscfgdb**.

c. Dans la zone **Option de jeu de caractères**, choisissez l'une des options suivantes pour créer un type de base de données :

Remarque : Créez une base de données DB2 universelle si vous envisagez de stocker des données dans plusieurs langues dans le serveur d'annuaire. Une base de données DB2 Universal très efficace aussi parce qu'elle nécessite moins de traduction de données. Si vous souhaitez utiliser des balises de langue, la base de donnée doit être une base de données UTF-8. Pour plus d'informations sur le format UTF-8, consultez l'«Prise en charge d'UTF-8», à la page 130.

- Pour créer une base de données au format UTF-8 (UCS Transformation Format) dans laquelle les clients LDAP peuvent stocker des données UTF-8, cliquez sur **Créer une base de données DB2 universelle**.
- Pour créer une base de données dans la page de code locale, cliquez sur **Créer une base de données DB2 dans la page de codes locale**.

d. Cliquez sur **Suivant**.

5. Si vous avez sélectionné **Affichage des options d'espace table avancées**, vous devez effectuer les opérations ci-après.
   a. Dans la liste **Sélectionnez le type d'espace table de base de données**, sélectionnez un type de base de données. DMS est le type d'espace table par défaut. Si vous sélectionnez le type d'espace table SMS, toutes les autres zones sont désactivées. Le support d'espace table DMS est applicable uniquement pour les espaces table USERSPACE1 et LDAPSPACE. Tous les autres espaces table, tels que les espaces table de catalogue et temporaires, sont de type SMS.
   a. Sous la zone **Détails de l'espace table USERSPACE1**, entrez les détails suivants :
      1) Dans la liste **Conteneur d'espace table**, sélectionnez le type de conteneur. Si l'emplacement de l'espace table USERSPACE1 doit être dans le système de fichiers, sélectionnez **Fichier**. Si le conteneur d'espace table de la base de données se trouve dans un système de fichiers, un espace table préparé DMS est créé. Vous pouvez définir la taille initiale de l'espace table, ainsi qu'une taille d'unité personnalisable pour l'extension automatique de cet espace table lorsqu'elle est nécessaire. Si vous voulez créer l'espace table USERSPACE1 sur une unité brute, sélectionnez **Disque dur**. Ce disque dur est de type "unité brute", c'est-à-dire une unité sur laquelle aucun système de fichiers n'est installé. Si le conteneur d'espace table de base de données se trouve sur une unité brute, un espace table brut DMS est créé. Dans ce cas, la taille du conteneur d'espace table de la base de données est fixe et non

extensible. Si vous sélectionnez **Disque dur**, indiquez la taille et l'emplacement du conteneur, plutôt que d'accepter les valeurs par défaut.

2) Si vous avez sélectionné **Fichier** dans la liste **Conteneur d'espace table**, entrez les détails suivants :
   a) Dans la zone **Chemin de répertoire**, entrez le chemin du répertoire dans lequel vous voulez créer l'espace table USERSPACE1. Vous pouvez cliquer sur **Parcourir** pour sélectionner le répertoire.
   b) Dans la zone **Nom de fichier**, entrez le nom du fichier de l'espace table que vous voulez créer, ou acceptez le nom de fichier par défaut, USPACE.
   c) Dans la zone **Taille initiale**, entrez la taille initiale de l'espace table USERSPACE1, en pages, ou acceptez la valeur par défaut. Pour le type de conteneur d'espace table **Fichier**, le conteneur USERSPACE1 est à incrémentation automatique. Vous pouvez entrer sa taille initiale dans la zone **Taille initiale**, et une taille d'unité personnalisable dans la zone **Taille personnalisable**. La taille initiale par défaut est 16 K pages, et la taille d'unité personnalisable par défaut est 8 K pages. La taille de page du conteneur d'espace table USERSPACE1 est égale à 4 ko par page.
3) Si vous avez sélectionné **Disque dur** dans la liste **Conteneur d'espace table**, entrez les détails suivants :
   a) Dans la zone **Chemin d'unité**, entrez l'emplacement de l'unité brute. Sous Windows, le chemin doit commencer par \\.\. Voici un exemple qui montre le chemin et le nom de l'unité : \\.*nom_unité*. Sous AIX, Linux et Solaris, le chemin de l'unité doit être un chemin valide.
   b) Dans la zone **Taille initiale**, entrez la taille initiale de l'espace table USERSPACE1, ou acceptez la valeur par défaut. Pour le type de conteneur d'espace table **Disque dur**, la taille du conteneur USERSPACE1 est fixe. Sa taille par défaut est 16 K pages. Pour de meilleurs résultats, entrez une taille de votre choix.

b. Sous la zone **Détails de l'espace table LDAPSPACE**, entrez les détails suivants :
   1) Dans la liste **Conteneur d'espace table**, sélectionnez le type de conteneur. Si l'emplacement de l'espace table LDAPSPACE doit être dans le système de fichiers, sélectionnez **Fichier**. Si vous voulez créer l'espace table LDAPSPACE sur une unité brute, sélectionnez **Disque dur**. Ce disque dur est de type "unité brute", c'est-à-dire une unité sur laquelle aucun système de fichiers n'est installé.
   2) Si vous avez sélectionné **Fichier** dans la liste **Conteneur d'espace table**, entrez les détails suivants :
      a) Dans la zone **Chemin de répertoire**, entrez le chemin du répertoire dans lequel vous voulez créer l'espace table LDAPSPACE. Vous pouvez cliquer sur **Parcourir** pour sélectionner le répertoire.
      b) Dans la zone **Nom de fichier**, entrez le nom du fichier de l'espace table que vous voulez créer, ou acceptez le nom de fichier par défaut, ldapspace.
      c) Dans la zone **Taille initiale**, entrez la taille initiale de l'espace table LDAPSPACE, en pages, ou acceptez la valeur par défaut. Pour le type de conteneur d'espace table **Fichier**, le conteneur LDAPSPACE est à incrémentation automatique. Vous pouvez entrer sa taille initiale dans la zone **Taille initiale**, et une taille d'unité personnalisable

dans la zone **Taille personnalisable**. La taille initiale par défaut est 16 K pages, et la taille d'unité personnalisable par défaut est 8 K pages. La taille de page du conteneur d'espace table LDAPSPACE est égale à 32 ko par page.

3) Si vous avez sélectionné **Disque dur** dans la liste **Conteneur d'espace table**, entrez les détails suivants :

a) Dans la zone **Chemin d'unité**, entrez l'emplacement de l'unité brute. Sous Windows, le chemin doit commencer par \\.\. Voici un exemple qui montre le chemin et le nom de l'unité : \\.*nom_unité*. Sous AIX, Linux et Solaris, le chemin de l'unité doit être un chemin valide.

b) Dans la zone **Taille initiale**, entrez la taille initiale de l'espace table LDAPSPACE, ou acceptez la valeur par défaut. Pour le type de conteneur d'espace table **Disque dur**, la taille du conteneur LDAPSPACE est fixe. Sa taille par défaut est 16 K pages. Pour de meilleurs résultats, entrez une taille de votre choix.

c. Si vous avez sélectionné **Fichier** dans au moins une des deux zones **Conteneur d'espace table**, dans la zone **Taille personnalisable**, indiquez le nombre de pages à utiliser pour l'extension des conteneurs d'espace table.

6. Cliquez sur **Terminer**.
7. Pour confirmer l'achèvement de la tâche, cliquez sur **OK**.
8. Vérifiez les journaux qui ont été générés lors de la configuration de la base de données.
9. Pour fermer la page **Configurer la base de données**, cliquez sur **Fermer**.
10. Pour fermer la fenêtre Outil de configuration, cliquez sur **Fichier** > **Quitter**.
11. Pour confirmer, cliquez sur **Oui**.

Que faire ensuite

Lorsque vous avez configuré une base de données, vous devez effectuer les opérations de configuration suivantes pour l'instance :

- Configurez le nom distinctif et le mot de passe de l'administrateur principal. Voir «Gestion du nom distinctif de l'administrateur principal à l'aide de l'outil de configuration», à la page 176 et «Gestion du mot de passe de l'administrateur principal à l'aide de l'outil de configuration», à la page 178.
- Configurez les suffixes requis. Voir «Configuration des suffixes», à la page 209.

Configuration d'une base de données pour une instance à l'aide de l'utilitaire de ligne de commande

Utilisez l'utilitaire de ligne de commande, **idscfgdb**, pour configurer une base de données DB2 destinée à une instance de serveur d'annuaire.

Avant de commencer

Avant de configurer une base de données DB2 pour une instance de serveur d'annuaire, vous devez effectuer les tâches ci-après.

- Ne définissez pas la variable d'environnement *DB2COMM* lorsque vous configurez un base de données.
- Arrêtez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide des utilitaires de ligne de commande», à la page 163.

- Un ID utilisateur système susceptible d'être le propriétaire de l'instance de base de données DB2 doit exister. Pour plus d'informations sur les conditions associées aux ID utilisateur système, voir «Utilisateurs et groupes associés à une instance de serveur d'annuaire», à la page 125.

Pourquoi et quand exécuter cette tâche

Vous pouvez exécuter la commande **idscfgdb** pour effectuer les opérations ci-après.

- Créer et configurer une base de données pour une instance de serveur d'annuaire. Les paramètres de bouclage local sont créés, s'ils n'existaient pas.
- Ajouter les informations relatives à la base de données dans le fichier `ibmslapd.conf` de l'instance de serveur d'annuaire.

Vous pouvez spécifier la création de la base de données en tant que base de données de page de codes locale, ou en tant que base de données UTF-8 (base de données par défaut).

Procédure

1. Connectez-vous en tant que propriétaire de l'instance de serveur d'annuaire.
2. Accédez à l'invite de commande.
3. Le répertoire de travail en cours doit être le sous-répertoire `sbin` du répertoire d'installation d'IBM Security Directory Server.
4. Pour configurer une base de données DB2 pour une instance de serveur d'annuaire avec les valeurs suivantes, lancez la commande ci-après.
   - Nom de l'instance : `ldapdb`
   - Nom de la base de données : `ldapdb`
   - ID administrateur de la base de données DB2 : `ldapdb`
   - Mot de passe administrateur de la base de données DB2 : `ldapdb123`
   - Emplacement de la base de données : `/home/ldapdb`

   ```
   idscfgdb -I ldapdb -a ldapdb -w ldapdb123 -t ldapdb
   -l /home/ldapdb
   ```

   Sous Windows, entrez l'unité sur laquelle réside la base de données. Sous Solaris, entrez l'emplacement de la base de données. Pour plus d'informations sur la commande **idscfgdb**, consultez le manuel *Command Reference*. La commande configure une base de données avec des espaces table DMS aux tailles par défaut.

Exemples

Exemple 1 :

Pour configurer une base de données avec un espace table DMS dans un système de fichiers et doté d'une taille spécifique, utilisez la commande **idscfgdb** avec les valeurs ci-après.

- Nom de l'instance : `ldapdb`
- Nom de la base de données : `ldapdb`
- ID administrateur de la base de données DB2 : `dbadmin`
- Mot de passe administrateur de la base de données DB2 : `ldapdb123`
- Emplacement de la base de données : `c:\dblocation`
- Emplacement de l'espace table `USERSPACE1` : `c:\dblocation\ldapinst\tablespaceloc\USPACE`

- Taille du conteneur des espaces table USERSPACE1 : 10000 pages
- Taille de l'extension : 16 pages

```
idscfgdb -I ldapdb -a dbadmin -t ldapdb
-w ldapdb123 -n -l c:\dblocation
-u c:\dblocation\ldapinst\tablespaceloc\USPACE -U 10000 -z 16
```

Exemple 2 :

Pour configurer la même base de données avec des espaces table SMS, utilisez la commande **idscfgdb** avec les valeurs ci-après.

- Nom de l'instance : ldapdb
- Nom de la base de données : ldapdb
- ID administrateur de la base de données DB2 : dbadmin
- Mot de passe administrateur de la base de données DB2 : ldapdb123
- Emplacement de la base de données : c:\dblocation

```
idscfgdb -I ldapdb -a dbadmin -t ldapdb
-w ldapdb123 -n -l c:\dblocation
-m SMS
```

Que faire ensuite

Lorsque vous avez configuré une base de données, vous devez effectuer les opérations de configuration suivantes pour l'instance :

- Configurez le nom distinctif et le mot de passe de l'administrateur principal. Voir «Gestion du nom distinctif de l'administrateur principal à l'aide de l'utilitaire de ligne de commande», à la page 177 et «Gestion du mot de passe de l'administrateur principal à l'aide de l'utilitaire de ligne de commande», à la page 179.
- Configurez les suffixes requis. Voir «Configuration des suffixes», à la page 209.

Gestion du mot de passe de l'administrateur de la base de données DB2

Si vous modifiez le mot de passe système du propriétaire de l'instance DB2, vous devez le mettre à jour dans le fichier de configuration de l'instance de serveur d'annuaire.

Lorsque vous modifiez le mot de passe système du propriétaire de l'instance DB2 d'une base de données configurée avec une instance, le mot de passe n'est pas mis à jour dans le fichier de configuration de l'instance. Si le mot de passe de l'administrateur de la base de données, dans le fichier de configuration d'une instance, ne correspond pas au mot de passe système du propriétaire de l'instance DB2 qui est associé à la base de données, l'instance ne démarre pas forcément en mode normal. Vous devez mettre à jour le mot de passe du propriétaire de l'instance DB2 dans le fichier de configuration de l'instance.

Pour mettre à jour le mot de passe de l'administrateur de la base de données DB2, vous pouvez utiliser l'outil de configuration, la commande **idscfgdb**, ou la commande **idsldapmodify**.

Avant d'utiliser l'outil de configuration ou la commande **idscfgdb** pour modifier le mot de passe de l'administrateur de la base de données, vous devez arrêter le serveur d'annuaire. Pour modifier le mot de passe de l'administrateur de la base de données avec la commande **idsldapmodify**, vous devez démarrer le serveur d'annuaire en mode de configuration. Lancez la commande **idsldapmodify** en tant

qu'administrateur principal du serveur d'annuaire, ou en tant que membre du groupe des administrateurs locaux disposant du rôle `dirdata`.

Pour plus d'informations sur les commandes **idscfgdb** et **idsldapmodify**, voir le manuel *Command Reference*.

Modification du mot de passe de l'administrateur principal à l'aide de l'outil de configuration

Utilisez l'outil de configuration pour mettre à jour le mot de passe de l'administrateur de la base de données DB2 dans le fichier de configuration de l'instance de serveur d'annuaire.

Avant de commencer

Pour mettre à jour le mot de passe de l'administrateur de la base de données DB2 dans le fichier de configuration de l'instance, vous devez effectuer les tâches ci-après.

- Une instance de serveur d'annuaire configurée avec une base de données DB2 doit exister. Voir «Configuration d'une base de données d'instance à l'aide de l'outil de configuration», à la page 180.
- Arrêtez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide de l'outil de configuration», à la page 175.

Pourquoi et quand exécuter cette tâche

L'outil de configuration met à jour le mot de passe de l'administrateur de la base de données DB2 dans le fichier de configuration de l'instance de serveur d'annuaire. Si le journal des modifications est activé pour l'instance, cet outil permet également de mettre à jour le mot de passe du propriétaire de la base de données de journal des modifications dans le fichier de configuration.

Procédure

1. Démarrez l'outil de configuration pour l'instance. Voir «Démarrage de l'outil de configuration», à la page 174.
2. Dans la liste des tâches du panneau de navigation situé à gauche, cliquez sur **Tâches de base de données** > **Configurer la base de données**.
3. Dans la page **Configurer la base de données**, procédez de la façon suivante :
   a. Sélectionnez **Redéfinir le mot de passe**.
   b. Dans la zone **Mot de passe**, entrez le mot de passe de l'administrateur de la base de données.
   c. Dans la zone **Confirmation du mot de passe**, entrez le mot de passe de l'administrateur de la base de données.
   d. Cliquez sur **Suivant**.
4. Cliquez sur **Terminer**.
5. Pour confirmer l'achèvement de la tâche, cliquez sur **OK**.
6. Vérifiez les journaux qui ont été générés pour la configuration du mot de passe de la base de données.
7. Pour fermer la page **Configurer la base de données**, cliquez sur **Fermer**.
8. Pour fermer la fenêtre Outil de configuration, cliquez sur **Fichier** > **Quitter**.
9. Pour confirmer, cliquez sur **Oui**.

Que faire ensuite

Démarrez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide de l'outil de configuration», à la page 175.

Modification du mot de passe de l'administrateur de la base de données DB2 à l'aide de l'utilitaire de ligne de commande

Utilisez l'utilitaire de ligne de commande **idscfgdb** ou **idsldapmodify** pour mettre à niveau le mot de passe de l'administrateur de la base de données DB2 dans le fichier de configuration de l'instance de serveur d'annuaire.

Avant de commencer

Pour mettre à jour le mot de passe de l'administrateur de la base de données DB2 dans le fichier de configuration de l'instance, vous devez effectuer les tâches ci-après.

- Une instance de serveur d'annuaire configurée avec une base de données DB2 doit exister. Voir «Configuration d'une base de données pour une instance à l'aide de l'utilitaire de ligne de commande», à la page 184.

Pourquoi et quand exécuter cette tâche

Vous pouvez exécuter la commande **idscfgdb** pour mettre à jour le mot de passe de l'administrateur de la base de données DB2 dans le fichier de configuration de l'instance. Vous devez arrêter le serveur d'annuaire avant de lancer la commande **idscfgdb**.

Vous pouvez utiliser la commande **idsldapmodify** pour modifier le mot de passe alors que l'instance de serveur d'annuaire est en cours. Lancez la commande **idsldapmodify** en tant qu'administrateur principal du serveur d'annuaire, ou en tant que membre du groupe des administrateurs locaux disposant du rôle `dirdata`.

Pour plus d'informations sur les commandes **idscfgdb** et **idsldapmodify**, voir le manuel *Command Reference*.

Procédure

1. Connectez-vous en tant que propriétaire de l'instance de serveur d'annuaire.
2. Accédez à l'invite de commande.
3. Pour modifier le mot de passe de l'administrateur de la base de données DB2, choisissez l'une des méthodes suivantes :
   - Pour modifier le mot de passe de l'administrateur de la base de données DB2 à l'aide de la commande **idscfgdb**, effectuez les opérations ci-après.
     a. Le répertoire de travail en cours doit être le sous-répertoire `sbin` du répertoire d'installation d'IBM Security Directory Server.
     b. Arrêtez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide des utilitaires de ligne de commande», à la page 163.
     c. Exécutez la commande **idscfgdb** avec la syntaxe ci-après.
        ```
        idscfgdb -I nom_instance -w mdp_admin_db2
        ```
     d. Démarrez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide des utilitaires de ligne de commande», à la page 163.

- Pour modifier le mot de passe de l'administrateur de la base de données DB2 à l'aide de la commande **idsldapmodify**, effectuez les opérations ci-après.
  a. Le répertoire de travail en cours doit être le sous-répertoire `bin` du répertoire d'installation d'IBM Security Directory Server.
  b. Exécutez la commande **idsldapmodify** avec la syntaxe ci-après.

     ```
     idscfgdb -h adresse_IP -p port -D DN_admin -w mdp_admin -i file1.ldif
     ```

     Le fichier `file1.ldif` contient les entrées suivantes :

     ```
     dn: cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas,
      cn=Configuration
     changetype: modify
     replace: ibm-slapdDbUserPW
     ibm-slapdDbUserPW: mdp_admin_db2
     ```
  c. Redémarrez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide des utilitaires de ligne de commande», à la page 163.

Annulation de la configuration de la base de données dans une instance de serveur d'annuaire

Pour utiliser une instance de serveur d'annuaire existante avec une autre base de données DB2, vous devez annuler la configuration de la base de données DB2 existante dans l'instance.

Vous ne pouvez annuler la configuration d'une base de données d'une instance de serveur d'annuaire que si vous avez configuré une base de données DB2 cette instance.

L'outil de configuration ou la commande **idsucfgdb** vous permettent de réaliser les opérations ci-après.

- Supprimer les informations sur la base de données DB2 dans le fichier de configuration d'une instance de serveur d'annuaire. Au cours de cette opération, l'utilitaire annule la configuration de la base de données DB2 dans une instance, mais ne supprime pas la base de données elle-même.
- Supprimer les informations sur la base de données DB2 dans le fichier de configuration d'une instance de serveur d'annuaire, et supprimer la base de données DB2. Au cours de cette opération, la base de données DB2 est supprimée et toutes les données sont perdues.

Lorsque vous annulez la configuration d'une base de données DB2 dans une instance de serveur d'annuaire, la base de données devient inaccessible à l'instance.

L'annulation de la configuration de la base de données n'et pas prise en charge pour une instance de serveur proxy.

Pour plus d'informations sur la commande **idsucfgdb**, consultez le manuel *Command Reference*.

Annulation de la configuration de la base de données DB2 d'une instance à l'aide de l'outil de configuration

Utilisez l'outil de configuration pour annuler la configuration de la base de données DB2 d'une instance de serveur d'annuaire.

Avant de commencer

Vous pouvez annuler la configuration de la base de données DB2 d'une instance si l'instance respecte les conditions ci-après.

- Une instance de serveur d'annuaire configurée avec une base de données DB2 doit exister. Voir «Configuration d'une base de données d'instance à l'aide de l'outil de configuration», à la page 180.
- Arrêtez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide de l'outil de configuration», à la page 175.

Procédure

1. Démarrez l'outil de configuration pour l'instance. Voir «Démarrage de l'outil de configuration», à la page 174.
2. Dans la liste des tâches du panneau de navigation situé à gauche, cliquez sur **Tâches de base de données** > **Annuler la configuration de la base de données**.
3. Dans la page **Annuler la configuration de la base de données**, procédez de la façon suivante :
   a. Dans la zone Options, sélectionnez l'une des options ci-après.
      - Pour annuler la configuration de la base de données DB2 d'une instance sans supprimer la base de données elle-même, cliquez sur **Annuler la configuration de la base de données**.
      - Pour annuler la configuration de la base de données DB2 d'une instance et supprimer la base de données, cliquez sur **Annuler la configuration et supprimer la base de données**.
   b. Pour supprimer la copie de sauvegarde de l'instance si la base de données est configurée pour la sauvegarde en ligne, sélectionnez **Supprimer la copie de sauvegarde de la base de données**.
   c. Pour démarrer l'annulation de la configuration, cliquez sur **Annuler la configuration**.
   d. Dans la fenêtre de confirmation, cliquez sur **Oui**.
4. Pour confirmer l'achèvement de la tâche, cliquez sur **OK**.
5. Vérifiez les journaux qui ont été générés lors de l'annulation de l'annulation de la configuration de la base de données.
6. Pour fermer la page **Annuler la configuration de la base de données**, cliquez sur **Annuler**.
7. Pour fermer la fenêtre Outil de configuration, cliquez sur **Fichier** > **Quitter**.
8. Pour confirmer, cliquez sur **Oui**.

