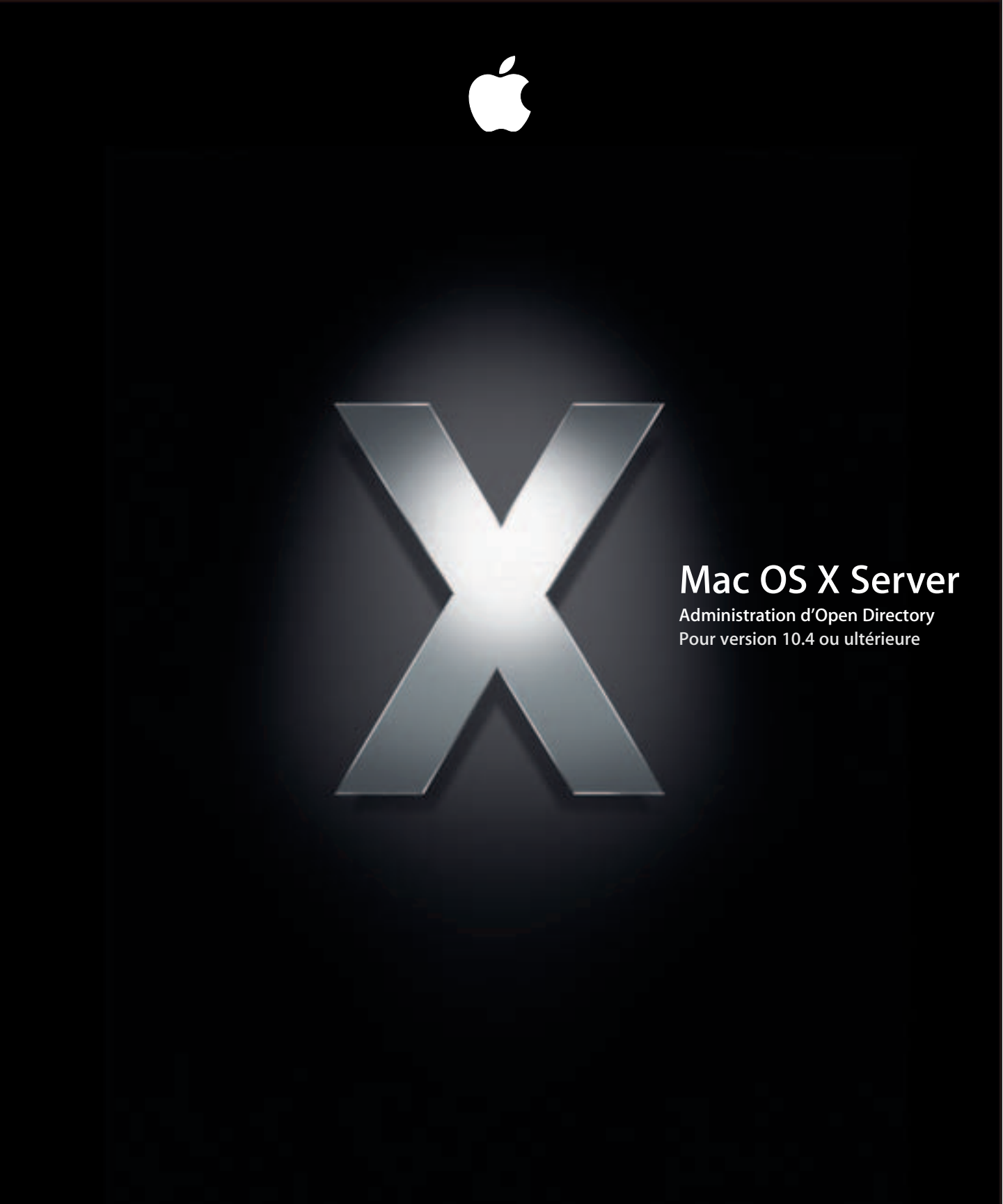

Mac OS X Server
Administration d'Open Directory
Pour version 10.4 ou ultérieure

Apple
1 Infinite Loop
Cupertino CA 95014-2084
www.apple.com

F019-0166/03-24-05

Table des matières

À propos de ce guide

Ce guide décrit les services de répertoire et d'authentification que vous pouvez configurer à l'aide de Mac OS X Server. Il explique aussi comment configurer les ordinateurs clients Mac OS X Server et Mac OS X pour les services de répertoire et la détection de services de réseau.

Open Directory de Mac OS X Server fournit des services de répertoire et d'authentification pour réseaux mixtes d'ordinateurs Mac OS X, Windows et UNIX. Open Directory utilise OpenLDAP, l'implémentation open source du protocole Lightweight Directory Access Protocol (LDAP), pour fournir des services de répertoire. OpenLDAP est compatible avec d'autres serveurs LDAP basés sur des standards et peut être intégré à des services propriétaires comme, par exemple, Active Directory de Microsoft et eDirectory de Novell. Pour la base de données LDAP principale, Open Directory utilise Berkeley DB, un système de gestion de bases de données open source. C'est une base de données très extensible pour l'indexation à hautes performances de centaines de milliers de comptes d'utilisateur et d'autres enregistrements.

Le module externe Open Directory permet à un client Mac OS X ou Mac OS X Server de lire et d'écrire des informations faisant autorité sur les ressources d'utilisateur et de réseau provenant de n'importe quel serveur LDAP, même Active Directory, le système propriétaire de Microsoft. Le serveur peut aussi accéder à des enregistrements qui se trouvent dans des répertoires hérités comme, par exemple, NIS, NetInfo et des fichiers de configuration BSD locaux (/etc).