Annulation de la configuration de la base de données DB2 d'une instance à l'aide de l'outil de configuration

Utilisez l'utilitaire de ligne de commande **idsucfgdb** pour annuler la configuration de la base de données à partir d'une instance de serveur d'annuaire.

Avant de commencer

Vous pouvez annuler la configuration de la base de données DB2 d'une instance si l'instance respecte les conditions ci-après.

- Une instance de serveur d'annuaire configurée avec une base de données DB2 doit exister. Voir «Configuration d'une base de données pour une instance à l'aide de l'utilitaire de ligne de commande», à la page 184.
- Arrêtez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide des utilitaires de ligne de commande», à la page 163.

Procédure

1. Connectez-vous en tant que propriétaire de l'instance de serveur d'annuaire.
2. Accédez à l'invite de commande.
3. Le répertoire de travail en cours doit être le sous-répertoire `sbin` du répertoire d'installation d'IBM Security Directory Server.
4. Pour annuler la configuration de la base de données DB2 d'une instance, choisissez l'une des options ci-après.
   - Pour annuler la configuration de la base de données d'une instance de serveur d'annuaire, entrez la commande **idsucfgdb** avec la syntaxe ci-après.
     ```
     idsucfgdb -I nom_instance
     ```
   - Pour annuler la configuration de la base de données d'une instance de serveur d'annuaire et la supprimer, entrez la commande **idsucfgdb** avec la syntaxe ci-après.
     ```
     idsucfgdb -I nom_instance -r
     ```

Optimisation de la base de données

Pour améliorer les performances de recherche de la base de données DB2, vous pouvez optimiser la base et mettre à jour les statistiques DB2 des tables de la base.

Vous pouvez utiliser l'outil de configuration ou la commande **idsrunstats** pour optimiser la base de données DB2. L'optimisation doit être réalisée régulièrement ou après les mises à jour de la base de données, par exemple après une importation.

Lorsque vous optimisez la base de données, l'outil collecte les statistiques de tous les index qui sont définis sur les tables, et les met à jour. L'optimiseur de requêtes DB2 utilise ces statistiques pour déterminer le meilleur chemin d'accès aux données.

Vous ne pouvez pas optimiser DB2 si l'instance est un serveur proxy, ou si elle n'est pas configurée avec une base de données DB2.

Pour plus d'informations sur la commande **idsrunstats**, consultez le manuel *Command Reference*.

Optimisation de la base de données avec l'Outil de configuration

Utilisez l'Outil de configuration pour optimiser la base de données associée à une instance.

Avant de commencer

Pour permettre l'optimisation de la base de données DB2 d'une instance, l'instance doit respecter les conditions ci-après.

- Une instance de serveur d'annuaire configurée avec une base de données DB2 doit exister. Voir «Configuration d'une base de données d'instance à l'aide de l'outil de configuration», à la page 180.

Procédure

1. Démarrez l'outil de configuration pour l'instance. Voir «Démarrage de l'outil de configuration», à la page 174.
2. Dans la liste des tâches du panneau de navigation situé à gauche, cliquez sur **Tâches de base de données** > **Optimiser la base de données**.
3. Dans la page **Optimiser la base de données**, procédez de la façon suivante :
   a. Pour démarrer l'opération d'optimisation de la base de données, cliquez sur **Optimiser**.
   b. Pour confirmer l'achèvement de la tâche, cliquez sur **OK**.
   c. Vérifiez les journaux qui ont été générés lors de l'optimisation de la base de données.
   d. Pour effacer leur contenu, cliquez sur **Effacer les résultats**.
4. Pour fermer la page **Optimiser la base de données**, cliquez sur **Fermer**.
5. Pour fermer la fenêtre Outil de configuration, cliquez sur **Fichier** > **Quitter**.
6. Pour confirmer, cliquez sur **Oui**.

Optimisation de la base de données à l'aide de l'utilitaire de ligne de commande

Utilisez l'utilitaire de ligne de commande **idsrunstats** pour optimiser la base de données DB2 associée à une instance.

Avant de commencer

Vous pouvez optimiser la base de données DB2 d'une instance si l'instance respecte les conditions ci-après.

- Une instance de serveur d'annuaire configurée avec une base de données DB2 doit exister. Voir «Configuration d'une base de données pour une instance à l'aide de l'utilitaire de ligne de commande», à la page 184.

Procédure

1. Connectez-vous en tant que propriétaire de l'instance de serveur d'annuaire.
2. Accédez à l'invite de commande.
3. Le répertoire de travail en cours doit être le sous-répertoire `sbin` du répertoire d'installation d'IBM Security Directory Server.
4. Pour optimiser la base de données DB2, lancez la commande **idsrunstats** avec la syntaxe ci-après.

   ```
   idsrunstats -I nom_instance
   ```

   Pour plus d'informations sur la commande **idsrunstats**, consultez le manuel *Command Reference*.

Maintenance de la base de données

Pour améliorer les opérations de recherche et de mise à jour sur une instance, vous pouvez lancer la réorganisation d'index DB2 ou la compression de ligne DB2.

Vous pouvez utiliser l'outil de configuration ou la commande **idsdbmaint** pour lancer la réorganisation d'index DB2 ou la compression de ligne DB2.

Lorsque les tables DB2 d'une base de données sont mises à jour avec de nombreuses insertions et suppressions, les recherches et les mises à jour dans la base de données ralentissent. Si vous réorganisez l'index DB2, les performances de recherche et de mise à jour s'améliorent.

Lorsque vous lancez la compression de ligne DB2, l'outil identifie les motifs qui se répètent et les remplace par des chaînes symboliques plus courtes. Après analyse, l'outil ne lance la compression des ligne que si ses résultats doivent apporter une amélioration supérieure à 30 pourcent.

Vous pouvez également utiliser la commande **idsdbmaint** pour convertir un espace table SMS en espace table DMS, ou inversement. La conversion des espaces table n'est pas prise en charge par l'outil de configuration. Pour plus d'informations sur la commande **idsdbmaint**, consultez le manuel *Command Reference*.

Exécution de la maintenance de la base de données avec l'Outil de configuration

Utilisez l'Outil de configuration pour effectuer la maintenance de la base de données associée à une instance.

Avant de commencer

Pour effectuer la maintenance de la base de données DB2 d'une instance, l'instance doit respecter les conditions ci-après.

- Une instance de serveur d'annuaire configurée avec une base de données DB2 doit exister. Voir «Configuration d'une base de données d'instance à l'aide de l'outil de configuration», à la page 180.
- Arrêtez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide de l'outil de configuration», à la page 175.

Procédure

1. Démarrez l'outil de configuration pour l'instance. Voir «Démarrage de l'outil de configuration», à la page 174.
2. Dans la liste des tâches du panneau de navigation situé à gauche, cliquez sur **Tâches de base de données** > **Maintenance**.
3. Dans la page **Maintenance** , procédez comme suit.
   a. Sélectionnez l'opération de maintenance de la base de données DB2 que vous souhaitez exécuter :
      - Pour réorganiser des index DB2, cliquez sur **Effectuer la réorganisation des index**.
      - Pour compresser les lignes dans DB2, cliquez sur **Inspecter les tables et effectuer la compression de lignes**.
   b. Cliquez sur **OK**.
   c. Dans la fenêtre d'achèvement de la tâche, cliquez sur **OK**.
   d. Vérifiez les journaux qui ont été générés lors de l'opération de maintenance de la base de données.
   e. Pour effacer leur contenu, cliquez sur **Effacer les résultats**.
4. Pour fermer la page **Maintenance**, cliquez sur **Fermer**.

5. Pour fermer la fenêtre Outil de configuration, cliquez sur **Fichier** > **Quitter**.
6. Pour confirmer, cliquez sur **Oui**.

Que faire ensuite

Démarrez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide de l'outil de configuration», à la page 175.

Exécution de la maintenance de la base de données à l'aide de l'utilitaire de ligne de commande

Utilisez l'utilitaire de ligne de commande **idsdbmaint** pour exécuter la maintenance de la base de données DB2 associée à une instance.

Avant de commencer

Pour effectuer la maintenance de la base de données DB2, l'instance doit respecter les conditions ci-après.

- Une instance de serveur d'annuaire configurée avec une base de données DB2 doit exister. Voir «Configuration d'une base de données pour une instance à l'aide de l'utilitaire de ligne de commande», à la page 184.
- Arrêtez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide des utilitaires de ligne de commande», à la page 163.

Procédure

1. Connectez-vous en tant que propriétaire de l'instance de serveur d'annuaire.
2. Accédez à l'invite de commande.
3. Le répertoire de travail en cours doit être le sous-répertoire `sbin` du répertoire d'installation d'IBM Security Directory Server.
4. Pour réorganiser des index DB2, lancez la commande **idsdbmaint** avec la syntaxe ci-après.

   ```
   idsdbmaint -I nom_instance -i
   ```

   Pour plus d'informations sur la commande **idsdbmaint**, consultez le manuel *Command Reference*.
5. Pour effectuer la compression de ligne DB2, lancez la commande **idsdbmaint** avec la syntaxe ci-après.

   ```
   idsdbmaint -I nom_instance -r
   ```

Que faire ensuite

Démarrez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide des utilitaires de ligne de commande», à la page 163.

Sauvegarde du serveur d'annuaire

Pour pouvoir effectuer une reprise en cas d'incident sur un serveur d'annuaire, vous devez sauvegarder fréquemment l'instance de ce serveur.

Vous pouvez utiliser l'outil de configuration ou la commande **idsdbback** pour sauvegarder une instance. Vous ne pouvez pas utiliser la commande **idsdbback** pour sauvegarder une instance de serveur proxy parce qu'aucune base de données ne lui est associée.

Pour configurer une base de données associée à une instance en vue d'une sauvegarde en ligne, vous pouvez utiliser la commande **idscfgdb**. Cependant, la configuration de la sauvegarde en ligne ne peut pas être annulée à l'aide de la commande **idscfgdb** et du paramètre **-c**. Si vous configurez une sauvegarde en ligne pour une instance à l'aide de l'outil d'administration d'instance ou de l'outil de configuration, vous pouvez annuler la configuration avec l'outil de configuration ou la commande **idscfgdb**. Pour obtenir les résultats les plus fiables, utilisez l'outil d'administration d'instance ou l'outil de configuration pour configurer la sauvegarde en ligne d'une instance avec une base de données.

Vous pouvez également utiliser la commande **idsdb2ldif** pour exporter les entrées d'un serveur d'annuaire dans un fichier LDIF. Vous pouvez utiliser la commande **migbkup** pour sauvegarder les fichiers de schéma et de configuration d'une instance de serveur d'annuaire et d'une instance de serveur proxy. Pour plus d'informations sur les commandes **idsdbback**, **idsdb2ldif** ou **migbkup**, consultez le manuel *Command Reference*. Pour plus d'informations sur le choix des commandes pour cet environnement, voir la section *Performance Tuning and Capacity Planning* de la documentation IBM Security Directory Server.

L'outil de configuration permet d'effectuer les opérations ci-après.

- Sauvegardez les paramètres de configuration d'une instance de serveur d'annuaire ou d'une instance de serveur proxy.
- Sauvegardez l'instance du serveur d'annuaire avec sa base de données.
- Sauvegardez l'instance du serveur d'annuaire et la base de données du journal des modifications si elle est configurée pour une instance.

Pour plus d'informations sur les opérations de sauvegarde et de restauration, voir la section *Administration* dans la documentation d'IBM Security Directory Server.

Sauvegarde de la base de données d'une instance de serveur d'annuaire à l'aide de l'outil de configuration

Utilisez l'outil de configuration pour sauvegarder une instance de serveur d'annuaire avec sa base de données dans l'objectif d'une éventuelle reprise après incident.

Avant de commencer

Vous pouvez sauvegarder une instance de serveur d'annuaire avec sa base de données si l'instance respecte les conditions ci-après.

- Une instance de serveur d'annuaire configurée avec une base de données DB2 doit exister. Voir «Configuration d'une base de données d'instance à l'aide de l'outil de configuration», à la page 180.

Procédure

1. Démarrez l'outil de configuration pour l'instance. Voir «Démarrage de l'outil de configuration», à la page 174.
2. Dans la liste des tâches du panneau de navigation situé à gauche, cliquez sur **Sauvegarder/Restaurer** > **Sauvegarder la base de données**.

3. Dans la page **Sauvegarder la base de données**, procédez de la façon suivante :
   a. Dans la zone **Répertoire de sauvegarde**, entrez le chemin du répertoire dans lequel vous voulez sauvegarder toutes les données d'annuaire et les fichiers de configuration. Vous pouvez également cliquer sur **Parcourir** pour entrer le chemin du répertoire.
   b. Pour la sauvegarde en ligne, choisissez l'une des options suivantes:
      - Pour configurer le serveur d'annuaire et sa base de données en vue de la sauvegarde en ligne si celle-ci n'est pas déjà configurée, sélectionnez **Mettre à jour la configuration de base de données pour la prise en charge de la sauvegarde en ligne**.
      - Pour exécuter la sauvegarde en ligne de l'instance de serveur d'annuaire si cette sauvegarde est configurée sur le serveur, sélectionnez **Effectuer la sauvegarde en ligne**.
   c. Pour sauvegarder la base de données du journal des modifications de l'instance si ce journal est configuré, sélectionnez **Inclure les données du journal des modifications dans la sauvegarde**.
   d. Pour exclure les fichiers de la base de données de la sauvegarde, sélectionnez **Ne pas sauvegarder les fichiers de base de données**. Si vous sélectionnez **Ne pas sauvegarder les fichiers de base de données**, les fichiers de la base de données et les fichiers de la base de données du journal des modifications de l'instance de serveur d'annuaire ne sont pas sauvegardés. L'outil sauvegarde les fichiers de l'instance de serveur d'annuaire, tels que les fichiers de dissimulation de clés, les fichiers de schéma et les fichiers de configuration.
   e. En fonction de l'existence ou de l'absence du répertoire de sauvegarde, vous disposez des options suivantes, relatives à la poursuite de la sauvegarde :
      - Pour créer le répertoire de sauvegarde s'il n'existe pas, cliquez sur **Création du répertoire de sauvegarde si nécessaire**.
      - Si le répertoire de sauvegarde n'existe pas, et si vous ne voulez pas le créer, cliquez sur **Interrompre si le répertoire de sauvegarde est introuvable**. Si le répertoire de sauvegarde n'existe pas et si vous sélectionnez cette option, la base de données n'est pas sauvegardée.

      Remarque : Ne quittez pas l'outil de configuration tant que l'opération de sauvegarde est en cours.
   f. Pour démarrer la sauvegarde, cliquez sur **Sauvegarder**.
   g. Si la sauvegarde demande l'arrêt du serveur d'annuaire, cliquez sur **Oui**.
   h. Pour confirmer l'achèvement de la tâche, cliquez sur **OK**.
   i. Vérifiez les journaux qui ont été générés lors de la sauvegarde.
   j. Pour effacer leur contenu, cliquez sur **Effacer les résultats**.
   k. Pour fermer la page **Sauvegarder la base de données**, cliquez sur **Fermer**.
4. Pour fermer la fenêtre Outil de configuration, cliquez sur **Fichier** > **Quitter**.
5. Pour confirmer, cliquez sur **Oui**.

Sauvegarde d'une instance de serveur proxy avec l'Outil de configuration

Utilisez l'outil de configuration pour sauvegarder une instance de serveur d'annuaire en vue d'une reprise après incident.

Avant de commencer

Vous ne pouvez sauvegarder une instance de serveur proxy que si elle existe déjà. Voir «Création d'une instance de serveur proxy avec des paramètres personnalisés» , à la page 148.

Procédure

1. Démarrez l'outil de configuration pour l'instance. Voir «Démarrage de l'outil de configuration», à la page 174.
2. Dans la liste des tâches du panneau de navigation situé à gauche, cliquez sur **Sauvegarder/Restaurer** > **Sauvegarder l'instance**.
3. Dans la page **Sauvegarder l'instance**, procédez comme suit.
   a. Dans la zone **Répertoire de sauvegarde**, entrez le chemin du répertoire dans lequel vous voulez sauvegarder le fichier schéma et les fichiers de configuration. Vous pouvez également cliquer sur **Parcourir** pour entrer le chemin du répertoire.
   b. Pour une instance de serveur proxy, la case **Ne pas sauvegarder les fichiers de base de données** est cochée.
   c. En fonction de l'existence ou de l'absence du répertoire de sauvegarde, vous disposez des options suivantes, relatives à la poursuite de la sauvegarde :
      - Pour créer le répertoire de sauvegarde s'il n'existe pas, cliquez sur **Création du répertoire de sauvegarde si nécessaire**.
      - Si le répertoire de sauvegarde n'existe pas, et si vous ne voulez pas le créer, cliquez sur **Interrompre si le répertoire de sauvegarde est introuvable**. Si le répertoire de sauvegarde n'existe pas et si vous sélectionnez cette option, l'instance de proxy n'est pas sauvegardée.

      Remarque : Ne quittez pas l'outil de configuration tant que l'opération de sauvegarde est en cours.
   d. Pour démarrer la sauvegarde, cliquez sur **Sauvegarder**.
   e. Si l'opération demande l'arrêt de l'instance, cliquez sur **Oui**.
   f. Pour confirmer l'achèvement de la tâche, cliquez sur **OK**.
   g. Vérifiez les journaux qui ont été générés lors de la sauvegarde.
   h. Pour effacer leur contenu, cliquez sur **Effacer les résultats**.
   i. Pour fermer la page **Sauvegarder l'instance**, cliquez sur **Fermer**.
4. Pour fermer la fenêtre Outil de configuration, cliquez sur **Fichier** > **Quitter**.
5. Pour confirmer, cliquez sur **Oui**.

Restauration d'un serveur d'annuaire

Si votre instance de serveur d'annuaire échoue, vous pouvez la restaurer à partir de la dernière image de sauvegarde.

Vous pouvez utiliser l'outil de configuration ou la commande **idsdbestore** pour restaurer des données d'annuaire et éventuellement les paramètres de configuration que vous avez précédemment sauvegardés. Vous devez arrêter le serveur d'annuaire avant de restaurer la base de données et/ou les paramètres de configuration.

Dans le cas d'un serveur proxy, vous pouvez restaurer les paramètres de configuration. Pour un serveur proxy, vous devez exécuter la commande **idsdbrestore** avec le paramètre **-x**.

Pour une instance avec une base de données DB2, vous pouvez restaurer la base de données dans une base de données et une instance de base de données qui portent le même nom que celui qui a été utilisé pour la sauvegarde de la base de données. Un serveur d'annuaire avec une base de données DB2 ne peut être restauré que s'il existe une base de données configurée pour l'instance de serveur d'annuaire. La commande **idsdbestore** permet de restaurer la base de données de sauvegarde dans la base de données en cours de configuration. La commande échoue si l'instance de base de données et la base de données sauvegardées ne correspondent pas à l'instance de base de données et à la base de données configurées. Pour que la base de données puisse être restaurée, l'emplacement de la base de données sauvegardée et celui de la base de données objet de la restauration doivent être les mêmes.

Pour plus d'informations sur la commande **idsdbrestore**, consultez le manuel *Command Reference*.

Restauration de la base de données d'un serveur d'annuaire à l'aide de l'outil de configuration

Utilisez l'outil de configuration pour restaurer une instance de serveur d'annuaire et sa base de données à partir d'une image de sauvegarde.

Avant de commencer

Vous pouvez restaurer une instance de serveur d'annuaire et sa base de données si l'instance respecte les conditions ci-après.

- Une instance de serveur d'annuaire configurée avec une base de données DB2 doit exister. Voir «Configuration d'une base de données d'instance à l'aide de l'outil de configuration», à la page 180.
- Une image de sauvegarde de l'instance de serveur d'annuaire doit exister. Voir «Sauvegarde de la base de données d'une instance de serveur d'annuaire à l'aide de l'outil de configuration», à la page 195.
- Arrêtez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide de l'outil de configuration», à la page 175.

Procédure

1. Démarrez l'outil de configuration pour l'instance. Voir «Démarrage de l'outil de configuration», à la page 174.
2. Dans la liste des tâches du panneau de navigation situé à gauche, cliquez sur **Sauvegarder/Restaurer** > **Restaurer la base de données**.
3. Dans la page **Restaurer la base de données**, procédez de la façon suivante :
   a. Dans la zone **Restaurer le répertoire**, entrez le chemin qui contient l'image de sauvegarde de l'instance. Vous pouvez également cliquer sur **Parcourir** pour entrer le chemin du répertoire.
   b. Si vous souhaitez restaurer uniquement les données d'annuaire et non les paramètres de configuration de l'image de sauvegarde, sélectionnez **Conserver les paramètres de configuration en cours**. i vous souhaitez restaurer à la fois la base de données et les paramètres de configuration, désélectionnez **Conserver les paramètres de configuration en cours**.
   c. Si le journal des modifications est configuré pour l'instance et si vous souhaitez également le restaurer, sélectionnez **Inclure les données du journal des modifications dans la restauration**.
   d. Pour lancer la restauration, cliquez sur **Restaurer**.

e. Si l'opération demande l'arrêt du serveur d'annuaire, cliquez sur **Oui**.
f. Pour confirmer l'achèvement de la tâche, cliquez sur **OK**.
g. Vérifiez les journaux qui ont été générés lors de la restauration.
h. Pour effacer leur contenu, cliquez sur **Effacer les résultats**.
i. Pour fermer la page **Restaurer la base de données**, cliquez sur **Fermer**.

4. Pour fermer la fenêtre Outil de configuration, cliquez sur **Fichier** > **Quitter**.
5. Pour confirmer, cliquez sur **Oui**.

Restauration d'une instance de serveur proxy avec l'Outil de configuration

Utilisez l'outil de configuration pour restaurer une instance de serveur proxy en vue d'une reprise après incident.

Avant de commencer

Pour restaurer une instance de serveur proxy, l'instance doit respecter les conditions ci-après.

- L'instance de serveur proxy doit exister. Voir «Création d'une instance de serveur proxy avec des paramètres personnalisés», à la page 148.
- Une image de sauvegarde de l'instance de serveur proxy doit exister. Voir «Sauvegarde d'une instance de serveur proxy avec l'Outil de configuration», à la page 196.
- Arrêtez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide de l'outil de configuration», à la page 175.

Procédure

1. Démarrez l'outil de configuration pour l'instance. Voir «Démarrage de l'outil de configuration», à la page 174.
2. Dans la liste des tâches du panneau de navigation situé à gauche, cliquez sur **Sauvegarder/Restaurer** > **Restaurer l'instance**.
3. Dans la page **Restaurer l'instance**, procédez comme suit.
   a. Dans la zone **Restaurer le répertoire**, entrez le chemin qui contient l'image de sauvegarde de l'instance. Vous pouvez également cliquer sur **Parcourir** pour entrer le chemin du répertoire.
   b. Si vous souhaitez restaurer les paramètres de configuration de l'image de sauvegarde, sélectionnez **Conserver les paramètres de configuration en cours**.
   c. Pour lancer la restauration, cliquez sur **Restaurer**.
   d. Si l'opération demande l'arrêt du serveur d'annuaire, cliquez sur **Oui**.
   e. Pour confirmer l'achèvement de la tâche, cliquez sur **OK**.
   f. Vérifiez les journaux qui ont été générés lors de la restauration.
   g. Pour effacer leur contenu, cliquez sur **Effacer les résultats**.
   h. Pour fermer la page **Restaurer l'instance**, cliquez sur **Fermer**.
4. Pour fermer la fenêtre Outil de configuration, cliquez sur **Fichier** > **Quitter**.
5. Pour confirmer, cliquez sur **Oui**.

Optimisation des performances d'un serveur d'annuaire

Vous devez optimiser les performances de recherche et de mise à jour des instances de serveur d'annuaire.

Vous pouvez optimiser une instance de serveur d'annuaire à l'aide de l'outil de configuration ou de la commande **idsperftune**. L'outil génère des valeurs de paramètre d'optimisation des performances pour les caches de serveur d'annuaire et les pools de mémoire tampon DB2. Ces valeurs sont basées sur celles que vous avez saisies pour l'instance de serveur d'annuaire. L'outil peut également modifier les paramètres d'optimisation d'une instance. Il sauvegarde le fichier `ibmslapd.conf` et l'enregistre dans le fichier `logs/ibmslapd.conf.save` du répertoire de base de l'instance de serveur d'annuaire.

L'outil enregistre les informations que vous saisissez dans le fichier `logs/perftune_input.conf` du répertoire de base de l'instance de serveur d'annuaire.

L'outil de configuration ou la commande **idsperftune** utilise vos valeurs pour calculer les paramètre suivants de l'instance :

- Taille du cache d'une entrée
- Taille du cache de filtrage
- Taille du cache d'un membre de groupe
- Limite du contournement du cache d'un membre de groupe
- Taille du pool de mémoire tampon `DB2 LDAPDB`
- Taille du pool de mémoire tampon `DB2 IBMDEFAULTDB`

Si l'instance de serveur d'annuaire est en cours d'exécution, l'outil surveille ses performances et fournit le diagnostic d'intégrité de la base de données. Le diagnostic d'intégrité comprend les paramètres DB2 suivants :

- `DB2 NUM_IOSERVERS`
- `DB2 NUM_IOCLEANERS`
- `CATALOGCACHE_SZ`
- `PCKCACHESZ`
- `LOGFILSIZ`
- `LOCKLIST`

Si vous lancez une optimisation avancée d'une instance de serveur d'annuaire, l'outil collecte et analyse ses données. L'instance doit fonctionner un certain temps pour que les données d'optimisation DB2 soient collectées au cours de l'analyse d'intégrité. L'outil génère les valeurs d'optimisation des paramètres DB2 suivants, et les enregistre dans le fichier `logs/perftune_stat.log` de l'instance.

- `SORTHEAP`
- `MAXFILOP`
- `DBHEAP`
- `CHNGPGS_THRESH`
- `NUM_IOSERVERS`
- `NUM_IOCLEANERS`

Les recommandations basées sur le diagnostic d'intégrité des paramètres DB2 peuvent être celles ci-après.

- OK
- Augmenter
- Réduire
- Non collecté

Le diagnostic des paramètres DB2 qui ne sont pas analysés prend la valeur Non collecté. Les valeurs recommandées vous permettent de sélectionner les paramètres DB2 à optimiser pour obtenir les meilleures performances.

Pour de meilleurs performances, vous devez lancer l'outil sur une instance dès le chargement des données d'annuaire initiales. Après la première optimisation, exécutez l'outil régulièrement, particulièrement après avoir chargé de nombreuses entrées ou effectué de nombreuses momifications dans les entrées.Pour plus d'informations sur l'optimisation d'une instance de serveur d'annuaire, consultez la section *Performance Tuning and Capacity Planning* de la documentation IBM Security Directory Server.

Vous ne pouvez pas utiliser l'outil de configuration ou la commande **idsperftune** pour optimiser une instance de serveur proxy ou une instance qui n'est pas configurée avec une base de données.

Configuration d'un serveur d'annuaire en vue de l'optimisation des performances à l'aide de l'outil de configuration

Utilisez l'outil de configuration pour optimiser un serveur d'annuaire et améliorer les performances des opérations de recherche et de mise à jour.

Avant de commencer

Vous pouvez optimiser une instance de serveur d'annuaire si elle respecte les conditions ci-après.

- Une instance de serveur d'annuaire configurée avec une base de données DB2 doit exister. Voir «Configuration d'une base de données d'instance à l'aide de l'outil de configuration», à la page 180.

Procédure

1. Démarrez l'outil de configuration pour l'instance. Voir «Démarrage de l'outil de configuration», à la page 174.
2. Dans la liste des tâches du panneau de navigation situé à gauche, cliquez sur **Tâches de base de données** > **Optimiser les performances**.
3. Dans la page **Optimiser les performances**, procédez de la façon suivante :
   a. Dans la zone **Pourcentage de la mémoire système disponible à allouer à cette instance d'annuaire**, entrez le pourcentage de mémoire système que vous souhaitez allouer à l'instance. La mémoire système disponible est répartie entre plusieurs instances de serveur, ou entre les instances et les autres serveurs que vous prévoyez d'exécuter sur le système. L'outil utilise les valeurs saisies pour calculer la taille des caches d'entrée et de filtrage.
   b. Dans la zone **Nombre planifié de groupes**, saisissez le nombre de groupes que vous prévoyez d'ajouter dans l'instance. L'outil utilise les valeurs saisies pour calculer la taille des caches de serveur d'annuaire.
   c. Dans la zone **Nombre maximal de membres dans un groupe pouvant être fréquemment utilisés en tant que référence**, saisissez le nombre moyen de membres de groupes qui peuvent être fréquemment utilisés en tant que référence.

d. Sous la section **Nombre d'entrées et taille d'entrée moyenne**, choisissez l'une des options ci-après.
   - Pour estimer le nombre d'entrées dans l'annuaire et la taille moyenne d'une entrée, procédez comme suit.
     1) Dans la zone **Nombre planifié d'entrées**, entrez le nombre total d'entrées prévu pour l'instance. L'outil tente de déterminer le nombre d'entrées dans l'instance de serveur d'annuaire. En cas d'échec, il utilise une valeur par défaut égale à 10 000 entrées. L'outil utilise cette valeur pour calculer la taille des caches de serveur d'annuaire.
     2) Dans la zone **Taille moyenne d'une entrée**, indiquez la taille moyenne en octets d'une entrée dans l'instance. L'outil tente de calculer la taille d'une entrée dans l'instance de serveur d'annuaire. En cas d'échec, il emploie une valeur par défaut égale à 2650 octets. L'outil utilise cette valeur pour calculer la taille des caches de serveur d'annuaire.
   - Si vous souhaitez que l'outil détermine le nombre total d'entrées et la taille moyenne d'une entrée, cliquez sur **Charger à partir de la base de données de l'instance de serveur**. L'outil remplit les zones **Nombre planifié d'entrées** et **Taille moyenne d'une entrée**.

e. Sous la zone **Fréquence des mises à jour**, sélectionnez l'une des options ci-après.
   - Si vous pensez que l'instance sera mise à jour fréquemment, cliquez sur **Mises à jour fréquentes**. En règle générale, les mises à jour sont considérées comme fréquentes si elles se produisent en moyenne toutes les 500 recherches.
   - Si les mises à jour attendues sont moins fréquentes ou si elles sont regroupées et effectuées à certaines heures de la journée, cliquez sur **Mises à jour par lots**.

   L'outil utilise ces informations pour définir la taille du cache de filtrage. Le cache de filtrage est utile uniquement lorsque des mises à jour non fréquentes sont effectuées sur l'instance et que les mêmes recherches sont exécutées plusieurs fois. Si des mises à jour fréquentes sont prévues, le cache de filtrage prend la valeur 0. Si des mises à jour peu fréquentes ou par lots sont prévues, le cache de filtrage prend la valeur de 1024 entrées de cache.

f. Si vous souhaitez que l'outil fournisse des données d'analyse des performances, sélectionnez **Activer la collecte de données système supplémentaires pour une optimisation étendue**.
   - Si vous cochez cette case, les inverseurs logiques du moniteur DB2, `BUFFERPOOL` et `SORTHEAP`, sont activés. Les performances de l'instance de serveur d'annuaire sont susceptibles de se dégrader lorsque l'outil active les inverseurs logiques du moniteur DB2 pour collecter les données.
   - Pour obtenir des données exactes en vue de la meilleure optimisation possible de l'instance de serveur d'annuaire, cochez la case lorsque l'activité de l'annuaire est réellement représentative de votre environnement. Si vous procédez à un diagnostic de la base de données lorsque le serveur est moins occupé que d'ordinaire, les recommandations liées aux performances ne sont pas optimales.

g. Cliquez sur **Suivant**. La fenêtre **Optimisation des performances : vérification** s'affiche.

4. Dans la page **Optimiser les performances : vérification**, procédez de la façon suivante :
   a. Dans la liste **Etat de santé de la base de données**, vérifiez les paramètres d'optimisation des performances générés par l'outil. S'il n'y a pas d'activité de la base de donnés pour l'instance, la liste **Etat de santé de la base de données** peut être vide. La liste est remplie si l'outil collecte des données relatives à au moins un paramètre associé à DB2. Les paramètres d'optimisation sont également consignés dans le fichier `perftune_stat.log`.
   b. Pour modifier les valeurs des paramètres de la base de données, cliquez sur **Optimiser les paramètres de base de données**. La fenêtre **Paramètres de base de données** s'ouvre.
   c. Dans la fenêtre **Paramètres de base de données**, vous pouvez indiquer les valeurs des paramètres de base de données suivants :
      1) Dans la zone **Pile de base de données**, entrez la taille maximale de la mémoire en pages à définir pour la pile de la base de données. La pile de base de données contient des informations de bloc de contrôle pour les tables, les index, les espaces table et les pools de mémoire tampon. Elle contient également la mémoire pour la mémoire tampon des journaux et la mémoire temporaire employée par les utilitaires.
      2) Dans la zone **Taille de la mémoire cache de package**, entrez la taille en pages de la mémoire destinée à la mise en cache des sections pour les instructions SQL et XQuery statiques et dynamiques sur une base de données.
      3) Dans la zone **Taille de mémoire tampon de journal**, entrez la taille en pages de la mémoire tampon à allouer aux enregistrements des journaux. Vous devez indiquer la taille de la pile de base de données à utiliser en tant que mémoire tampon pour les enregistrements des journaux.
      4) Dans la zone **Nombre maximal de fichiers de base de données ouverts par application**, entrez le nombre maximal de descripteurs de fichier pouvant être ouverts pour chaque agent de base de données.
      5) Dans la zone **Seuil de pages modifié**, entrez le pourcentage de pages modifiées.
      6) Dans la zone **Taille de pile de tri**, entrez la taille maximale de la pile de tri, en pages. La pile de tri peut être utilisée comme des pages de mémoire privée pour les tris privés, ou comme des pages de mémoire partagée pour des tris partagés.
      7) Dans la zone **Taille du fichier journal**, entrez la taille en Ko réservée aux fichiers journaux. Ce paramètre définit la taille de chaque fichier journal principal et secondaire.
      8) Dans la zone **Chemin d'accès du journal de base de données**, indiquez l'emplacement dans lequel vous voulez stocker les fichiers journaux. Vous pouvez cliquer sur **Parcourir** pour rechercher cet emplacement.
      9) Pour enregistrer les valeurs définies et les utiliser pour mettre à jour les paramètres de base de données, cliquez sur **OK**. Les valeurs par défaut sont définies pour les paramètres pour lesquels vous ne définissez pas de valeur.
5. Pour confirmer si vous voulez mettre à jour les paramètres de l'annuaire et de la base de données avec les valeurs d'optimisation, choisissez l'une des options ci-après.

- Pour mettre à jour l'instance de serveur d'annuaire avec les paramètres d'optimisation, cliquez sur **Oui, utiliser les valeurs recommandées pour la mise à jour des paramètres de configuration de l'annuaire et de la base de données**.
- Si vous ne souhaitez pas utiliser les paramètres d'optimisation, cliquez sur **Non, conserver les paramètres en cours. Aucun paramètre de configuration ne sera mis à jour.**.

6. Pour appliquer les modifications, cliquez sur **Terminer**.
7. Pour confirmer l'achèvement de la tâche, cliquez sur **OK**.
8. Vérifiez les journaux qui ont été générés lors de la mise à jour des paramètres d'optimisation.
9. Pour effacer leur contenu, cliquez sur **Effacer les résultats**.
10. Pour fermer la page **Optimiser les performances**, cliquez sur **Fermer**.
11. Pour fermer la fenêtre Outil de configuration, cliquez sur **Fichier** > **Quitter**.
12. Pour confirmer, cliquez sur **Oui**.

Configuration d'un serveur d'annuaire en vue de l'optimisation des performances à l'aide de l'utilitaire de ligne de commande

Utilisez l'utilitaire de ligne de commande **idsperftune** pour optimiser un serveur d'annuaire et améliorer les performances des opérations de recherche et de mise à jour.

Avant de commencer

Vous pouvez optimiser une instance de serveur d'annuaire si elle respecte les conditions ci-après.

- Une instance de serveur d'annuaire configurée avec une base de données DB2 doit exister. Voir «Configuration d'une base de données pour une instance à l'aide de l'utilitaire de ligne de commande», à la page 184.

Procédure

1. Connectez-vous en tant que propriétaire de l'instance de serveur d'annuaire.
2. Accédez à l'invite de commande.
3. Le répertoire de travail en cours doit être le sous-répertoire `sbin` du répertoire d'installation d'IBM Security Directory Server.
4. Pour optimiser un serveur d'annuaire et sa base de données, utilisez la commande **idsperftune**.
   - Pour effectuer une optimisation de base du serveur d'annuaire, exécutez la commande **idsperftune** avec la syntaxe ci-après.

     ```
     idsperftune -I nom_instance -i fichier_propriétés -B -u
     ```

     Le paramètre **-u** met à jour les paramètres de cache LDAP et de pool de mémoire tampon DB2 dans le serveur et la base de données. Si vous n'ajoutez pas le paramètre **-u**, les paramètres d'optimisation ne sont consignés que dans le fichier `perftune_stat.log`.
   - Pour extraire d'une instance et de la base de données associée le nombre d'entrées et leur taille moyenne, exécutez la commande **idsperftune** avec la syntaxe ci-après.

     ```
     idsperftune -I nom_instance -s
     ```
   - Pour effectuer une optimisation avancée du serveur d'annuaire, exécutez la commande **idsperftune** avec la syntaxe ci-après.

```
idsperftune -I nom_instance -i fichier_propriétés -A -m
```

Le paramètre **-m** active les inverseurs logiques du moniteur pour BUFFERPOOL et SORT. Pour obtenir des données exactes en vue de la meilleure optimisation possible de l'instance, exécutez la commande lorsque l'activité de l'annuaire est réellement représentative de votre environnement.

Pour plus d'informations sur la commande **idsperftune**, consultez le manuel *Command Reference*.

Gestion du journal des modifications d'une instance de serveur d'annuaire

Vous pouvez configurer la base de données des modifications pour enregistrer les modifications du schéma et des entrées d'annuaire d'une instance.

Le journal des modifications enregistre les opérations de mise à jour, telles que les ajouts (add), les suppressions (delete), les modifications (modify) et les modification du nom distinctif relatif (modrdn) réalisées dans une instance de serveur d'annuaire. Vous pouvez utiliser les utilitaires client pour restaurer les données du journal des modifications qui sont enregistrées lorsque des changements sont effectués dans la base de données du serveur d'annuaire.

Vous pouvez utiliser l'outil de configuration ou les utilitaires de ligne de commande pour activer ou désactiver la base de données du journal des modifications. Vous devez arrêter le serveur d'annuaire avant de configurer la base de données du journal des modifications ou d'annuler sa configuration.

Pour configurer le journal des modifications d'un serveur d'annuaire, utilisez la commande **idscfgchglg**. Pour annuler ce type de configuration, utilisez la commande **idsucfgchglg**. Vous ne pouvez pas configurer la base de données du journal des modifications d'une instance de serveur proxy.

Avant de configurer le journal des modifications d'une instance de serveur d'annuaire, vous devez vérifier que les conditions suivantes sont remplies :

1. Une instance DB2 portant le même nom que l'instance de serveur d'annuaires doit exister.
2. Vous devez configurer une base de données pour l'instance de serveur d'annuaire .
3. Sous AIX, Linux et Solaris, le service de bouclage local doit être enregistré dans le fichier /etc/services.

Lorsque vous configurez la base de données d'un journal des modifications, elle est créée dans la même instance de base de données que la base de données de l'instance de serveur d'annuaire. 30 Mo d'espace sur disque dur sont nécessaires pour la base de données du journal des modifications. Lorsque vous configurez le journal des modifications, l'entrée du journal est ajoutée au fichier de configuration de l'instance du serveur d'annuaire.

Configuration du journal des modifications à l'aide de l'Outil de configuration

Utilisez l'Outil de configuration pour configurer la base de données du journal des modifications d'une instance de serveur d'annuaire.

Avant de commencer

Pour configurer le journal des modifications d'une instance, l'instance doit respecter les conditions ci-après.

- Une instance de serveur d'annuaire configurée avec une base de données DB2 doit exister. Voir «Configuration d'une base de données d'instance à l'aide de l'outil de configuration», à la page 180.
- Arrêtez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide de l'outil de configuration», à la page 175.

Procédure

1. Démarrez l'outil de configuration pour l'instance. Voir «Démarrage de l'outil de configuration», à la page 174.
2. Dans la liste des tâches du panneau de navigation situé à gauche, cliquez sur **Gérer le journal des modifications**.
3. Dans la page **Gérer le journal des modifications**, procédez de la façon suivante :
   a. Pour configurer le journal des modifications, sélectionnez **Activer la base de données du journal des modifications**.
   b. Dans la zone **Nombre maximal d'entrées du journal**, cliquez sur le nombre maximum d'entrées que vous souhaitez enregistrer dans la base de données du journal des modifications.
      - Pour enregistrer un nombre illimité d'entrées dans le journal des modifications, cliquez sur **Sans limite**.
      - Pour enregistrer un nombre spécifique d'entrées, cliquez sur **Entrées** et indiquez le nombre d'entrées. Le nombre d'entrées par défaut est 1 000 000.
   c. Dans la zone **Age maximal**, cliquez sur le nombre maximum de durées pour lesquelles vous souhaitez enregistrer des entrées dans la base de données du journal des modifications.
      - Pour enregistrer les entrées dans le journal des modifications de façon indéfinie, cliquez sur **Sans limite**.
      - Pour enregistrer les entrées pendant une durée précise, cliquez sur **Age** et entrez le nombre de jours et d'heures.
   d. Pour appliquer les modifications, cliquez sur **Mettre à jour**.
   e. Pour confirmer l'achèvement de la tâche, cliquez sur **OK**.
   f. Vérifiez les journaux qui sont générés lors de la configuration de la base de données du journal des modifications.
   g. Pour effacer leur contenu, cliquez sur **Effacer les résultats**.
   h. Pour fermer la page **Gérer le journal des modifications**, cliquez sur **Fermer**.
4. Pour fermer la fenêtre Outil de configuration, cliquez sur **Fichier** > **Quitter**.
5. Pour confirmer, cliquez sur **Oui**.

Que faire ensuite

Démarrez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide de l'outil de configuration», à la page 175.

Configuration du journal des modifications à l'aide de l'utilitaire de ligne de commande

Utilisez l'utilitaire de ligne de commande **idscfgchglg** pour annuler la configuration de la base de données du journal des modifications d'une instance de serveur d'annuaire.

Avant de commencer

Pour configurer le journal des modifications d'une instance, l'instance respecte les conditions ci-après.

- Une instance de serveur d'annuaire configurée avec une base de données DB2 doit exister. Voir «Configuration d'une base de données pour une instance à l'aide de l'utilitaire de ligne de commande», à la page 184.
- Arrêtez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide des utilitaires de ligne de commande», à la page 163.

Procédure

1. Connectez-vous en tant que propriétaire de l'instance de serveur d'annuaire.
2. Accédez à l'invite de commande.
3. Le répertoire de travail en cours doit être le sous-répertoire `sbin` du répertoire d'installation d'IBM Security Directory Server.
4. Pour configurer le journal des modifications de l'instance d'un serveur d'annuaire, utilisez la commande **idscfgchglg**.
   - Pour configurer le journal des modifications de l'instance sans limite d'âge, exécutez la commande **idscfgchglg** :

     ```
     idscfgchglg -I nom_instance -m 0
     ```

   - Pour configurer le journal des modifications d'une instance avec une limite de taille de 1 000 000 et une limite d'âge de 25 heures, exécutez la commande **idscfgchglg** :

     ```
     idscfgchglg -I nom_instance -m 1000000 -y 1 -h 1
     ```

   Pour plus d'informations sur la commande **idscfgchglg**, consultez le *Guide des commandes*.

Que faire ensuite

Démarrez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide des utilitaires de ligne de commande», à la page 163.

Annulation de la configuration du journal des modification à l'aide de l'outil de configuration

Utilisez l'outil de configuration pour annuler la configuration de la base de données du journal des modifications d'une instance de serveur d'annuaire.

Avant de commencer

Vous pouvez annuler la configuration du journal des modifications d'une instance si l'instance respecte les conditions ci-après.

- Le journal des modifications de l'instance doit être configuré. Voir «Configuration du journal des modifications à l'aide de l'Outil de configuration», à la page 205.
- Arrêtez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide de l'outil de configuration», à la page 175.

Procédure

1. Démarrez l'outil de configuration pour l'instance. Voir «Démarrage de l'outil de configuration», à la page 174.
2. Dans la liste des tâches du panneau de navigation situé à gauche, cliquez sur **Gérer le journal des modifications**.
3. Dans la page **Gérer le journal des modifications**, procédez de la façon suivante :
   a. Pour annuler la configuration du journal des modifications, désélectionnez **Activer la base de données du journal des modifications**.
   b. Pour appliquer les modifications, cliquez sur **Mettre à jour**.
   c. Dans la fenêtre **Gérer le journal des modifications**, cliquez sur **Oui** pour confirmer la suppression de l'instance.
   d. Vérifiez les journaux qui ont été générés lors de l'annulation de la configuration du journal des modifications.
   e. Pour effacer leur contenu, cliquez sur **Effacer les résultats**.
   f. Pour fermer la page **Gérer le journal des modifications**, cliquez sur **Fermer**.
4. Pour fermer la fenêtre Outil de configuration, cliquez sur **Fichier** > **Quitter**.
5. Pour confirmer, cliquez sur **Oui**.

Que faire ensuite

Démarrez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide de l'outil de configuration», à la page 175.

Annulation de la configuration du journal des modification à l'aide de l'utilitaire de ligne de commande

Utilisez l'utilitaire de ligne de commande **idsucfgchglg** pour annuler la configuration de la base de données du journal des modifications d'une instance de serveur d'annuaire.

Avant de commencer

Vous pouvez annuler la configuration du journal des modifications d'une instance si l'instance respecte les conditions ci-après.

- Le journal des modifications de l'instance doit être configuré. Voir «Configuration du journal des modifications à l'aide de l'utilitaire de ligne de commande», à la page 207.
- Arrêtez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide des utilitaires de ligne de commande», à la page 163.

Procédure

1. Connectez-vous en tant que propriétaire de l'instance de serveur d'annuaire.
2. Accédez à l'invite de commande.

3. Le répertoire de travail en cours doit être le sous-répertoire `sbin` du répertoire d'installation d'IBM Security Directory Server.
4. Pour annuler la configuration du jouranl des modifications de l'instance de serveur d'annuaire, entrez la commande **idsucfgchglg** avec la syntaxe ci-après.

   ```
   idsucfgchglg -I nom_instance
   ```

   Pour plus d'informations sur la commande **idsucfgchglg**, consultez le manuel *Command Reference*.

Que faire ensuite

Démarrez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide des utilitaires de ligne de commande», à la page 163.

Configuration des suffixes

Pour créer une hiérarchie d'annuaire, vous devez configurer le suffixe requis pour l'instance de serveur d'annuaire.

Un suffixe est appelé un contexte d'affectation de nom. Il s'agit d'un nom distinctif (DN) qui identifie la première entrée d'une arborescence d'annuaire. LDAP utilise un schéma d'affectation de nom relatif. Le nom distinctif est également le suffixe de chaque entrée au sein de la hiérarchie d'annuaire. Dans un serveur d'annuaire, vous pouvez ajouter plusieurs suffixes, chacun identifiant une hiérarchie d'annuaire. Lorsque vous ajoutez un suffixe, l'entrée est ajoutée au fichier de configuration d'une instance de serveur d'annuaire. L'exemple suivant montre une entrée de suffixe, `o=sample`.

Vous pouvez ajouter l'outil de configuration pour ajouter ou supprimer des suffixes. Vous pouvez également utiliser la commande **idscfgsuf** pour ajouter des suffixes, et la commande **idsucfgsuf** pour en supprimer. Vous devez arrêter le serveur d'annuaire avant d'ajouter ou de retirer des suffixes. Pour plus d'informations sur les commandes **idscfgsuf** et **idsucfgsuf**, voir le manuel *Command Reference*.

Dans une instance de serveur d'annuaire, les suffixes définis par le système ne peuvent pas être supprimés. Ces suffixes ne sont pas disponibles dans les instances de serveur proxy. Les suffixes suivants sont définis par le système :

- `cn=localhost`
- `cn=configuration`
- `cn=ibmpolicies`
- `cn=Deleted Objects`

Lorsque vous ajoutez des entrées à un serveur d'annuaire, vous devez prendre en compte les points suivants :

- Vous devez ajouter une entrée de suffixe dans un serveur d'annuaire pour un nom distinctif de suffixe.
- Un nom distinctif d'entrée que vous ajoutez à un serveur d'annuaire doit contenir un suffixe qui correspond au nom distinctif du suffixe. L'exemple suivant montre une entrée avec un nom distinctif de suffixe : `ou=Marketing,o=sample`.

- Vous ne pouvez pas ajouter une entrée dans une instance de serveur proxy, ou dans un serveur d'annuaire qui n'est pas configuré avec une base de données DB2.

Si une requête contient un suffixe ne correspondant à aucun des suffixes configurés pour la base de données locale, la requête est renvoyée au serveur LDAP identifié pour le renvoi par défaut. Si aucun renvoi LDAP par défaut n'est défini, le message suivant est généré : `Object does not exist`.

Ajout d'un suffixe avec l'Outil de configuration

Utilisez l'Outil de configuration pour ajouter un suffixe à une instance.

Avant de commencer

Pour ajouter un suffixe à une instance, procédez comme suit.

- Arrêtez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide de l'outil de configuration», à la page 175.

Pourquoi et quand exécuter cette tâche

Lorsque vous ajoutez un suffixe à une instance, l'entrée du suffixe est ajoutée au fichier de configuration d'une instance.

Procédure

1. Démarrez l'outil de configuration pour l'instance. Voir «Démarrage de l'outil de configuration», à la page 174.
2. Dans la liste des tâches du panneau de navigation situé à gauche, cliquez sur **Gérer les suffixes**.
3. Dans la page **Gérer les suffixes**, procédez comme suit.
   a. Dans la zone DN de suffixe, entrez le suffixe à ajouter à l'instance.
   b. Cliquez sur **Ajouter**.
   c. Pour appliquer les modifications, cliquez sur **OK**.
4. Pour fermer la fenêtre Outil de configuration, cliquez sur **Fichier** > **Quitter**.
5. Pour confirmer, cliquez sur **Oui**.

Que faire ensuite

Démarrez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide de l'outil de configuration», à la page 175.

Ajout d'un suffixe à l'aide de l'utilitaire de ligne de commande

Utilisez l'utilitaire de ligne de commande **idscfgsuf** pour ajouter un suffixe à une instance.

Avant de commencer

Pour ajouter un suffixe à une instance, procédez comme suit.

- Arrêtez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide des utilitaires de ligne de commande», à la page 163.

Pourquoi et quand exécuter cette tâche

Lorsque vous ajoutez un suffixe à une instance, l'entrée du suffixe est ajoutée au fichier de configuration d'une instance.

Procédure

1. Connectez-vous en tant que propriétaire de l'instance de serveur d'annuaire.
2. Accédez à l'invite de commande.
3. Le répertoire de travail en cours doit être le sous-répertoire `sbin` du répertoire d'installation d'IBM Security Directory Server.
4. Pour ajouter le suffixe `o=sample` à une instance, exécutez la commande **`idscfgsuf`** dans le format suivant :

   ```
   idscfgsuf -I nom_instance -s "o=sample"
   ```

   Pour plus d'informations sur la commande **`idscfgsuf`**, consultez le manuel *Guide des commandes*.

Que faire ensuite

Démarrez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide des utilitaires de ligne de commande», à la page 163.

Suppression d'un suffixe avec l'Outil de configuration

Utilisez l'outil de configuration pour supprimer un suffixe d'une instance de serveur d'annuaire.

Avant de commencer

Pour supprimer un suffixe d'une instance de serveur d'annuaire, procédez comme suit.

- Arrêtez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide de l'outil de configuration», à la page 175.

Pourquoi et quand exécuter cette tâche

Lorsque vous supprimez un suffixe d'une instance, l'entrée du suffixe est supprimée du fichier de configuration d'une instance.

Procédure

1. Démarrez l'outil de configuration pour l'instance. Voir «Démarrage de l'outil de configuration», à la page 174.
2. Dans la liste des tâches du panneau de navigation situé à gauche, cliquez sur **Gérer les suffixes**.
3. Dans la page **Gérer les suffixes**, procédez comme suit.
   a. Dans la liste des **Noms distinctifs de suffixe actuels**, sélectionnez le suffixe à supprimer. Pour un serveur d'annuaire complet, vous ne pouvez pas supprimer les suffixes suivants définis par le système :
      - `cn=localhost`
      - `cn=configuration`
      - `cn=ibmpolicies`

- `cn=Deleted Objects`

b. Cliquez sur **Supprimer**.
c. Dans la fenêtre de confirmation **Gérer des suffixes**, cliquez sur **OK**.
d. Pour appliquer les modifications, cliquez sur **OK**.

4. Pour fermer la fenêtre Outil de configuration, cliquez sur **Fichier** > **Quitter**.
5. Pour confirmer, cliquez sur **Oui**.

Que faire ensuite

Démarrez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide de l'outil de configuration», à la page 175.

Suppression d'un suffixe à l'aide de l'utilitaire de ligne de commande

Utilisez l'utilitaire de ligne de commande **idsucfgsuf** pour supprimer un suffixe d'une instance.

Avant de commencer

Pour supprimer un suffixe d'une instance, procédez comme suit.

- Arrêtez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide de l'outil de configuration», à la page 175.

Pourquoi et quand exécuter cette tâche

Lorsque vous supprimez un suffixe d'une instance, l'entrée du suffixe est supprimée du fichier de configuration d'une instance. Pour un serveur d'annuaire complet, vous ne pouvez pas supprimer les suffixes suivants définis par le système :

- `cn=localhost`
- `cn=configuration`
- `cn=ibmpolicies`
- `cn=Deleted Objects`

Procédure

1. Connectez-vous en tant que propriétaire de l'instance de serveur d'annuaire.
2. Accédez à l'invite de commande.
3. Le répertoire de travail en cours doit être le sous-répertoire `sbin` du répertoire d'installation d'IBM Security Directory Server.
4. Pour supprimer le suffixe `o=sample` d'une instance, exécutez la commande **idsucfgsuf** :

   ```
   idsucfgsuf -I nom_instance -s "o=sample"
   ```

   Pour plus d'informations sur la commande **idsucfgsuf**, consultez le manuel *Guide des commandes*.

Que faire ensuite

Démarrez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide des utilitaires de ligne de commande», à la page 163.

Gérer les schémas

Pour qu'une instance prenne en charge des classes d'objets personnalisées, vous devez créer un fichier de schéma qui définit ces classes d'objets et leurs attributs.

Vous pouvez utiliser l'outil de configuration ou les utilitaires de ligne de commande, par exemple **idscfgsch** ou **idsucfgsch**, pour gérer les fichier de schéma. Les fichiers de schéma doivent être disponibles sur l'ordinateur. Pour plus d'informations sur les commandes **idscfgsch** et **idsucfgsch**, voir le manuel *Command Reference*.

Vous devez arrêter le serveur d'annuaire avant d'ajouter ou de retirer des fichiers de schéma.

Lorsque vous ajoutez ou supprimez des fichiers de schéma, le fichier de configuration de l'instance est mis à jour. Les opérations de gestion du schéma sont celles ci-après.

- Ajouter un fichier de schéma à la liste des fichiers de schéma qui sont chargés au démarrage du serveur
- Ajouter un fichier de schéma à la liste des fichiers de schéma qui est mise à jour au démarrage du serveur
- Modifier le type de contrôle de validation qui est effectué pour les fichiers schéma

Les fichiers de schéma suivants sont définis par le système. Vous ne pouvez pas les supprimer :

- `V3.config.at`
- `V3.config.oc`
- `V3.ibm.at`
- `V3.ibm.oc`
- `V3.system.at`
- `V3.system.oc`
- `V3.user.at`
- `V3.user.oc`
- `V3.ldapsyntaxes`
- `V3.matchingrules`
- `V3.modifiedschema`

Vous pouvez également utiliser l'outil de configuration pour définir la règle de validation du schéma qui contrôle la bonne adhésion des entrées au schéma. Par défaut, la règle de validation du schéma est `Version 3 (modérée)`. Les règles de validation suivantes sont prises en charge par un serveur d'annuaire :

Version 3 (stricte)
Le serveur effectue sur les entrées un contrôle de validation LDAP de type version 3 stricte. Avec ce type de validation, toutes les classes d'objets parent doivent exister au moment de l'ajout des entrées.

Version 3 (modérée)
Le serveur effectue sur les entrées un contrôle de validation LDAP de type version 3 modérée. Avec ce type de validation, il n'est pas nécessaire que toutes les classes d'objets parent existent au moment de l'ajout des entrées. La validation LDAP version 3 modérée est la règle de validation par défaut du schéma.

Version 2
Le serveur effectue sur les entrées un contrôle de validation LDAP de type version 2.

Aucune
Le serveur n'effectue pas de contrôle de validation.

Gestion d'un fichier schéma à l'aide de l'outil de

Utilisez l'outil de configuration pour gérer les fichiers schéma d'une instance.

Avant de commencer

Pour gérer les fichiers de schéma d'une instance, effectuez les opérations ci-après.

- Arrêtez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide de l'outil de configuration», à la page 175.

Pourquoi et quand exécuter cette tâche

Lorsque vous ajoutez ou supprimez un fichier de schéma, l'entrée du fichier est mise à jour dans le fichier de configuration de l'instance.

Procédure

1. Démarrez l'outil de configuration pour l'instance. Voir «Démarrage de l'outil de configuration», à la page 174.
2. Dans la liste des tâches du panneau de navigation situé à gauche, cliquez sur **Gérer des fichiers schéma**.
3. Dans la page **Gérer des fichiers schéma**, choisissez l'opération à effectuer.
   - Pour ajouter un fichier schéma dans le fichier de configuration d'une instance, procédez comme suit.
     a. Dans la zone **Chemin d'accès et nom du fichier**, entrez le nom du fichier schéma avec son chemin. Vous pouvez également cliquer sur **Parcourir** pour entrer le nom et l'emplacement du fichier schéma.
     b. Cliquez sur **Ajouter**.
   - Pour supprimer un fichier schéma dans le fichier de configuration d'une instance, procédez comme suit.
     a. Dans la liste des **fichiers schéma en cours**, sélectionnez le nom de fichier schéma à supprimer.
     b. Cliquez sur **Supprimer**.
     c. Dans la fenêtre de confirmation **Gérer des fichiers schéma**, cliquez sur **OK**.
4. Pour appliquer les modifications, cliquez sur **OK**.
5. Pour fermer la fenêtre Outil de configuration, cliquez sur **Fichier** > **Quitter**.
6. Pour confirmer, cliquez sur **Oui**.

Que faire ensuite

Démarrez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide de l'outil de configuration», à la page 175.

Gestion d'un fichier de schéma à l'aide de l'utilitaire de ligne de commande

Utilisez les utilitaires de ligne de commande pour gérer les fichiers de schéma d'une instance de serveur d'annuaire.

Avant de commencer

Pour gérer les fichiers de schéma d'une instance, effectuez les opérations ci-après.

- Arrêtez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide des utilitaires de ligne de commande», à la page 163.

Pourquoi et quand exécuter cette tâche

Lorsque vous ajoutez ou supprimez un fichier de schéma, l'entrée du fichier est mise à jour dans le fichier de configuration de l'instance.

Procédure

1. Connectez-vous en tant que propriétaire de l'instance de serveur d'annuaire.
2. Accédez à l'invite de commande.
3. Le répertoire de travail en cours doit être le sous-répertoire `sbin` du répertoire d'installation d'IBM Security Directory Server.
4. Pour gérer le fichier de schéma d'une instance, choisissez l'opération à effectuer.
   - Pour ajouter un fichier de schéma à une instance, entrez la commande **idscfgsch** avec la syntaxe ci-après.

     ```
     idscfgsch -I nom_instance -s schema_file.oc
     ```

   - Pour supprimer un fichier de schéma dans une instance, entrez la commande **idsucfgsch** avec la syntaxe ci-après.

     ```
     idsucfgsch -I nom_instance -s schema_file.oc
     ```

   Pour plus d'informations sur les commandes **idscfgsch** et **idsucfgsch**, voir le manuel *Command Reference*.

Que faire ensuite

Démarrez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide des utilitaires de ligne de commande», à la page 163.

Configuration de la validation du schéma à l'aide de l'outil de configuration

Utilisez l'outil de configuration pour configurer la validation du schéma d'une instance.

Avant de commencer

Pour configurer les règles de validation du schéma d'une instance, effectuez les opérations ci-après.

- Arrêtez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide de l'outil de configuration», à la page 175.

Pourquoi et quand exécuter cette tâche

Lorsque vous configurez la validation du schéma d'une instance, la valeur est mise à jour dans le fichier de configuration de l'instance.

Procédure

1. Démarrez l'outil de configuration pour l'instance. Voir «Démarrage de l'outil de configuration», à la page 174.
2. Dans la liste des tâches du panneau de navigation situé à gauche, cliquez sur **Gérer des fichiers schéma**.
3. Sous la zone **Règles de validation de schéma** de la page **Gérer des fichiers schéma**, sélectionnez l'une des règles de validation de schéma suivante pour la configurer :
   - Pour configurer le contrôle de validation LDAP version 3 stricte, cliquez sur **Version 3 (stricte)**.
   - Pour configurer le contrôle de validation LDAP version 3 modérée, cliquez sur **Version 3 (modérée)**.
   - Pour configurer le contrôle de validation LDAP version 2, cliquez sur **Version 2**.
   - Pour configurer le contrôle LDAP version 2, cliquez sur **Aucun**.
4. Pour appliquer les modifications, cliquez sur **OK**.
5. Pour fermer la fenêtre Outil de configuration, cliquez sur **Fichier** > **Quitter**.
6. Pour confirmer, cliquez sur **Oui**.

Que faire ensuite

Démarrez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide de l'outil de configuration», à la page 175.

Gestion des données LDIF

Pour utiliser des données d'annuaire, vous devez les ajouter à une instance de serveur d'annuaire à partir d'une instance existante ou d'un fichier LDIF (LDAP Data Interchange Format).

Vous pouvez utiliser l'outil de configuration pour importer des données à partir d'un fichier LDIF ou pour exporter des données de la base de données vers un fichier LDIF. LDIF permet de représenter les entrées LDAP au format texte. L'importation permet d'ajouter des entrées à une base de données d'annuaire vide ou à une base de données contenant déjà des entrées. Vous pouvez également utiliser l'outil de configuration pour valider les données du fichier LDIF sans les ajouter à l'annuaire.

Vous pouvez ajouter des données à une instance qui est configurée avec une base de données DB2. Vous ne devez pas ajouter des données à une instance de serveur proxy, car cette opération n'est pas prise en charge.

Si vous souhaitez importer des données LDIF en provenance d'une autre instance de serveur, vous devez synchroniser le chiffrement des instances. Vous devez

synchroniser la cryptographie bidirectionnelle entre les instances de serveur d'annuaire pour réduire le temps nécessaire au chiffrement et au déchiffrement des données pendant les communications avec le serveur. Lorsque vous importez des données dont le chiffrement n'est pas synchronisé, les entrées du fichier chiffrées AES ne sont pas importées. Pour plus d'informations sur la synchronisation de la cryptographie bidirectionnelle, consultez le manuel *Command Reference*.

Si le chiffrement des instances de serveur n'est pas synchronisé, indiquez la valeur de départ et le sel de chiffrement du serveur cible lorsque vous exportez un fichier LDIF depuis le serveur source. Les données chiffrées AES sont déchiffrées à l'aide des clés AES du serveur source, puis chiffrées à l'aide de la valeur de départ et du sel de chiffrement du serveur cible. Ces données chiffrées sont stockées dans le fichier LDIF.

Avant d'importer des données, vous devez vérifier que les conditions ci-après sont remplies.

- L'importation ou l'exportation des données LDIF n'est pas prise en charge pour une instance de serveur proxy ou une instance qui n'est pas configurée avec une base de données DB2.
- Ajoutez les suffixes requis au serveur cible dans lequel vous voulez importer des données. Voir «Configuration des suffixes», à la page 209.
- Vous devez arrêter le serveur cible dans lequel vous voulez importer les données.

Après le chargement de grandes quantités de données, par exemple lors du remplissage de la base de données avec **idsbulkload**, vous devez optimiser la base de données. Cette opération peut améliorer ses performances.

Vous pouvez également utiliser la ligne de commande pour importer, exporter ou valider des données LDIF :

- Pour importer des données à partir d'un fichier LDIF, utilisez l'utilitaire **idsldif2db** ou l'utilitaire **idsbulkload**.
- Pour exporter des données vers un fichier LDIF, utilisez l'utilitaire **idsdb2ldif**.
- Pour valider les données du fichier LDIF, utilisez l'utilitaire **idsbulkload**.

Pour plus d'informations sur les utilitaires de ligne de commande, consultez le manuel *Command Reference*.

Exemples

Pour connaître la valeur du sel de chiffrement d'un serveur, lancez la commande **idsldapsearch** avec la syntaxe ci-après.

```
idsldapsearch -h nom_hôte -p port -D DN_admin -w mdp_admin \
 -b "cn=crypto,cn=localhost" objectclass=* ibm-slapdCryptoSalt

ibm-slapdCryptoSalt=:SxaQ+.qdKor
```

La chaîne située après le signe égal (=) dans l'attribut `ibm-slapdCryptoSalt` correspond au sel de chiffrement. Dans l'exemple, `:SxaQ+.qdKor` est le sel de chiffrement.

Importation des données LDIF à l'aide de l'outil de configuration

Utilisez l'outil de configuration pour importer des données dans une instance de serveur d'annuaire à partir d'un fichier LDIF.

Avant de commencer

Vous pouvez importer les données d'un fichier LDIF dans une instance si l'instance respecte les conditions ci-après.

- Une instance de serveur d'annuaire configurée avec une base de données DB2 doit exister. Voir «Configuration d'une base de données d'instance à l'aide de l'outil de configuration», à la page 180.
- Les entrées de suffixe requises doivent être configurées. Voir «Ajout d'un suffixe avec l'Outil de configuration», à la page 210.
- Arrêtez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide de l'outil de configuration», à la page 175.

Procédure

1. Démarrez l'outil de configuration pour l'instance. Voir «Démarrage de l'outil de configuration», à la page 174.
2. Dans la liste des tâches du panneau de navigation situé à gauche, cliquez sur **Tâches LDIF** > **Importer des données LDIF**.
3. Dans la page **Importer des données LDIF**, procédez de la façon suivante :
   a. Dans la zone **Chemin d'accès et nom du fichier LDIF**, entrez le chemin et le nom du fichier LDIF à partir duquel vous voulez importer des données. Vous pouvez également cliquer sur **Parcourir** pour entrer le nom et le fichier du fichier LDIF.
   b. Si vous souhaitez supprimer les espaces de fin de ligne dans les données, sélectionnez **Supprimer les espaces de fin de ligne en Importation standard ou Bulkload**.
   c. En fonction du nombre d'entrées à importer, sélectionnez une option :
      - Pour importer les données à l'aide de l'utilitaire **idsldif2db**, cliquez sur **Importation standard**. Utilisez cette option si le fichier LDIF contient peu d'entrées.
      - Pour importer les données à l'aide de l'utilitaire **idsbulkload**, cliquez sur **Bulkload**. Lorsque le fichier LDIF contient un grand nombre d'entrées, l'utilitaire **idsbulkload** importe les données plus rapidement que l'utilitaire **idsldif2db**.
   d. Si vous avez sélectionné l'option **Bulkload** pour importer les données, indiquez les étapes de validation à appliquer aux données LDIF :
      1) Pour vérifier si les données LDIF sont conformes au schéma, sélectionnez **Activer la vérification des schémas**.
      2) Pour vérifier si les données LDIF contiennent les listes de contrôle d'accès appropriées, sélectionnez **Activer la vérification des ACL**.
   e. Pour démarrer l'importation, cliquez sur **Importer**.
   f. Pour confirmer l'achèvement de la tâche, cliquez sur **OK**.
   g. Vérifiez les journaux qui ont été générés lors de l'importation des données LDIF.
   h. Pour effacer leur contenu, cliquez sur **Effacer les résultats**.

i. Pour fermer la page **Importer des données LDIF**, cliquez sur **Fermer**.

4. Pour fermer la fenêtre Outil de configuration, cliquez sur **Fichier** > **Quitter**.
5. Pour confirmer, cliquez sur **Oui**.

Que faire ensuite

Démarrez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide de l'outil de configuration», à la page 175. Après le chargement de grandes quantités de données, par exemple lors du remplissage de la base de données avec **idsbulkload**, vous devez optimiser la base de données. Pour plus d'informations sur l'optimisation de la base de données, consultez «Optimisation de la base de données avec l'Outil de configuration», à la page 191.

Validation des données LDIF à l'aide de l'outil de configuration

Utilisez l'outil de configuration pour valider un fichier LDIF par rapport au schéma du serveur d'annuaire sans ajouter ses données à la base de données.

Avant de commencer

Pour valider les données d'un fichier LDIF par rapport au schéma du serveur d'annuaire, l'instance doit respecter les conditions ci-après.

- Une instance de serveur d'annuaire configurée avec une base de données DB2 doit exister. Voir «Configuration d'une base de données d'instance à l'aide de l'outil de configuration», à la page 180.
- Arrêtez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide de l'outil de configuration», à la page 175.

Procédure

1. Démarrez l'outil de configuration pour l'instance. Voir «Démarrage de l'outil de configuration», à la page 174.
2. Dans la liste des tâches du panneau de navigation situé à gauche, cliquez sur **Tâches LDIF** > **Importer des données LDIF**.
3. Dans la page **Importer des données LDIF**, procédez de la façon suivante :
   a. Dans la zone **Chemin d'accès et nom du fichier LDIF**, entrez le chemin et le nom du fichier LDIF à partir duquel vous voulez importer des données. Vous pouvez également cliquer sur **Parcourir** pour entrer le nom et le fichier du fichier LDIF.
   b. Cliquez sur **Validation des données uniquement**.
   c. Pour démarrer la validation de données, cliquez sur **Importer**.
   d. Pour confirmer l'achèvement de la tâche, cliquez sur **OK**.
   e. Vérifiez les journaux qui ont été générés lors de la validation des données.
   f. Pour effacer leur contenu, cliquez sur **Effacer les résultats**.
   g. Pour fermer la page **Importer des données LDIF**, cliquez sur **Fermer**.
4. Pour fermer la fenêtre Outil de configuration, cliquez sur **Fichier** > **Quitter**.
5. Pour confirmer, cliquez sur **Oui**.

Que faire ensuite

Démarrez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide de l'outil de configuration», à la page 175.

Exportation des données LDIF à l'aide de l'outil de configuration

Utilisez l'outil de configuration pour exporter directement les données d'une instance vers un fichier LDIF.

Avant de commencer

Vous pouvez exporter les données d'une instance dans un fichier LDIF si l'instance respecte les conditions ci-après.

- Une instance de serveur d'annuaire configurée avec une base de données DB2 doit exister. Voir «Configuration d'une base de données d'instance à l'aide de l'outil de configuration», à la page 180.
- L'instance doit contenir des entrées d'annuaire.

Procédure

1. Démarrez l'outil de configuration pour l'instance. Voir «Démarrage de l'outil de configuration», à la page 174.
2. Dans la liste des tâches du panneau de navigation situé à gauche, cliquez sur **Tâches LDIF** > **Exporter des données LDIF**.
3. Dans la page **Exporter des données LDIF**, procédez de la façon suivante :
   a. Dans la zone **Chemin d'accès et nom du fichier LDIF**, entrez le chemin et le nom du fichier LDIF dans lequel vous voulez exporter les données. Vous pouvez également cliquer sur **Parcourir** pour entrer le nom et le fichier du fichier LDIF.
   b. Si le fichier existe et si vous voulez remplacer les données qu'il contient, sélectionnez **Ecraser si le fichier existe**.
   c. Si vous souhaitez exporter les attributs opérationnels, `creatorsName`, `createTimestamp`, `modifiersName` et `modifyTimestamp`, sélectionnez **Exporter des attributs opérationnels**. Les attributs opérationnels sont créés et modifiés par le serveur lorsqu'une entrée d'annuaire est créée ou modifiée. Ils contiennent des informations sur l'utilisateur qui a créé ou modifié l'entrée, et sur l'heure à laquelle l'entrée a été créée ou modifiée. Les entrées sont stockées dans le fichier LDIF sous forme de contrôles codés en base 64.
   d. Pour importer des données dans un serveur de destination AES (Advanced Encryption Standard) si le chiffrement du serveur n'est pas synchronisé avec celui du serveur source, sélectionnez **Exporter les données pour le serveur de destination AES**.
   e. Pour exporter les entrées supprimées mais encore stockées dans la sous-arborescence des tombstones, sélectionnez **Exporter les entrées supprimées**. Pour plus d'informations sur la sous-arborescence de tombstones, voir la section Administration de la documentation IBM Security Directory Server.
   f. Si vous avez sélectionné **Exporter les données pour le serveur de destination AES**, entrez les valeurs ci-après.
      - Dans la zone **Valeur de départ de chiffrement**, entrez la valeur de départ de chiffrement du serveur de destination.

- Dans la zone **Sel de chiffrement**, entrez le sel de chiffrement du serveur de destination. Pour plus d'informations sur la manière de connaître le sel de chiffrement, voir «Gestion des données LDIF», à la page 216.

g. Pour définir un filtre pour les entrées qui sont exportées dans un fichier LDIF, entrez le nom distinctif d'un filtre de réplication valide dans la zone **DN de l'entrée du filtre**. Le filtre exporte les entrées de la base de données qui correspondent aux critères du filtre LDIF. Pour plus d'informations sur les filtres de replication, voir la section Administration de la documentation IBM Security Directory Server.

h. Si vous souhaitez ajouter des commentaires au fichier LDIF, entrez-les dans la zone **Commentaires**.

i. Pour exporter les entrées d'une sous-arborescence spécifique, entrez son nom distinctif dans la zone **DN de la sous-arborescence**. Le nom distinctif de la sous-arborescence identifie la première entrée de la sous-arborescence à enregistrer dans le fichier LDIF. La sous-arborescence, et toutes les entrées qu'elle contient dans la hiérarchie d'annuaire, sont enregistrées dans le fichier. Si vous ne spécifiez pas de nom distinctif de sous-arborescence, toutes les entrées d'annuaire stockées dans la base de données sont enregistrées dans le fichier de sortie. Les entrées sont identifiées en fonction des suffixes spécifiés dans le fichier de configuration de l'instance de serveur d'annuaire.

j. Pour démarrer l'exportation, cliquez sur **Exporter**.

k. Pour confirmer l'achèvement de la tâche, cliquez sur **OK**.

l. Vérifiez les journaux qui ont été générés lors de l'exportation des données LDIF.

m. Pour effacer leur contenu, cliquez sur **Effacer les résultats**.

n. Pour fermer la page **Exporter des données LDIF**, cliquez sur **Fermer**.

4. Pour fermer la fenêtre Outil de configuration, cliquez sur **Fichier** > **Quitter**.
5. Pour confirmer, cliquez sur **Oui**.

Synchronisation Active Directory

Vous pouvez synchroniser les entrées des conteneurs d'utilisateurs et de groupes d'un annuaire Microsoft Active Directory associé à une instance IBM Security Directory Server. La synchronisation des données se fait à sens unique, d'Active Directory vers une instance de serveur d'annuaire.

Remarque : Dans IBM Security Directory Server version 6.3.1, la solution de synchronisation d'Active Directory est obsolète. Utilisez la solution LDAPSync à la place.

Vous pouvez utiliser l'outil de configuration ou les utilitaires de ligne de commande, par exemple **idsadscfg** et **idsadsrun**, pour configurer et exécuter l'application de synchronisation d'Active Directory.

Remarque : La synchronisation des utilisateurs et des groupes depuis Active Directory vers une instance IBM Security Directory Server par l'intermédiaire du serveur proxy IBM Security Directory n'est pas prise en charge.

L'outil se synchronisation d'Active Directory utilise IBM Security Directory Integrator pour la synchronisation des conteneurs d'utilisateurs et de groupes. Vous devez installer IBM Security Directory Integrator avant d'utiliser l'outil de synchronisation d'Active Directory.

IBM Security Directory Integrator est nécessaire pour les actions suivantes :

- Exécuter la configuration
- Démarrer, arrêter et redémarrer les opérations de surveillance

Vous devez prendre en compte les éléments suivants lorsque vous configurez l'outil de synchronisation d'Active Directory :

- L'application de synchronisation d'Active Directory et IBM Security Directory Integrator doivent être sur le même ordinateur que l'instance du serveur d'annuaire.
- L'application de synchronisation d'Active Directory ne synchronise que les conteneurs d'utilisateurs et de groupes. L'outil ne synchronise pas les autres objets et conteneurs vers une instance de serveur d'annuaire.
- La solution vérifie aussi l'appartenance aux groupes des entrées d'utilisateur, et celles-ci sont ajoutées aux groupes de l'instance qui sont synchronisés avec Active Directory. Les entrées d'utilisateur existantes déplacées hors d'un conteneur sont supprimées de l'instance. Les entrées utilisateur sont également supprimées de tous les groupes de l'instance.
- L'application de synchronisation d'Active Directory ne permet pas de synchroniser les unités organisationnelles imbriquées (`ou`).
- Il est impossible de mapper plusieurs attributs Active Directory à un même attribut d'une instance de serveur d'annuaire.
- L'attribut `userpassword` d'Active Directory ne peut pas être mappé à une instance de serveur d'annuaire. Le mot de passe n'est pas synchronisé par cette solution.
- L'outil de synchronisation d'Active Directory permet de synchroniser des utilisateurs et des groupes d'un ou de plusieurs conteneurs Active Directory avec une unité organisationnelle (`ou`) d'un serveur d'annuaire. Cependant, l'outil ne peut pas synchroniser plusieurs conteneurs d'utilisateurs et de groupes Active Directory vers plusieurs unités organisationnelles (`ou`) d'un serveur d'annuaire.
- Vous pouvez indiquer plusieurs conteneurs d'utilisateurs en vue de leur synchronisation avec une unité organisationnelle (`ou`) d'un serveur d'annuaire en utilisant un point-virgule (`;`) comme séparateur. L'utilisation d'autres caractères comme séparateur ne sont pas pris en charge. Si vous utilisez le point-virgule (`;`) comme séparateur, insérez l'argument entre guillemets (`"`). L'exemple suivant montre l'utilisation d'un point-virgule comme (`;`) séparateur : `"ou=SWUGroups,dc=adsync,dc=com;ou=STGGroups,dc=adsync,dc=com"`.
- L'attribut `SAMAccountName` d'Active Directory sert à composer l'attribut `$dn` dans IBM Security Directory Server. Etant donné que l'attribut `SAMAccountName` est unique dans un domaine, aucun conflit n'a lieu lors de la synchronisation de plusieurs conteneurs d'utilisateurs Active Directory avec une unité organisationnelle d'un serveur d'annuaire.
- La solution prend en charge une connexion sécurisée avec Active Directory, mais pas avec une instance de serveur d'annuaire.
- Si vous modifiez le nom distinctif et/ou le mot de passe de l'administrateur d'une instance de serveur d'annuaire après avoir configuré l'application de synchronisation d'Active Directory, vous devez reconfigurer cette dernière.
- Si les conteneurs d'utilisateurs ou de groupes d'Active Directory sont modifiés pendant l'exécution de la fonction de synchronisation d'Active Directory, vous devez reconfigurer cette dernière avec les nouveaux noms. Faute de quoi, le programme de synchronisation d'Active Directory risque de ne pas fonctionner.

- Si vous modifiez les utilisateurs et les groupes IBM Security Directory Server en utilisant un autre outil que la fonction de synchronisation d'Active Directory, vous pouvez perturber le fonctionnement de celle-ci.

Configuration et exécution de la synchronisation Active Directory

Pour synchroniser les conteneurs d'utilisateurs et de groupes d'Active Directory avec une instance IBM Security Directory Server, vous devez configurer et exécuter la synchronisation Active Directory.

Avant de commencer

Pour configurer et exécuter la synchronisation Active Directory, vous devez installer les logiciels suivants :

- IBM Security Directory Server
- IBM Security Directory Integrator

Procédure

1. Si vous avez installé IBM Security Directory Integrator dans un chemin personnalisé, définissez ce chemin dans la variable d'environnement *IDS_LDAP_TDI_HOME*.

   Remarque : Sur les systèmes Windows, le chemin d'installation défini dans la variable d'environnement ne doit contenir ni espaces, ni guillemets. Dans le chemin, utilisez le nom abrégé.
   Le chemin d'installation par défaut d'IBM Security Directory Integrator est le suivant :

   AIX et Solaris
   `/opt/IBM/TDI/V7.1`

   Linux `/opt/ibm/TDI/V7.1`

   Windows
   `C:\Program Files\IBM\TDI\V7.1`
2. Facultatif : Charger les exemples de fichiers `users.ldif` et `groups.ldif` dans Active Directory.
3. Utilisez la commande **idsadscfg** pour configurer la synchronisation Active Directory. Vous pouvez aussi utiliser l'outil de configuration pour configurer la synchronisation Active Directory. La commande crée les fichiers `adsync_private.prop` et `adsync_public.prop`.
4. Modifiez le fichier `adsync_public.prop` pour personnaliser des attributs facultatifs et des paramètres SSL, si nécessaire. Pour plus d'informations sur les fichiers et sur la communication sécurisée, voir la section *Administration* de la documentation IBM Security Directory Server.
5. Utilisez la commande **idsadsrun** pour démarrer la synchronisation Active Directory. Un message vous demande si vous souhaitez effectuer une synchronisation complète, suivie d'une synchronisation en temps réel ou si vous souhaitez lancer uniquement une synchronisation en temps réel. L'outil de synchronisation d'Active Directory identifie les modifications dans les entrées Active Directory, et les synchronise avec celles d'IBM Security Directory Server.
6. Facultatif : Exécutez la console d'administration et de surveillance d'IBM Security Directory Integrator pour administrer et surveiller la synchronisation.

Configuration de la synchronisation Active Directory à l'aide de l'outil de configuration

Utilisez l'outil de configuration pour configurer la synchronisation Active Directory avec une instance de serveur d'annuaire.

Avant de commencer

Pour configurer la synchronisation Active Directory, vous devez vérifier que les conditions ci-après sont remplies.

- Installez IBM Security Directory Integrator.
- Arrêtez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide de l'outil de configuration», à la page 175.

Procédure

1. Démarrez l'outil de configuration pour l'instance. Voir «Démarrage de l'outil de configuration», à la page 174.
2. Dans la liste des tâches du panneau de navigation situé à gauche, cliquez sur **Synchroniser avec Active Directory**.
3. Dans la page **Synchroniser avec Active Directory : Détails de l'instance**, entrez les détails de la configuration pour l'instance IBM Security Directory Server. Les informations fournies sont sauvegardées dans les fichiers `adsync_private.properties` et `adsync_public.properties`. Les fichiers sont stockés dans le sous-répertoire `etc/tdisoldir` du répertoire de base de l'instance.
4. Dans la zone **Suffixe de l'annuaire**, entrez le suffixe de serveur d'annuaire que vous souhaitez utiliser pour la synchronisation Active Directory. La zone **Adresse URL LDAP** est renseignée avec l'adresse URL de l'instance de serveur d'annuaire. Vous ne pouvez pas modifier cette zone.
5. Dans la zone **Nom distinctif de l'entrée du conteneur de groupes**, entrez le nom distinctif d'un conteneur existant dans lequel vous souhaitez copier les groupes Active Directory. Les groupes et l'appartenance des utilisateurs aux groupes sont synchronisés entre Active Directory et IBM Security Directory Server. Lorsqu'un utilisateur est ajouté ou supprimé dans un groupe Active Directory, l'entrée est ajoutée ou supprimée dans le groupe correspondant de l'instance IBM Security Directory Server.
6. Dans la zone **Nom distinctif de l'entrée du conteneur d'utilisateurs**, entrez le nom distinctif d'un conteneur existant dans lequel vous souhaitez copier les utilisateurs Active Directory.
7. Si vous souhaitez utiliser une connexion SSL vers Active Directory, sélectionnez **Utiliser la connexion SSL vers Active Directory**. La connexion SSL à IBM Security Directory Server n'est pas prise en charge. Pour plus d'informations sur la procédure de configuration d'une connexion SSL à Active Directory, voir la section *Administration* de la documentation IBM Security Directory Server.
8. Cliquez sur **Suivant**. La page **Synchronisation avec Active Directory : Détails d'Active Directory** s'affiche.
9. Dans la zone **Adresse hôte**, entrez le nom d'hôte ou l'adresse IP du contrôleur de domaine d'Active Directory.
10. Dans la zone **Port hôte**, saisissez le port employé par Active Directory.
11. Dans la zone **Nom de connexion**, entrez le nom de connexion qui doit être utilisé par IBM Security Directory Integrator pour établir une connexion à

Active Directory. L'ID de connexion doit disposer des droits requis pour lire les entrées d'Active Directory qui doivent être propagées sur l'instance de serveur d'annuaire.

12. Dans la zone **Mot de passe de connexion**, entrez le mot de passe qui doit être utilisé par IBM Security Directory Integrator pour établir une connexion à Active Directory.
13. Dans la zone **Base de recherche**, saisissez la sous-arborescence d'Active Directory à partir de laquelle les modifications doivent être propagées à l'instance. Les modifications apportées aux entrées utilisateur dans la sous-arborescence sont propagées à l'instance de serveur d'annuaire. Pour propager tous les utilisateurs des groupes Active Directory à l'instance, définissez la base de recherche sur le haut de la hiérarchie d'Active Directory.
14. Dans la zone **Nom distinctif de l'entrée du conteneur de groupes**, entrez le nom distinctif du conteneur Active Directory à partir duquel vous voulez synchroniser les groupes avec l'instance.
15. Dans la zone **Nom distinctif de l'entrée du conteneur d'utilisateurs**, entrez le nom distinctif du conteneur Active Directory à partir duquel vous voulez synchroniser les entrées utilisateur avec l'instance.
16. Cliquez sur **Terminer**. La fenêtre **Synchronisation avec Active Directory : Résultats** s'affiche.
17. Vérifiez les messages d'erreur qui ont été générés par la configuration de la synchronisation Active Directory.
18. Pour effacer leur contenu, cliquez sur **Effacer les résultats**.
19. Pour fermer la page **Synchronisation avec Active Directory**, cliquez sur **Fermer**.
20. Pour fermer la fenêtre Outil de configuration, cliquez sur **Fichier** > **Quitter**.
21. Pour confirmer, cliquez sur **Oui**.

Configuration de la synchronisation Active Directory à l'aide de l'utilitaire de ligne de commande

Utilisez l'utilitaire de ligne de commande **idsadscfg** pour configurer la synchronisation Active Directory avec une instance de serveur d'annuaire.

Avant de commencer

Pour configurer la synchronisation Active Directory, vous devez vérifier que les conditions ci-après sont remplies.

- Installez IBM Security Directory Integrator.
- Arrêtez le serveur d'annuaire. Voir «Démarrage et arrêt d'un serveur d'annuaire et d'un serveur d'administration à l'aide des utilitaires de ligne de commande», à la page 163.

Procédure

1. Connectez-vous en tant qu'utilisateur root sous AIX, Linux ou Solaris, et en tant que membre du groupe des administrateurs sous Windows.
2. Accédez à l'invite de commande.
3. Le répertoire de travail en cours doit être le sous-répertoire `sbin` du répertoire d'installation d'IBM Security Directory Server.
4. Pour configurer la synchronisation Active Directory avec une instance, entrez la commande **idsadscfg** avec la syntaxe ci-après.

```
idsadscfg -I nom_instance -adH ldap://LDAP_server1:389 -adb dc=adsynctest,dc=com
-adD cn=administrator,cn=users,dc=adsynctest,dc=com -adw secret -adg ou=testgroup1,
dc=adsynctest,dc=com -adu ou=testuser1,dc=adsynctest,dc=com -idss o=sample -idsg
ou=Testgroup1,ou=groups,o=sample -idsu ou=Testuser1,ou=users,o=sample
```

Pour plus d'informations sur la commande **idsadscfg**, consultez le manuel *Command Reference*.

Que faire ensuite

Utilisez la commande **idsadsrun** pour démarrer la synchronisation Active Directory. Pour plus d'informations sur la commande **idsadsrun**, consultez le manuel *Command Reference*.

Chapitre 21. Démarrage automatique des instances de serveur d'annuaire au démarrage du système d'exploitation

Vous pouvez configurer le démarrage automatique des instances de serveur d'annuaire lorsqu'un ordinateur redémarre après qu'il a été arrêté en vue d'opérations de maintenance ou de mise à niveau.

Lorsque vous créez une instance de serveur d'annuaire, le serveur d'administration démarre si la création a réussi. Pour démarrer une serveur d'annuaire avec une base de données DB2, vous devez démarrer le pricessus `ibmslapd` ou `idsslapd` de l'instance.

Lorsque vous redémarrez un ordinateur, vous devez redémarrer à la fois le serveur d'administration et le processus `ibmslapd` qui est associé à l'instance. Cependant, vous pouvez configurer les services et les processus qui sont associés à une instance pour qu'ils démarrent automatiquement avec le système d'exploitation.

Sous AIX, Linux ou Solaris, pour faire démarrer l'instance de serveur d'annuaire en même temps que le système d'exploitation, vous devez entrer les informations relatives au serveur dans le fichier `/etc/inittab`. Le fichier `inittab` définit quels processus doivent démarrer au démarrage du système et fonctionnement normal. Vous devez ajouter une entrée pour le serveur d'annuaire dans le fichier `inittab`, au format suivant :

```
id:runlevels:action:process
```

Les attributs du fichier `inittab` ont besoin des valeurs ci-après.

ID Cet attribut définit un identificateur de 1 à 4 chiffres unique dans le fichier.

runlevels
L'attribut `runlevels` indique le mode `runlevel` du système d'exploitation dans lequel le processus doit démarrer automatiquement. Il se rapporte au mode de fonctionnement d'un système d'exploitation AIX, Linux ou Solaris. La configuration de l'attribut `runlevels` diffère selon les systèmes d'exploitation. Voir le manuel du système d'exploitation utilisé pour obtenir des informations détaillées sur la configuration de `runlevel`.

action L'attribut `action` définit le type de l'action.

process
L'attribut `process` définit le processus à démarrer.

Configuration du démarrage automatique d'une instance de serveur d'annuaire sous Windows

Utilisez la fenêtre **Services** pour configurer le démarrage automatique d'une instance de serveur d'annuaire sous Windows.

Avant de commencer

Il est possible de configurer le démarrage automatique d'une instance de serveur d'annuaire après le démarrage du système d'exploitation, si votre ordinateur respecte les conditions ci-après.

- L'ordinateur doit contenir une instance de serveur d'annuaire capable de fonctionner en mode normal.

Pourquoi et quand exécuter cette tâche

Sous Windows, vous pouvez démarrer un serveur d'annuaire, le processus `idsslapd`, à partir de la fenêtre **Services** ou par la commande **idsslapd**. Pour les instances de serveur d'annuaire dotées d'une base de données DB2, vous devez définir une dépendance du service associé au serveur d'annuaire vise-à-vis du service de l'instance DB2. Lorsque l'instance de serveur d'annuaire est dotée d'une base de données DB2, le processus `idsslapd` ne peut démarrer qu'après DB2. Si vous ne définissez pas la dépendance, et si vous configurez la zone **Type de démarrage** sur `Automatique` pour le service associé au serveur, une erreur peut survenir au démarrage de celui-ci. Dans le cas d'une instance de serveur proxy, il n'est pas nécessaire de configurer la dépendance au service associé à l'instance DB2.

Pour une instance de serveur proxy, reportez-vous aux étapes1, 2, 4, 5 et 6.

Procédure

1. Connectez-vous en tant que membre du groupe des administrateurs.
2. Pour ouvrir la fenêtre **Services**, procédez de la manière suivante :
   a. Cliquez sur **Démarrer** > **Exécuter**.
   b. Dans la zone **Ouvrir**, entrez `services.msc`.
   c. Cliquez sur **OK**.
3. Recherchez le nom du service DB2 associé à l'instance de serveur d'annuaire à démarrer automatiquement. Le nom du service commence par `DB2 - SDSV631DB2 -`. Si le nom de l'instance DB2 est `DSRDBM01`, l'entrée est `DB2 - SDSV631DB2 - DSRDBM01`. Cliquez deux fois sur le service, et enregistrez la valeur qui suit `DB2 - SDSV631DB2 -` dans la zone **Nom affiché**. Dans l'exemple, le nom est `DSRDBM01`.
4. Recherchez le service de l'instance de serveur d'annuaire que vous souhaitez démarrer automatiquement. Le nom du service commence par `IBM Security Directory Server Instance 6.3.1`. Si le nom de l'instance est `dsrdbm01`, l'entrée est `IBM Security Directory Server Instance 6.3.1 - dsrdbm01`. Cliquez deux fois sur le service, et enregistrez la valeur qui suit `IBM Security Directory Server Instance 6.3.1 -` dans la zone **Nom affiché**. Dans l'exemple, pour l'instance `dsrdbm01`, la valeur est `idsslapd-dsrdbm01`.
5. Dans la fenêtre des propriétés d'`IBM Security Directory Server Instance 6.3.1 - dsrdbm01`, sélectionnez `Automatique` dans la liste **Type de démarrage**.
6. Cliquez sur **OK**.
7. Pour fermer la fenêtre **Services**, cliquez sur **Fichier** > **Quitter**.
8. Pour ouvrir le registre Windows, procédez de la manière suivante :
   a. Cliquez sur **Démarrer** > **Exécuter**.
   b. Dans la zone **Ouvrir**, entrez `regedit`.
   c. Cliquez sur **OK**.
9. Dans le panneau de navigation situé à gauche, accédez à **Mon ordinateur** > **HKEY_LOCAL_MACHINE** > **SYSTEM** > **CurrentControlSet** > **Services**.
10. Identifiez le service qui est associé à l'instance du serveur d'annuaire. Dans l'exemple, il s'agit d'`idsslapd-dsrdbm01`.
11. Cliquez sur le service associé à l'instance.

12. Dans le panneau situé à droite de la fenêtre, cliquez deux fois sur l'attribut DependOnService.
13. Dans la fenêtre **Modifier les chaînes multiples**, ajoutez le nom du service DB2 qui est associé à l'instance sous **LanmanServer**. Dans l'exemple, il s'agit de DSRDBM01.
14. Cliquez sur **OK**. La dépendance au service DB2 est créée.
15. Pour fermer le registre Windows, cliquez sur **Fichier** > **Quitter**.

Résultats

Au redémarrage du système, l'instance de serveur d'annuaire démarre automatiquement.

Configuration du démarrage automatique d'une instance de serveur d'annuaire sous UNIX

Mettez à jour les entrées du serveur d'annuaire dans le fichier /etc/inittab pour configurer le démarrage automatique d'une instance de serveur d'annuaire sous AIX, Linux ou Solaris.

Avant de commencer

Il est possible de configurer le démarrage automatique d'une instance de serveur d'annuaire après le démarrage du système d'exploitation, si votre ordinateur respecte les conditions ci-après.

- L'ordinateur doit contenir une instance de serveur d'annuaire capable de fonctionner en mode normal.

Procédure

1. Connectez-vous en tant qu'utilisateur root.
2. Pour configurer le démarrage automatique d'une instance de serveur d'annuaire ou de serveur proxy, ajoutez les entrées suivantes au fichier /etc/inittab :
   a. Pour ajouter le processus idsslapd et le serveur d'administration associés à une instance de serveur d'annuaire, ajoutez les entrées suivantes :

      AIX
      ```
      srv1:2:once:/opt/IBM/ldap/V6.3.1/sbin/idsslapd -I nom_instance
      > /dev/null 2>&1 #Autostart IBM Directory Server Instance

      adm1:2:once:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I
      nom_instance > /dev/null 2>&1 #Autostart IBM Directory
      Administration Server
      ```

      Linux
      ```
      srv1:2345:once:/opt/ibm/ldap/V6.3.1/sbin/ibmslapd -I
      nom_instance > /dev/null 2>&1 #Autostart IBM Directory Server
      Instance

      adm1:2345:once:/opt/ibm/ldap/V6.3.1/sbin/ibmdiradm -I
      nom_instance > /dev/null 2>&1 #Autostart IBM Directory
      Administration Server
      ```

      Solaris
      ```
      srv1:234:once:/opt/IBM/ldap/V6.3.1/sbin/ibmslapd -I
      nom_instance > /dev/null 2>&1 #Autostart IBM Directory Server
      Instance
      ```

```
adm1:234:once:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I
nom_instance > /dev/null 2>&1 #Autostart IBM Directory
Administration Server
```

Remplacez la variable *nom_instance* par le nom de l'instance.

b. Pour ajouter le processus `idsslapd` et le serveur d'administration associés à une instance de serveur proxy, vous devez d'abord démarrer les instances de serveur d'annuaire. Vous devez démarrer tous les serveurs d'annuaire avec une base de données DB2 avant de démarrer le serveur proxy. Si un serveur d'annuaire complet et un serveur proxy cohabitent sur l'ordinateur, ajoutez une temporisation entre le démarrage du serveur d'annuaire complet et celui du serveur proxy. Dans l'exemple suivant, la temporisation est introduite par l'ajout d'une entrée au format `id:2345:wait` dans le fichier `/etc/inittab`.

AIX

```
srv1:2345:once:/opt/IBM/ldap/V6.3.1/sbin/idsslapd -I
nom_instance1 > /dev/null 2>&1 #Autostart IBM Directory Server
Instance

adm1:2345:once:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I
nom_instance1 > /dev/null 2>&1 #Autostart IBM Directory
Administration Server

srv2:2345:once:/opt/IBM/ldap/V6.3.1/sbin/idsslapd -I
nom_instance2 > /dev/null 2>&1 #Autostart IBM Directory Server
Instance

adm2:2345:once:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I
nom_instance2 > /dev/null 2>&1 #Autostart IBM Directory
Administration Server

srv3:2345:wait:/opt/IBM/ldap/V6.3.1/sbin/idsslapd -I
instance_proxy1 -k > /dev/null 2>&1 #Autostart IBM Directory
Proxy Server Instance

adm3:2345:wait:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I
instance_proxy1 -k > /dev/null 2>&1 #Autostart IBM Directory
Administration Server

srv4:2345:wait:/opt/IBM/ldap/V6.3.1/sbin/idsslapd -I
instance_proxy1 > /dev/null 2>&1 #Autostart IBM Directory
Proxy Server Instance

adm4:2345:wait:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I
instance_proxy1 > /dev/null 2>&1 #Autostart IBM Directory
Administration Server
```

Remplacez les variables *nom_instance1* et *nom_instance2* par le nom des instances de serveur d'annuaire. Remplacez la variable *instance_proxy1* par le nom de l'instance du serveur proxy.

Résultats

Une fois que les entrées ont été ajoutées au fichier `/etc/inittab`, l'instance de serveur d'annuaire (complet ou proxy) peut démarrer automatiquement après le redémarrage du système.

Chapitre 22. Stratégie appliquée aux groupes de correctifs

Les informations suivantes concernent les correctifs et les groupes de correctifs d'IBM Security Directory Server.

Pour les correctifs ou les groupes de correctifs AIX, Linux, Solaris et HP-UX sont disponibles pour l'installation basée sur un script natif.

Pour Windows, des correctifs et des groupes de correctifs basés sur IBM Installation Manager sont disponibles.

Les correctifs ou les groupes de correctifs basés sur IBM Installation Manager peuvent être installés avec l'interface graphique utilisateur et en mode silencieux.

Vous pouvez identifier la version du correctif ou du groupe de correctifs installé avec IBM Installation Manager de l'une des façons suivantes :

- Sélectionnez **Fichier** > **View Installed Packages**
- Utilisez la commande **imcl** à partir du répertoire des outils du répertoire d'installation d'IBM Installation Manager.

Sur les systèmes UNIX, vérifiez la version des modules natifs pour déterminer celle des correctifs et des groupes de correctifs installés.

Remarque : Une fois que le groupe de correctifs est appliqué à la version de base, aucune modification ni désinstallation ne doit être effectuée par IBM Installation Manager. Après l'application du groupe de correctifs en mode natif, vous devez continuer à utiliser ce mode pour les opérations ultérieures.

Installation des groupes de correctifs avec IBM Installation Manager

Utilisez IBM Installation Manager pour appliquer les groupes de correctifs ou installer les améliorations du flot de services sur les systèmes d'exploitation Microsoft Windows.

Avant de commencer

- Lisez les informations sur la stratégie de correctifs.
- Assurez-vous qu'IBM Installation Manager, version 1.7.0 ou version ultérieure est installé sur votre système. Consultez la documentation IBM Installation Manager.
- Avant de commencer à installer le groupe de correctifs,vous devez arrêter tous les processus ou services IBM Security Directory Server en cours d'exécution. Vous pouvez le faire manuellement ou en cliquant sur **Stop all blocking processes** dans Installation Manager.

Pourquoi et quand exécuter cette tâche

Le groupe de correctifs ne met à jour que les fonctions déjà installées. Vous devez mettre à jour le produit avant d'utiliser l'assistant **Modify** pour installer des fonctions qui ne sont pas déjà installées sur votre système.

Le groupe de correctifs ne met pas à jour IBM DB2, IBM GSKit, IBM embedded WebSphere Application Server et IBM Java Development Kit. Utilisez l'assistant **Modifier** pour mettre à jour ces logiciels.

Procédure

1. Téléchargez le groupe de correctifs à partir de http://www-01.ibm.com/support/docview.wss?uid=swg21496581#v631.
2. Définissez les préférences de référentiel dans IBM Installation Manager.
   a. Pour démarrer IBM Installation Manager à partir du menu **Démarrer**,sélectionnez **Tous les programmes** > **IBM Installation Manager** > **IBM Installation Manager**.
   b. Dans la page d'accueil d'IBM Installation Manager, cliquez sur **Fichier** > **Préférences**.
   c. Dans la page Référentiels, cliquez sur **Ajouter un référentiel**.
   d. Dans la page Add Repository, spécifiez l'un des emplacements de référentiel suivants :
      - Chemin du fichier d'un répertoire local ou d'une unité partagée distante contenant le package du produit téléchargé sur le site web de support d'IBM.
      - URL du référentiel sur un serveur web.
   e. Cliquez sur **OK**. Si vous définissez une adresse HTTPS ou si l'accès au référentiel est restreint, vous êtes invités à saisir un ID utilisateur et un mot de passe. Le nouvel emplacement ou l'emplacement modifié du référentiel apparaît alors dans la liste.
   f. Pour vérifier l'accès au référentiel, cliquez sur **Tester les connexions**.
   g. Cliquez sur **OK** pour quitter la page Référentiels.
3. Commencez l'installation.
   - Si IBM Security Directory Server version 6.3.1 n'est pas installé sur votre système, procédez comme suit.
     a. Dans la page d'accueil d'IBM Installation Manager, cliquez sur **Install**. L'assistant **Installer** vous guide tout au long de laprocédure d'installation.
     b. Terminez la procédure d'installation décrite dans «Installation à l'aide d'IBM Installation Manager», à la page 31.
   - Si IBM Security Directory Server version 6.3.1 est installé sur votre système, pour appliquer le groupe de correctifs, procédez comme suit.
     a. Dans la page d'accueil d'IBM Installation Manager, cliquez sur **Update**. L'assistant **Mettre à jour** cherche les mises à jour disponibles des packages installés sur votre système.
     b. Sélectionnez **IBM Security Directory Server**. Le répertoire d'installation correspond à l'emplacement auquel la version 6.3.1 a été installée et ne peut pas être modifié. Cliquez sur **Suivant**.
     c. Sélectionnez le produit à mettre à jour, **IBM Security Directory Server**, puis sélectionnez la mise à jour à appliquer, **Version 6.3.1.5**. Cliquez sur **Suivant**.
     d. Acceptez la licence du groupe de correctifs, puis cliquez sur **Suivant**.
     e. Les fonctions à mettre à jour sont sélectionnées par défaut. Seules les fonctions installées précédemment sur le système sont affichées pour la mise à jour. Cliquez sur **Suivant**.

        Remarque : Si vous essayez d'effacer les sélections, cette fonction est marqué pour être désinstallée.

        Restriction : Même si IBM DB2 est répertorié dans cette page comme fonction et est sélectionné pour la mise à jour par défaut, il n'est pas mis à jour. Le logiciel prérequis n'est pas mis à jour lorsque vous sélectionnez

l'assistant **Mettre à jour** dans IBM Installation Manager. N'effacez pas la sélection IBM DB2, car cela efface également la fonction du serveur.

f. Dans la page de résumé, vérifiez les informations, puis cliquez sur **Suivant** pour commencer l'installation.

4. Vérifiez votre installation. Pour plus d'informations sur la vérification avec IBM Installation Manager et la vérification pour le système d'exploitation concerné, consultez la section Chapitre 13, «Vérification des fonctions d'IBM Security Directory Server», à la page 85.

Que faire ensuite

Pour désinstaller le groupe de correctifs, utilisez l'assistant **Annuler**, qui rétablit la version précédente du package.

Installation des groupes de correctifs en mode silencieux

Vous pouvez utiliser IBM Installation Manager pour installer les groupes de correctifs en mode silencieux.

Remarque : Dans un fichier de réponses pour les mises à jour, vous ne pouvez pas indiquer une fonction qui n'a pas encore été installée. Si vous le faites, la procédure de mise à jour du groupe de correctifs échoue.

Génération d'un nouveau fichier de réponses pour l'installation du groupe de correctifs

Si le fichier de réponses utilisé pour l'installation du produit n'est pas disponible, enregistrez un nouveau fichier de réponses.

1. Démarrez IBM Installation Manager en mode de simulation d'installation. Par exemple :

   ```
   C:\Program Files\IBM\Installation Manager\eclipse\IBMIM.exe
        -record c:\SDS_6310\install_resp.xml -skipInstall agentDataLocation
   ```

   où

   l'emplacement *agentDataLocation* stocke les données pour l'installation du produit.

2. Définissez les préférences de référentiel dans la version 6.3.1.0.
3. Terminez la procédure de simulation d'installation.
4. Fermez IBM Installation Manager. Un fichier de réponses pour la procédure d'installation est créé sans installer le produit.
5. Exécutez la procédure de la section suivante.

Installation avec le fichier de réponses utilisé lors de l'installation du produit

1. Modifiez le fichier de réponses `install_resp.xml` et apportez les modifications suivantes :

   a. Mettez à jour le chemin du référentiel avec le chemin du référentiel de la version 6.3.1.5.

      ```
      <repository location='C:\SDS_6315\ibm_sds'/>
      ```

   b. Mettez à jour la version proposée sur 6.3.1.5.

      ```
      <offering id='com.ibm.security.directoryserver.v631' version='6.3.1.5' profile=.......
      ```

2. Commencez l'installation en mode silencieux pour appliquer le groupe de correctifs.

Par exemple :

```
C:\Program Files\IBM\Installation Manager\eclipse\tools\imcl.exe
      input c:\SDS_6310\install_resp.xml -acceptLicense -showProgress
```

Dans cette commande, vous pouvez également utiliser l'option `-stopBlockingProcesses` si nécessaire, pour arrêter tous les processus de blocage en mode silencieux avant que le groupe de correctifs soit installé.

Installation des groupes de correctifs avec des scripts natifs

Exécutez le script fourni dans la ligne de commande pour appliquer les groupes de correctifs ou pour installer les améliorations du flot de services sur les systèmes AIX, Linux et Solaris.

Avant de commencer

Lisez les informations sur la stratégie de correctifs.

Procédure

1. Téléchargez le groupe de correctifs à partir de http://www-01.ibm.com/support/docview.wss?uid=swg21496581#v631.
2. Extrayez l'archive du correctif dans un répertoire disposant de suffisamment d'espace. Les détails concernant le contenu du groupe de correctifs, dont les noms de répertoire et de fichier, sont fournis dans le fichier *README* inclus avec le groupe de correctifs.
3. Arrêtez tous les processus du client ou du serveur associés à IBM Security Directory Server. L'ensemble de processus démon inclut le serveur d'annuaire, le serveur d'administration, le serveur proxy (le cas échéant) et les applications LDAP personnalisées. Les programmes et les bibliothèques ne peuvent pas être remplacés lorsqu'ils sont en cours d'utilisation. Si la fonction de trace est activée, exécutez **ldtrc off** pour le désactiver. Pour plus d'informations sur l'arrêt des instances du serveur d'annuaire et des processus d'administration, consultez les rubriques sous Tâches d'administration de serveur standard dans la documentation d'IBM Security Directory Server.
4. Dans la ligne de commande, modifiez le répertoire pour utiliser le dossier d'extraction de l'archive du correctif.
5. Exécutez la commande ci-après en tant que `root` :

   ```
   idsinstall -u -f
   ```

   Le programme d'installation installe les mises à jour des composants déjà installés sur votre système.
6. Vérifiez votre installation.
   a. Le programme d'installation affiche un message qui indique si l'installation a réussi. Consultez le journal d'installation dans le répertoire `/tmp/idsinstall_`*`horodatage`*.
   b. Si l'installation n'a pas réussi ou si vous avez reçu un message indiquant que les modules n'ont pas tous été installés, corrigez les erreurs indiquées dans le journal, par exemple, l'espace disque insuffisant. Ensuite, réexécutez le programme d'installation et assurez-vous que tous les modules ont bien été installés.
   c. Vérifiez le numéro de version des modules pour vous assurer qu'ils sont du niveau approprié. Pour plus d'informations, voir Chapitre 6, «Interrogation des modules d'IBM Security Directory Server», à la page 47.

Chapitre 23. Désinstallation d'IBM Security Directory Server : Présentation

Lisez une présentation sur la désinstallation du produit IBM Security Directory Server et les aspects importants à prendre en compte avant la désinstallation.

Avant de commencer

Pour désinstaller IBM Security Directory Server, vous devez vous connecter avec des droits root sur les systèmes AIX, Linux, Solaris ou HP-UX et comme membre d'un groupe administrateur sur les systèmes Windows.

Pourquoi et quand exécuter cette tâche

Lorsque vous désinstallez IBM Security Directory Server, les instances et leurs fichiers de configuration ne sont pas supprimés.

Procédure

1. Arrêtez tous les processus IBM Security Directory Server client ou serveur, y compris le serveur d'annuaire, le démon d'administration et les applications LDAP personnalisées. Les programmes et les bibliothèques ne peuvent pas être remplacés lorsqu'ils sont en cours d'utilisation. Si le traçage est activé, lancez la commande **ldtrc off** pour le désactiver.
2. Désinstallez IBM Security Directory Server en utilisant le même mode que celui dans lequel vous l'avez installé et en tenant compte du système d'exploitation. Les méthodes disponibles pour la désinstallation des modules d'IBM Security Directory Server sont celles ci-après.
   a. Programme de désinstallation de l'interface graphique.
   b. Utilitaires du système d'exploitation Le nom des modules sur les systèmes Linux varie légèrement selon qu'il s'agit de la version de disponibilité générale (GA) ou de mises à jour. Par exemple, le nom du module du client de base pour la version de disponibilité générale sur xSeries Linux est `idsldap-cltbase63-6.3.0-0.i386.rpm`. La commande **rpm -qa** permet d'afficher la liste de tous les modules.
3. Après avoir désinstallé IBM Security Directory Server, vérifiez si tous les modules du produit ont bien été supprimés. Pour plus d'informations, voir Chapitre 6, «Interrogation des modules d'IBM Security Directory Server», à la page 47.

Information associée:

http://www-01.ibm.com/support/knowledgecenter/SSVJJU/welcome
Pour plus d'informations, voir la rubrique *Désinstallation d'IBM Security Directory Server* dans la section *Installation et configuration* de la documentation du produit IBM Security Directory Server.

Chapitre 24. Désinstallation d'IBM Security Directory Server et des logiciels corequis

Vous pouvez vouloir désinstaller IBM Security Directory Server et les logiciels corequis si vous destinez l'ordinateur à une autre utilisation, ou s'il arrive en fin de vie.

Vous pouvez utiliser IBM Installation Manager ou les utilitaires du système d'exploitation pour désinstaller IBM Security Directory Server. Vous devez le désinstaller selon la même méthode que celle employée pour l'installer. Vous devez l'installer et le désinstaller à l'aide d'IBM Installation Manager, ou l'installer et le désinstaller à l'aide des utilitaires du système d'exploitation. Ces méthodes ne doivent pas être utilisées l'une après l'autre.

Pour désinstaller IBM Security Directory Server sur un ordinateur, vérifiez que les conditions ci-après sont réunies.

1. Vous devez arrêter tous les processus IBM Security Directory Server client et serveur.
   - Serveur d'annuaire
   - Serveur d'administration
   - Traces LDAP
   - Outil d'administration Web et serveur d'applications associé
   - Applications LDAP personnalisées
2. Si vous prévoyez de réinstaller IBM Security Directory Server sur l'ordinateur, il est inutile de supprimer l'instance de serveur d'annuaire ou d'annuler la configuration de la base de données DB2 sur l'instance. Lorsque vous retirez IBM Security Directory Server de l'ordinateur, les instances de serveur d'annuaire sont conservées intactes jusqu'à leur retrait manuel ou l'annulation de leur configuration.
3. L'utilisateur et le groupe `idsldap` qui ont été créés lors de l'installation d'IBM Security Directory Server restent sur le système après la désinstallation. Vous devez également prendre en compte les éléments suivants avant de désinstaller IBM Security Directory Server sous AIX, Linux ou Solaris.
   - Si vous ne voulez pas de l'utilisateur et du groupe `idsldap` qui sont définis, supprimez-les à l'aide des utilitaires du système d'exploitation. L'utilisateur et le groupe `idsldap` sont requis par le serveur proxy et le serveur d'annuaire complet, et ils doivent exister sur l'ordinateur si IBM Security Directory Server est installé.
   - Si vous supprimez l'utilisateur `idsldap` mais pas son répertoire de base, des problèmes peuvent se produire lors de la création de cet utilisateur si vous réinstallez IBM Security Directory Server. Par conséquent, si vous supprimez l'utilisateur `idsldap`, veillez à supprimer également son répertoire de base. Si vous supprimez l'utilisateur `idsldap` à l'aide de la commande **`userdel`**, vous devez utiliser le paramètre **`-r`** pour supprimer le répertoire de base correspondant, `userdel -r idsldap`.
4. Sous Windows, les services du serveur d'administration et du serveur d'annuaire sont supprimés lors de la désinstallation d'IBM Security Directory Server. Ils ne sont pas remplacés si vous réinstallez IBM Security Directory Server. Vous pouvez utiliser la commande **`idsslapd`** pour ajouter le service du serveur et la commande **`idsdiradm`** pour ajouter le service du serveur

d'administration. Pour plus d'informations sur les commandes **idsslapd** et **idsdiradm**, voir le manuel *IBM Security Directory ServerCommand Reference*.

Désinstallation à l'aide d'IBM Installation Manager

Si vous avez utilisé IBM Installation Manager pour l'installation d'IBM Security Directory Server, utilisez-le aussi pour sa désinstallation et celle de ses composants.

Lorsque vous utilisez IBM Installation Manager pour la désinstallation d'IBM Security Directory Server, le programme retire IBM Security Directory Server et les logiciels corequis qui ont été installés. En cas de désinstallation par IBM Installation Manager, il n'est pas possible de désinstaller sélectivement certaines fonctions d'IBM Security Directory Server.

Pour réussir à désinstaller IBM DB2, si vous avez installé la version d'IBM DB2 qui est fournie avec IBM Security Directory Server, vous devez retirer toutes les instances de DB2 qui ont été créées avec la copie de DB2. S'il reste sur l'ordinateur une instance de DB2 créée avec la copie de DB2, DB2 n'est pas supprimé lors de la désinstallation d'IBM Security Directory Server. IBM Installation Manager consigne les messages d'erreur dans son fichier journal.

Vous devez utiliser IBM Installation Manager ou les utilitaires du système d'exploitation pour installer, modifier ou désinstaller IBM Security Directory Server et ses composants. Vous ne devez pas utiliser à la fois IBM Installation Manager et les utilitaires du système d'exploitation pour installer, modifier ou désinstaller IBM Security Directory Server et ses composants.

Désinstallation avec IBM Installation Manager

Utilisez IBM Installation Manager pour désinstaller IBM Security Directory Server, si vous avez utilisé IBM Installation Manager pour installer IBM Security Directory Server.

Avant de commencer

Vous devez arrêter tous les processus IBM Security Directory Server client et serveur.

- Serveur d'annuaire
- Serveur d'administration
- Traces LDAP
- Applications LDAP personnalisées

Si des processus sont en cours d'utilisation, les programmes et les bibliothèques ne peuvent pas être supprimés.

Procédure

1. Démarrez IBM Installation Manager.
   - AIX et Linux :
     a. Ouvrez une fenêtre de commande et accédez au répertoire qui contient IBM Installation Manager. Voici le répertoire d'installation par défaut d'IBM Installation Manager :

        ```
        opt/IBM/InstallationManager/eclipse
        ```

     b. Exécutez la commande ci-après.

        ```
        ./IBMIM
        ```

- Microsoft Windows :
  a. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Installation Manager** > **IBM Installation Manager**.

2. Cliquez sur **Désinstaller**.
3. Sélectionnez **IBM Security Directory Server** avec la version appropriée, puis cliquez sur **Suivant**.
4. Dans la fenêtre de **désinstallation des modules**, passez en revue les modules sélectionnés que vous allez désinstaller.

   Important : Si vous choisissez d'utiliser une version existante de DB2 ou de GSKit pendant l'installation, IBM Installation Manager met à jour l'entrée de la fonction dans son registre. Si vous supprimez une fonction qui a été installée avec l'option **Continuer avec l'élément existant**, Installation Manager :
   - Supprime l'entrée de son propre registre.
   - Ne désinstalle pas la fonction sur l'ordinateur.

   S'il existe des instances DB2 que vous avez créées avec la copie de DB2 installée à l'aide d'IBM Installation Manager, IBM Security Directory Server ne peut pas être supprimé. Dans ce cas, retirez manuellement les instances DB2 et réessayez. Il est recommandé de sauvegarder la base de données avant de supprimer les instances DB2.
5. Cliquez sur **Désinstaller**. Lorsque la désinstallation est terminée, IBM Installation Manager indique si la désinstallation a réussi ou échoué.
6. Facultatif : En cas d'erreur lors de la désinstallation, cliquez sur **Afficher le fichier journal** pour en lire les détails. Pour plus d'informations, voir Chapitre 5, «Fichiers journaux d'IBM Installation Manager», à la page 45.
7. Cliquez sur **Terminer**.
8. Cliquez sur **Fichier** > **Quitter**.

Résultats

IBM Installation Manager désinstalle IBM Security Directory Server et ses composants.

Désinstallation en mode silencieux avec un fichier de réponses

Exécutez la procédure suivante pour désinstaller les composants d'IBM Security Directory Server en mode silencieux avec un fichier de réponse.

Avant de commencer

IBM Installation Manager, version 1.7.0 ou version supérieure est requis pour l'installation en mode silencieux des modules IBM Security Directory Server0

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser le fichier de réponses ou enregistrer un fichier de réponses personnalisé et l'utiliser comme fichier en entrée de la désinstallation en mode silencieux.

Procédure

1. Connectez-vous au système en tant qu'administrateur.

2. Accédez à la commande **IBMIM** dans l'emplacement d'installation d'IBM Installation Manager.

Système d'exploitation	Emplacement par défaut de la commande **IBMIM** :
Microsoft Windows	`C:\Program Files\IBM\ InstallationManager\eclipse`
AIX et Linux	`/opt/IBM/InstallationManager/eclipse`

3. Facultatif : Exécutez la commande **IBMIM** pour enregistrer un fichier de réponses pour l'installation en mode silencieux.
   a. Exécutez les commandes suivantes sur les différents systèmes d'exploitation :

      Microsoft Windows

      ```
      IBMIM.exe -record path_name\uninstall_responseFile.xml
      -skipInstall agentDataLocation
      ```

      AIX et Linux

      ```
      ./IBMIM -record path_name/uninstall_responseFile.xml
      -skipInstall agentDataLocation
      ```

      la commande ouvre IBM Installation Manager.
   b. Terminez l'enregistrement de la désinstallation d'IBM Security Directory Server0 Pour plus d'informations, voir 2, à la page 239
4. Exécutez la commande **IBMIM** pour démarrer la désinstallation en mode silencieux avec le fichier de réponses comme entrée.

Système d'exploitation	Commande à exécuter :
Microsoft Windows	`IBMIM.exe -silent -input path_name\uninstsll_responseFile.xml -noSplash`
AIX et Linux	`./IBMIM -silent -input path_name/uninstall_responseFile.xml -noSplash`

5. Vérifiez le récapitulatif de désinstallation et les fichiers journaux.

Système d'exploitation	Chemin d'accès au journal par défaut :
Microsoft Windows	`C:\ProgramData\IBM\InstallationManager\ logs`
AIX et Linux	`/var/ibm/InstallationManager/logs/`

6. Vérifiez que les modules d'IBM Security Directory Server sont désinstallés.

Système d'exploitation	Vérification des modules :
Microsoft Windows	Voir «Vérification des fonctions d'IBM Security Directory Server sous Windows», à la page 85.
AIX et Linux	Voir «Vérification des modules d'IBM Security Directory Server», à la page 87.

Résultats

IBM Installation Manager désinstalle les composants d'IBM Security Directory Server en mode silencieux.

Désinstallation en mode silencieux avec la commande `imcl uninstall`

Exécutez la procédure suivante pour désinstaller les composants d'IBM Security Directory Server en mode silencieux avec la commande **`imcl uninstall`**.

Avant de commencer

IBM Installation Manager, version 1.7.0 ou version supérieure est requis pour l'installation en mode silencieux des modules IBM Security Directory Server0

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la commande **`imcl uninstall`** pour désinstaller IBM Security Directory Server en mode silencieux.

Procédure

1. Connectez-vous au système en tant qu'administrateur.
2.
3. Exécutez la commande **`imcl listInstalledPackages`** depuis le répertoire *<IBM_Installation_Manager_install_dir>*/eclipse/tools0

Système d'exploitation	Commande à exécuter
Microsoft Windows	`imcl.exe listInstalledPackages`
AIX et Linux	`./imcl listInstalledPackages`

   Cette commande liste tous les modules installés par IBM Installation Manager.
4. Exécutez **`imcl uninstall com.ibm.security.directoryserver. v631_6.3.1.0`**. Utilisez l'entrée de Security Directory Server, qui igure dans la sortie de la commande **`imcl listInstalledPackages`** ci-dessus.

Système d'exploitation	Commande à exécuter :
Microsoft Windows	`imcl.exe uninstall com.ibm.security.directoryserver. v631_6.3.1.0`
AIX et Linux	`./imcl uninstall com.ibm.security.directoryserver. v631_6.3.1.0`

Résultats

IBM Installation Manager désinstalle les composants d'IBM Security Directory Server en mode silencieux.

Désinstallation d'IBM Security Directory Server avec les utilitaires du système d'exploitation

Si vous avez utilisé les utilitaires du système d'exploitation pour installer IBM Security Directory Server, utilisez-les aussi pour le désinstaller.

Vous pouvez utiliser les utilitaires du système d'exploitation pour désinstaller IBM Security Directory Server sur les postes fonctionnant sous AIX, Linux, Solaris et HP-UX. Sous Windows, vous devez l'installer et le désinstaller à l'aide d'IBM Installation Manager.. Voir «Désinstallation avec IBM Installation Manager», à la page 238.

Lorsque vous utilisez les utilitaires du système d'exploitation pour désinstaller IBM Security Directory Server, le programme supprime IBM Security Directory Server. En cas de désinstallation par les utilitaires du système d'exploitation, vous pouvez désinstaller sélectivement certaines fonctions d'IBM Security Directory Server.

Vous devez arrêter tous les processus IBM Security Directory Server client et serveur avant la désinstallation du produit.

- Serveur d'annuaire
- Serveur d'administration
- Traces LDAP
- Outil d'administration Web et serveur d'applications associé
- Applications LDAP personnalisées

Si vous avez créé et configuré une instance de serveur d'annuaire avec une base de données DB2, elles ne sont pas supprimées si vous utilisez les utilitaires du système d'exploitation pour désinstaller IBM Security Directory Server.

Désinstallation à l'aide des utilitaires AIX

Vous pouvez utiliser les utilitaires de ligne de commande AIX pour désinstaller IBM Security Directory Server sur un système AIX.

Vous pouvez utiliser l'un des utilitaires suivants pour la désinstallation d'IBM Security Directory Server :

SMIT La méthode de désinstallation recommandée est celle de l'utilitaire. Pour plus d'informations, voir «Désinstallation à l'aide de SMIT».

installp
Pour plus d'informations, voir «Désinstallation avec la commande **installp**», à la page 243.

Désinstallation à l'aide de SMIT

Utilisez la commande **smit** pour désinstaller IBM Security Directory Server sur un système AIX.

Avant de commencer

Vous devez arrêter tous les processus IBM Security Directory Server client et serveur.

- Serveur d'annuaire
- Serveur d'administration
- Traces LDAP

- Outil d'administration Web et serveur d'applications associé
- Applications LDAP personnalisées

Procédure

1. Connectez-vous en tant qu'utilisateur root.
2. Accédez à l'invite de commande.
3. Lancez la commande **smit**. La fenêtre **Maintenance et installation de logiciels** s'ouvre.
4. Sélectionnez **Installation et maintenance de logiciels** > **Maintenance et utilitaires logiciels**.
5. Sélectionnez **Supprimer les logiciels installés**.
6. Dans la zone **Nom du logiciel**, appuyez sur la touche **F4** pour afficher la liste des logiciels installés. Vous pouvez entrer la valeur `idsldap` dans la zone pour lister tous les modules d'IBM Security Directory Server.
7. Sélectionnez les modules à supprimer, puis appuyez sur la touche Entrée.

Résultats

L'utilitaire SMIT retire IBM Security Directory Server du système AIX. Si vous avez sélectionné le retrait de tous les modules d'IBM Security Directory Server, retire aussi le répertoire d'installation d'IBM Security Directory Server, `/opt/IBM/ldap/V6.3.1`, du système AIX.

Que faire ensuite

Vérifiez que la désinstallation d'IBM Security Directory Server a abouti. Pour plus d'informations, voir «Vérification des modules d'IBM Security Directory Server», à la page 87.

Désinstallation avec la commande `installp`

Utilisez la commande **installp** pour désinstaller IBM Security Directory Server sur un système AIX.

Avant de commencer

Vous devez arrêter tous les processus IBM Security Directory Server client et serveur.

- Serveur d'annuaire
- Serveur d'administration
- Traces LDAP
- Outil d'administration Web et serveur d'applications associé
- Applications LDAP personnalisées

Procédure

1. Connectez-vous en tant qu'utilisateur root.
2. Accédez à l'invite de commande.
3. Lancez la commande ci-après pour déterminer les modules d'IBM Security Directory Server à désinstaller.

   ```
   lslpp -l 'idsldap*'
   ```

4. Pour supprimer un module IBM Security Directory Server, entrez la commande ci-après.

```
installp -u nom_module
```

Pour désinstaller entièrement IBM Security Directory Server, retirez tous les modules IBM Security Directory Server de la même version. Les modules d'IBM Security Directory Server, doivent être installés dans l'ordre inverse de leur ordre d'installation pour permettre la désinstallation. Pour plus d'informations sur la séquence, voir «Modules pour l'installation sur un système AIX», à la page 69. Pour supprimer le module `idsldap.ent631` , entrez la commande ci-après.

```
installp -u idsldap.ent631
```

Que faire ensuite

Vérifiez que la désinstallation d'IBM Security Directory Server a abouti. Pour plus d'informations, voir «Vérification des modules d'IBM Security Directory Server», à la page 87.

Désinstallation à l'aide des utilitaires Linux

Vous pouvez utiliser les utilitaires de ligne de commande Linux pour désinstaller IBM Security Directory Server sur un système Linux.

Les noms des modules d'IBM Security Directory Server diffèrent selon le système d'exploitation et l'architecture des ordinateurs. Vous devez vérifier quels modules d'IBM Security Directory Server ont été installés avant de commencer la désinstallation.

Désinstallation à l'aide des utilitaires Linux

Utilisez la commande **rpm** pour désinstaller IBM Security Directory Server sur un système Linux.

Avant de commencer

Vous devez arrêter tous les processus IBM Security Directory Server client et serveur.

- Serveur d'annuaire
- Serveur d'administration
- Traces LDAP
- Outil d'administration Web et serveur d'applications associé
- Applications LDAP personnalisées

Pourquoi et quand exécuter cette tâche

L'exemple qui suit montre la désinstallation des modules d'IBM Security Directory Server sur un système Linux AMD64 Opteron/EM64T. Pour Linux System z, System i, System p ou System x, remplacez les noms de module par des noms appropriés.

Procédure

1. Connectez-vous en tant qu'utilisateur root.
2. Accédez à l'invite de commande.
3. Lancez la commande ci-après pour déterminer les modules d'IBM Security Directory Server à désinstaller.

   ```
   rpm -qa | grep -i idsldap
   ```

4. Pour supprimer un module IBM Security Directory Server, entrez la commande ci-après.

   ```
   rpm -ev
   nom_module
   ```

   Pour désinstaller entièrement IBM Security Directory Server, retirez tous les modules IBM Security Directory Server de la même version. Les modules d'IBM Security Directory Server, doivent être installé dans l'ordre inverse de leur ordre d'installation. Pour plus d'informations sur la séquence, voir «Modules pour l'installation sur un système Linux», à la page 75. Pour supprimer le module `idsldap-srv64bit631-6.3.1-0.x86_64.rpm`, entrez la commande ci-après.

   ```
   rpm -ev idsldap-srv64bit631-6.3.1-0.x86_64.rpm
   ```

Que faire ensuite

Vérifiez que la désinstallation d'IBM Security Directory Server a abouti. Pour plus d'informations, voir «Vérification des modules d'IBM Security Directory Server», à la page 87.

Désinstallation à l'aide des utilitaires Solaris

Vous pouvez utiliser les utilitaires de ligne de commande Solaris pour désinstaller IBM Security Directory Server sur un système Solaris.

Les noms des modules d'IBM Security Directory Server sont les mêmes pour les systèmes Solaris SPARC et Solaris X64.

Désinstallation à l'aide des utilitaires Solaris

Utilisez la commande **pkgrm** pour désinstaller IBM Security Directory Server sur un système Solaris.

Avant de commencer

Vous devez arrêter tous les processus IBM Security Directory Server client et serveur.

- Serveur d'annuaire
- Serveur d'administration
- Traces LDAP
- Outil d'administration Web et serveur d'applications associé
- Applications LDAP personnalisées

Procédure

1. Connectez-vous en tant qu'utilisateur root.
2. Accédez à l'invite de commande.
3. Lancez la commande ci-après pour déterminer les modules d'IBM Security Directory Server à désinstaller.

   ```
   pkginfo | grep -i IDSl
   ```

4. Pour supprimer un module IBM Security Directory Server, entrez la commande ci-après.

   ```
   pkgrm nom_module
   ```

   Pour désinstaller entièrement IBM Security Directory Server, retirez tous les modules IBM Security Directory Server de la même version. Les modules

d'IBM Security Directory Server, doivent être installé dans l'ordre inverse de leur ordre d'installation. Pour plus d'informations sur la séquence, voir «Modules pour l'installation sur un système Solaris», à la page 79. Pour supprimer le module `IDSlent631` , entrez la commande ci-après.

```
pkgrm IDSlent631
```

Que faire ensuite

Vérifiez que la désinstallation d'IBM Security Directory Server a abouti. Pour plus d'informations, voir «Vérification des modules d'IBM Security Directory Server», à la page 87.

Désinstallation à l'aide des utilitaires HP-UX

Vous pouvez utiliser les utilitaires de ligne de commande HP-UX pour désinstaller IBM Security Directory Server sur un système HP-UX.

Sur les ordinateurs HP-UX (Itanium), seuls les modules client d'IBM Security Directory Server sont pris en charge.

Désinstallation à l'aide des utilitaires HP-UX

Utilisez la commande **swremove** pour désinstaller IBM Security Directory Server sur un système HP-UX.

Avant de commencer

Vous devez arrêter tous les processus clients d'IBM Security Directory Server.

- Traces LDAP
- Applications LDAP personnalisées

Procédure

1. Connectez-vous en tant qu'utilisateur root.
2. Accédez à l'invite de commande.
3. Lancez la commande ci-après pour déterminer les modules d'IBM Security Directory Server à désinstaller.

   ```
   swlist | grep -i idsldap
   ```

4. Pour supprimer un module IBM Security Directory Server, entrez la commande ci-après.

   ```
   swremove nom_progiciel
   ```

   Pour désinstaller entièrement IBM Security Directory Server, retirez tous les modules IBM Security Directory Server de la même version. Les modules d'IBM Security Directory Server, doivent être installé dans l'ordre inverse de leur ordre d'installation. Pour plus d'informations sur la séquence, voir «Modules pour l'installation sur un système HP-UX Itanium», à la page 82. Pour supprimer le module `idsldap.cltjava631.depot` , entrez la commande ci-après.

   ```
   swremove idsldap.cltjava631.depot
   ```

Que faire ensuite

Vérifiez que la désinstallation d'IBM Security Directory Server a abouti. Pour plus d'informations, voir «Vérification des modules d'IBM Security Directory Server», à la page 87.

Désinstallation d'IBM DB2 avec des commandes DB2

Si vous avez installé manuellement la copie d'IBM DB2 qui est fournie avec IBM Security Directory Server, utilisez les commandes DB2 pour retirer IBM DB2 de l'ordinateur.

Si vous avez installé la copie d'IBM DB2 avec IBM Installation Manager pendant l'installation d'IBM Security Directory Server, IBM DB2 est installé à un emplacement prédéfini. Pour plus d'informations sur l'emplacement par défaut, voir «Emplacements d'installation par défaut», à la page 27. Si vous avez installé la copie d'IBM DB2 avec IBM Installation Manager, vous devez utiliser IBM Installation Manager pour le désinstaller.

Si votre ordinateur contient des instances DB2 de la copie d'IBM DB2, vous devez les supprimer manuellement avant de désinstaller IBM DB2. Il est recommandé de sauvegarder les bases de données DB2 et les données avant de procéder à la désinstallation.

Si vous avez installé IBM DB2 manuellement à un emplacement personnalisé à l'aide des commandes DB2, utilisez-les pour désinstaller IBM DB2. Sous AIX, Linux, et Solaris, lancez la commande **db2_deinstall** dans le répertoire *DB2_installation_location*/install/ pour désinstaller IBM DB2. Sous Windows, lancez la commande **db2unins** dans le répertoire *rép_installation_DB2*\bin pour désinstaller IBM DB2. Pour plus d'informations sur la désinstallation d'IBM DB2, voir la documentation du produit IBM DB2 à l'adresse http://www-01.ibm.com/support/knowledgecenter/SSEPGG/welcome.

Désinstallation d'IBM Global Security Kit à l'aide des utilitaires du système d'exploitation

Si vous avez utilisé les utilitaires du système d'exploitation pour installer IBM Global Security Kit (GSKit), utilisez-les aussi pour le désinstaller.

Vous pouvez utiliser les utilitaires du système d'exploitation pour désinstaller GSKit sur les postes fonctionnant sous AIX, Linux, Solaris et HP-UX.

Sous Windows, vous ne pouvez désinstaller GSKit manuellement que si vous avez choisi d'utiliser une version installée de GSKit avec IBM Installation Manager pendant l'installation. Si IBM Security Directory Server est installé sur l'ordinateur, vous ne devez pas supprimer GSKit s'il est utilisé. Si vous voulez utiliser la dernière version de GSKit, vous devez utiliser IBM Installation Manager pour modifier la fonction GSKit et la supprimer de son registre. Vous pouvez ensuite désinstaller GSKit.

Désinstallation d'IBM Global Security Kit avec SMIT

Utilisez la commande **smit** pour désinstaller IBM Global Security Kit (GSKit) sur un système AIX.

Procédure

1. Connectez-vous en tant qu'utilisateur root.
2. Accédez à l'invite de commande.
3. Lancez la commande **smit**. La fenêtre **Maintenance et installation de logiciels** s'ouvre.

4. Sélectionnez **Installation et maintenance de logiciels** > **Maintenance et utilitaires logiciels**.
5. Sélectionnez **Supprimer les logiciels installés**.
6. Dans la zone **Nom du logiciel**, appuyez sur la touche **F4** pour afficher la liste des logiciels installés. Vous pouvez entrer la valeur `GSKit` dans la zone pour lister tous les modules GSKit.
7. Définissez la valeur de **REMOVE dependent software** sur `YES` pour supprimer automatiquement les produits et les mises à jour logiciels dépendants du produit que vous supprimez.
8. Sélectionnez les modules à supprimer, puis appuyez sur la touche Entrée.
9. Vérifiez si la désinstallation de GSKit a abouti.

   ```
   lslpp -l 'GSK*'
   ```

Désinstallation d'IBM Global Security Kit à l'aide de la commande `installp`

Utilisez la commande **`installp`** pour désinstaller IBM Global Security Kit (GSKit) sur un système AIX.

Procédure

1. Connectez-vous en tant qu'utilisateur root.
2. Accédez à l'invite de commande.
3. Lancez la commande ci-après pour déterminer les modules GSKit à désinstaller.

   ```
   lslpp -l 'GSK*'
   ```
4. Pour supprimer un module GSKit, entrez la commande ci-après.

   ```
   installp -u nom_module
   ```

   Pour désinstaller entièrement GSKit, retirez tous les modules GSKit de la même version. Pour désinstaller GSKit, vous devez commencer par supprimer le module GSKit SSL avant de retirer le module GSKit crypt. Pour supprimer les modules `GSKit8.gsksslx64.ppc.rte` and `GSKit8.gskcryptx64.ppc.rte`, exécutez la commande ci-après.

   ```
   installp -u GSKit8.gsksslx64.ppc.rte
   installp -u GSKit8.gskcryptx64.ppc.rte
   ```
5. Vérifiez si la désinstallation de GSKit a abouti.

   ```
   lslpp -l 'GSK*'
   ```

Désinstallation d'IBM Global Security Kit à l'aide des utilitaires Linux

Utilisez la commande **`rpm`** pour désinstaller IBM Global Security Kit (GSKit) sur un système Linux.

Pourquoi et quand exécuter cette tâche

L'exemple qui suit montre la désinstallation des modules GSKit sur un système AMD64 Opteron/EM64T Linux. Pour Linux System z, System i, System p ou System x, remplacez les noms de module par des noms appropriés.

Procédure

1. Connectez-vous en tant qu'utilisateur root.
2. Accédez à l'invite de commande.

3. Lancez la commande ci-après pour déterminer les modules GSKit à désinstaller.
   ```
   rpm -qa | grep -i gsk
   ```
4. Pour supprimer un module GSKit, entrez la commande ci-après.
   ```
   rpm -ev
   nom_module
   ```

   Pour désinstaller entièrement GSKit, retirez tous les modules GSKit de la même version. Pour désinstaller GSKit, vous devez commencer par supprimer le module GSKit SSL avant de retirer le module GSKit crypt. Pour supprimer les modules `gskssl64-8.0-14.26.x86_64` et `gskcrypt64-8.0-14.26.x86_64`, exécutez la commande ci-après.
   ```
   rpm -ev gskssl64-8.0-14.26.x86_64
   rpm -ev gskcrypt64-8.0-14.26.x86_64
   ```
5. Vérifiez si la désinstallation de GSKit a abouti.
   ```
   rpm -qa | grep -i gsk
   ```

Désinstallation d'IBM Global Security Kit à l'aide des utilitaires Solaris

Utilisez la commande **pkgrm** pour désinstaller IBM Global Security Kit (GSKit) sur un système Solaris.

Procédure

1. Connectez-vous en tant qu'utilisateur root.
2. Accédez à l'invite de commande.
3. Lancez la commande ci-après pour déterminer les modules GSKit à désinstaller.
   ```
   pkginfo | grep -i gsk
   ```
4. Pour supprimer un module GSKit, entrez la commande ci-après.
   ```
   pkgrm nom_module
   ```

   Pour désinstaller entièrement GSKit, retirez tous les modules GSKit de la même version. Pour désinstaller GSKit, vous devez commencer par supprimer le module GSKit SSL avant de retirer le module GSKit crypt. Pour supprimer les modules `gsk8ssl64` et `gsk8cry64`, exécutez la commande ci-après.
   ```
   pkgrm gsk8ssl64
   pkgrm gsk8cry64
   ```
5. Vérifiez si la désinstallation de GSKit a abouti.
   ```
   pkginfo | grep -i gsk
   ```

Désinstallation d'IBM Global Security Kit à l'aide des utilitaires HP-UX

Utilisez la commande **swremove** pour désinstaller IBM Global Security Kit (GSKit) sur un système HP-UX.

Procédure

1. Connectez-vous en tant qu'utilisateur root.
2. Accédez à l'invite de commande.
3. Lancez la commande ci-après pour déterminer les modules GSKit à désinstaller.
   ```
   swlist | grep -i gsk
   ```
4. Pour supprimer un module GSKit, entrez la commande ci-après.
   ```
   swremove nom_progiciel
   ```

Pour désinstaller entièrement GSKit, retirez tous les modules GSKit de la même version. Pour désinstaller GSKit, vous devez commencer par supprimer le module GSKit SSL avant de retirer le module GSKit crypt. Pour supprimer les modules `gskssl64` et `gskcrypt64`, exécutez la commande ci-après.

```
swremove gskssl64
swremove gskcrypt64
```

5. Vérifiez si la désinstallation de GSKit a abouti.

```
swlist | grep -i gsk
```

Désinstallation d'IBM Global Security Kit sous Windows

Utilisez les commandes IBM Global Security Kit (GSKit) pour exécuter la désinstallation de GSKit depuis un système Windows.

Pourquoi et quand exécuter cette tâche

L'exemple illustre la désinstallation en mode silencieux des modules GSKit SSL 64 bits et GSKit crypt 64 bits depuis un système Windows sur une architecture AMD64/EM64T. Pour un système d'exploitation Windows Windows sur une architecture IA32/x86, les noms du module GSKit sont différents. Pour plus d'informations sur le nom des modules, voir Chapitre 10, «Installation d'IBM Global Security Kit», à la page 57.

Remarque : Vous pouvez aussi utiliser **Démarrer** > **Panneau de configuration** > **Ajouter/supprimer des programmes** pour supprimer les modules GSKit.

Procédure

1. Connectez-vous en tant que membre du groupe des administrateurs.
2. Accédez à l'invite de commande.
3. Le répertoire de travail en cours doit être le répertoire `gskit` dans lequel l'installable d'IBM Global Security Kit est stocké.
4. Pour désinstaller les modules GSKit 64 bits en mode silencieux, exécutez les commandes suivantes : Pour désinstaller entièrement GSKit, retirez tous les modules GSKit de la même version. Pour désinstaller GSKit, vous devez commencer par supprimer le module GSKit SSL avant de retirer le module GSKit crypt.

```
gsk8ssl64.exe /s /x /v"/quiet"
gsk8crypt64.exe /s /x /v"/quiet"
```

Désinstallation des modules de langue

Pour désinstaller IBM Security Directory Server, vous devez aussi désinstaller les modules de langue que vous avez installés sur votre ordinateur.

Si vous avez installé IBM Security Directory Server et les modules de langue sur votre ordinateur avec IBM Installation Manager, vous devez utiliser IBM Installation Manager pour désinstaller les modules de langue.

Si vous avez utilisé les utilitaires du système d'exploitation pour installer les modules de langue, utilisez-les aussi pour les désinstaller.

Tous les modules de langue sont désinstallés du système si vous ne sélectionnez pas la fonction serveur proxy ou serveur pour l'installation.

Désinstallation des modules de langue à l'aide des utilitaires du système d'exploitation

Utilisez les utilitaires du système d'exploitation pour exécuter la désinstallation des modules de langue si vous les avez installés avec ces utilitaires.

Avant de commencer

Vous devez arrêter tous les processus IBM Security Directory Server client et serveur avant la désinstallation des modules de langue d'IBM Security Directory Server.

- Serveur d'annuaire
- Serveur d'administration
- Traces LDAP
- Applications LDAP personnalisées

Procédure

1. Connectez-vous en tant qu'utilisateur root.
2. Accédez à l'invite de commande.
3. Déterminez les modules de langue que vous voulez supprimer sur votre ordinateur :

Système d'exploitation	Commande à exécuter :
AIX	`lslpp -l 'idsldap.msg631*'`
Linux	`rpm -qa | grep -i idsldap-msg631`
Solaris	`pkginfo | grep IDSl`

4. Pour désinstaller le module de langue d'une langue, exécutez les commandes de désinstallation du module. L'exemple suivant illustre la désinstallation du module de langue français. Vous pouvez désinstaller n'importe quel module de langue en remplaçant les noms du module appropriés par le nom de votre choix correspondant au système d'exploitation.

Système d'exploitation	Commande à exécuter :
AIX	`installp -u idsldap.msg631.fr_FR`
Linux	`rpm -ev idsldap-msg631-fr-6.3.1-0.noarch.rpm`
Solaris	`pkgrm IDSlfr631`

5. Vérifiez la bonne installation du module de langue. Pour plus d'informations, voir «Vérification des modules d'IBM Security Directory Server», à la page 87.

Annexe A. Directory Services Markup Language

Le langage DSML (Directory Services Markup Language) peut être utilisé pour représenter les informations sur la structure de l'annuaire, les requêtes et les mises à jour de l'annuaire, et les résultats des opérations sur l'annuaire au format XML.

Lorsque vous installez l'outil d'administration Web d'IBM Security Directory Server, une archive de fichiers DSML, `DSML.zip`, est copiée sur l'ordinateur. Le fichier `DSML.zip` est stocké dans le sous-répertoire `idstools` du répertoire d'installation d'IBM Security Directory Server. Pour plus d'informations sur le répertoire d'installation par défaut d'IBM Security Directory Server, voir «Emplacements d'installation par défaut», à la page 27.

Le fichier `DSML.zip` contient l'installable DSML et la documentation relative à l'installation, la configuration et l'utilisation de DSML. Le fichier `DSML.zip` contient les fichiers suivants :

`DSMLReadme.txt`
: Le fichier `DSMLReadme.txt` contient la liste des fichiers du module, ainsi que des instruction d'installation et de configuration de DSML.

`dsml.pdf`
: Le fichier `dsml.pdf` est au format PDF et décrit l'utilisation de DSML.

`dsml.htm`
: Le fichier `dsml.htm` est au format HTML et décrit l'utilisation de DSML.

Annexe B. Chargement d'une base de données exemple et démarrage du serveur

Chargez la base de données exemple et démarrez le serveur d'annuaire afin d'ajouter, mettre à jour et rechercher des entrées.

Avant de commencer

Créez une instance de serveur d'annuaire. Voir «Création d'une instance de serveur d'annuaire», à la page 137.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser l'Outil de configuration pour charger les données LDIF sur un serveur d'annuaire et démarrer le serveur.

Procédure

1. Pour utiliser l'Outil de configuration, lancez la commande ci-après.
   ```
   idsxcfg -I nom_instance
   ```
2. Dans la zone de de navigation de gauche, cliquez sur **Tâches LDIF** > **Importer des données LDIF**.
3. Dans la zone **Chemin d'accès et nom du fichier LDIF**, entrez le chemin et le nom du fichier LDIF. Vous pouvez également cliquer sur Parcourir et spécifier le fichier de données LDIF. Chemin d'accès et fichier de données LDIF sur les différents systèmes d'exploitation :

   Windows
   chemin_installation\examples\sample.ldif

   AIX et Solaris
   /opt/IBM/ldap/V6.3.1/examples/sample.ldif

   Linus /opt/ibm/ldap/V6.3.1/examples/sample.ldif
4. Cliquez sur **Importation standard**.
5. Cliquez sur **Importer**.
6. Pour démarrer l'instance de serveur d'annuaire, procédez comme suit.
   a. Dans la zone de navigation de gauche, cliquez sur **Gérer l'état du serveur**.
   b. Cliquez sur **Démarrer le serveur**.

Annexe C. Mise à jour manuelle du fichier ldapdb.properties

Si vous installez IBM Security Directory Server sur un ordinateur qui ne contient pas une version compatible d'IBM DB2, le fichier ldapdb.properties n'est pas rempli pendant l'installation. Dans ce cas, vous devez installer une version prise en charge d'IBM DB2, puis mettre à jour manuellement le fichier ldapdb.properties.

Avant de commencer

Le module du serveur d'annuaire complet doit être installé.

Procédure

1. Installez une version compatible d'IBM DB2, si cela n'est pas déjà fait.
2. Lancez la commande **db2ls** pour lister les versions de DB2 qui sont installées sur l'ordinateur et leur chemin d'installation.
3. Mettez à jour le fichier ldapdb.properties avec la version de DB2 compatible et le chemin d'installation . Emplacement par défaut du fichier ldapdb.properties et exemples de valeur pour les différents systèmes d'exploitation :

   Microsoft Windows

   ```
   C:\Program Files\IBM\ldap\V6.3.1\etc\ldapdb.properties

   currentDB2InstallPath=C:\Program Files\IBM\SQLLIB
   currentDB2Version=9.7.0.6
   ```

   AIX et Solaris

   ```
   /opt/IBM/ldap/V6.3.1/etc/ldapdb.properties

   currentDB2InstallPath=/opt/IBM/db2/V9.7
   currentDB2Version=9.7.0.6
   ```

   Linux `/opt/ibm/ldap/V6.3.1/etc/ldapdb.properties`

   ```
   currentDB2InstallPath=/opt/ibm/db2/V9.7
   currentDB2Version=9.7.0.6
   ```

4. Enregistrez le fichier ldapdb.properties.

Annexe D. Fonctions d'accessibilité de Security Directory Server

Les fonctions d'accessibilité permettent aux utilisateurs souffrant d'un handicap physique, comme une mobilité réduite ou une déficience visuelle, de pouvoir utiliser correctement les produits informatiques.

Les principales fonctions d'accessibilité de ce produit permettent aux utilisateurs d'effectuer les opérations ci-après.

- Utiliser les technologies d'assistance, telles que les logiciels de lecture d'écran, pour entendre ce qui apparaît à l'écran. Pour plus d'informations sur l'utilisation de ces technologies avec ce produit, consultez la documentation du produit relative à celles-ci.
- Accéder à des fonctions spécifiques ou équivalentes à l'aide du clavier uniquement.
- Agrandir les éléments affichés à l'écran.

En outre, la documentation du produit a été modifiée pour inclure les fonctions suivantes dans le but d'améliorer l'accessibilité :

- La documentation complète est disponible au format HTML pour permettre à un maximum d'utilisateurs d'employer un logiciel de lecture d'écran.
- Toutes les images figurant dans la documentation sont accompagnées d'un texte pour que les utilisateurs malvoyants puissent comprendre le contenu des images.

Accessibilité

La liste suivante répertorie les principales fonctions d'accessibilité de IBM Security Directory Server.

- Prise en charge d'opérations effectuées uniquement à l'aide du clavier
- Prise en charge d'interfaces fréquemment utilisées par les lecteurs d'écran
- Les touches sont identifiables au toucher et ne s'activent pas par simple effleurement

La documentation d'IBM Security Directory Server est dotée de fonctions d'accessibilité. Ces fonctions sont décrites dans la documentation en ligne.

Navigation à l'aide du clavier

Le produit utilise des raccourcis clavier standard qui sont documentés par le système d'exploitation. Pour plus d'informations, consultez la documentation fournie par votre système d'exploitation.

Ce produit utilise des touches de navigation standard Microsoft Windows.

Agrandissement des éléments affichés à l'écran

Vous pouvez agrandir les informations affichées dans les fenêtres du produit à l'aide des fonctions fournies par les systèmes d'exploitation sur lesquels s'exécute le produit. Par exemple, dans un environnement Microsoft Windows, vous pouvez réduire la résolution de l'écran afin d'agrandir la taille de police du texte à l'écran.

Pour plus d'informations, consultez la documentation fournie par votre système d'exploitation.

IBM et l'accessibilité

Pour plus d'informations sur les engagements d'IBM en matière d'accessibilité, voir le site IBM Human Ability and Accessibility Center : `http://www.ibm.com/able`

Index

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W

Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service IBM puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

Pour le Canada, veuillez adresser votre courrier :

IBM Director of Commercial Relations
IBM Canada Ltd.
3600 Steeles Avenue East
Markham, Ontario
L3R 9Z7
Canada

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues par écrit à l'adresse suivante :

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japon

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales.

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT. IBM DECLINE TOUTE RESPONSABILITE, EXPLICITE OU IMPLICITE, RELATIVE AUX INFORMATIONS QUI Y SONT CONTENUES, Y COMPRIS EN CE QUI CONCERNE LES GARANTIES DE VALEUR MARCHANDE OU D'ADAPTATION A VOS BESOINS.

Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Corporation
2Z4A/101
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 dispositions du Livret contractuel IBM, des Conditions Internationales d'Utilisation de 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.

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

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

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 lesquels ils ont été écrits ou aux interfaces de programmation IBM. Ces exemples de programmes n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation IBM.

Toute copie intégrale ou partielle de ces exemples de programmes et des oeuvres qui en sont dérivées doit inclure une mention de droits d'auteur libellée comme suit :

© (nom de votre société) (année). Des segments de code sont dérivés des Exemples de programmes IBM Corp. © Copyright IBM Corp. _saisissez l'année ou les années_. All rights reserved.

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

Marques déposées

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corp. dans de nombreux pays. Les autres noms de produits et de services peuvent être des marques d'IBM ou d'autres sociétés. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript et toutes les marques incluant Adobe sont des marques d'Adobe Systems Incorporated aux Etats-Unis et/ou dans certains autres pays.

IT Infrastructure Library est une marque de The Central Computer and Telecommunications Agency qui fait désormais partie de The Office of Government Commerce.

Intel, le logo Intel, Intel Inside, le logo Intel Inside, Intel Centrino, le logo Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium et Pentium sont des marques d'Intel Corporation ou de ses filiales aux Etats-Unis et dans certains autres pays.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

ITIL est une marque de The Office of Government Commerce et est enregistrée au bureau américain Patent and Trademark Office.

UNIX est une marque enregistrée de The Open Group aux Etats-Unis et/ou dans certains autres pays.

Java ainsi que tous les logos et toutes les marques incluant Java sont des marques d'Oracle et/ou de ses sociétés affiliées.

Cell Broadband Engine est une marque de Sony Computer Entertainment, Inc. aux Etats-Unis et/ou dans certains autres pays, utilisée sous licence.

Linear Tape-Open, LTO, le logo LTO, Ultrium et le logoUltrium sont des marques d'HP, IBM Corp. et Quantum aux Etats-Unis et dans d'autres pays.

SC11-6792-02