Open Directory fournit aussi un service d'authentification. Il peut stocker et valider en toute sécurité les mots de passe des utilisateurs désireux de se connecter à des ordinateurs clients de votre réseau ou d'utiliser d'autres ressources réseau qui nécessitent une authentification. Open Directory permet également d'appliquer certaines politiques concernant notamment l'expiration des mots de passe ou leur longueur minimale. Open Directory peut en outre authentifier des utilisateurs d'ordinateurs Windows pour la connexion à des domaines, le service de fichiers et d'autres services Windows fournis par Mac OS X Server.

Un centre de distribution de clés (KDC) Kerberos MIT est entièrement intégré à Open Directory et fournit une authentification sécurisée qui prend en charge la signature unique. Cela signifie que les utilisateurs ne doivent s'authentifier qu'une seule fois, avec une seule et unique paire nom d'utilisateur/mot de passe, pour accéder à l'ensemble des services de réseau pour lesquels Kerberos a été activé. Pour les services qui n'acceptent pas l'authentification Kerberos, le service Secure Authentication and Service Layer (SASL) intégré négocie automatiquement le mécanisme d'authentification le plus sûr possible.

De plus, la réplication de répertoires et d'authentification optimise la disponibilité et l'extensibilité. En créant des répliques des serveurs Open Directory, vous pouvez aisément maintenir des serveurs de basculement ainsi que des serveurs distants pour l'interaction rapide entre les clients sur des réseaux distribués.

Open Directory gère aussi la détection des services de réseau. Mac OS X et Mac OS X Server peuvent utiliser Open Directory pour détecter les services de réseau, comme, par exemple, les serveurs de fichiers, qui se manifestent par l'intermédiaire de protocoles de détection de services tels que Bonjour, AppleTalk, SLP ou SMB/CIFS.

Nouveautés de la version 10.4

Mac OS X Server 10.4 offre les améliorations majeures suivantes dans Open Directory :

- **Configuration simplifiée de l'accès LDAPv3 :** format de répertoire vous aide à configurer une connexion vers un répertoire LDAP.
- **Liaison de répertoire LDAPv3 sécurisée :** établit une connexion d'authentification mutuelle entre le répertoire LDAP et ses clients. Le client prouve son identité au répertoire LDAP et le répertoire prouve son authenticité au client.
- **Intégration Active Directory améliorée :** les répertoires de départ réseau des utilisateurs de Mac OS X peuvent être montés à partir de l'emplacement spécifié dans Active Directory. Vous pouvez mapper plusieurs attributs Mac OS X — identifiant d'utilisateur, identifiant de groupe principal d'utilisateur et identifiant de groupe — à des attributs Active Directory existants.
- **Serveur LDAP amélioré :** Mac OS X Server 10.4 utilise OpenLDAP 2.2.19 et Berkeley DB 4.2.52.
- **Archivage et restauration simplifiés :** cliquez sur un bouton pour sauvegarder ou restaurer des bases de données de répertoire et d'authentification.
- **Authentification améliorée :** vous pouvez connecter un serveur à un royaume Kerberos Active Directory ou à un royaume Kerberos MIT. Les comptes d'utilisateur locaux peuvent utiliser davantage de méthodes d'authentification.
- **Sécurité du stockage des mots de passe configurable :** les méthodes d'authentification peuvent être désactivées de manière sélective afin de rendre plus sûr le stockage des mots de passe sur le serveur.
- **Réplication des schémas LDAP :** le répertoire LDAP peut stocker son propre schéma personnalisé et le propager du maître Open Directory à toutes ses répliques.

Contenu de ce guide

Le présent guide contient les chapitres suivants :

- le chapitre 1, "Service de répertoire avec Open Directory" présente les domaines de répertoire, la façon dont ils sont organisés et utilisés. Il décrit également comment la détection des services de réseau est intégrée aux services de répertoires.
- le chapitre 2, "Politiques de recherche Open Directory" présente les politiques de recherche pour un ou plusieurs domaines de répertoire et décrit les politiques de recherche automatisées, personnalisées ou locales uniquement.
- le chapitre 3, "Authentification Open Directory" décrit l'authentification Open Directory, les mots de passe shadow et cryptés, Kerberos, la liaison LDAP et la signature unique.
- le chapitre 4, "Planification Open Directory" vous aide à déterminer vos besoins en matière de domaines de répertoire, à estimer vos exigences en matière de répertoires et d'authentification, à identifier les serveurs pour l'hébergement des domaines partagés, à améliorer les performances et la redondance, à gérer la réplication dans un campus multiliaison et à sécuriser vos services Open Directory. Ce chapitre présente également les outils de gestion des services Open Directory.
- le chapitre 5, "Configuration des services Open Directory" indique comment définir le rôle Open Directory de Mac OS X Server : serveur autonome, connecté à un système de répertoire, maître Open Directory ou réplique Open Directory. Vous apprendrez également comment régler certaines options du service LDAP d'un maître ou d'une réplique Open Directory et comment faire migrer un domaine de répertoire de NetInfo vers LDAP. Enfin, ce chapitre explique comment configurer l'authentification Kerberos par signature unique sur un maître Open Directory.
- le chapitre 6, "Gestion de l'authentification d'utilisateur" montre comment définir des politiques de mot de passe, modifier le type de mot de passe d'un utilisateur, attribuer des droits d'administrateur pour l'authentification Open Directory, réinitialiser les mots de passe de comptes d'utilisateurs importés et faire migrer des mots de passe vers l'authentification Open Directory.
- le chapitre 7, "Gestion de Format de répertoire" explique comment utiliser l'application Format de répertoire pour activer, désactiver et configurer des protocoles de détection de services. Il explique également comment configurer des politiques de recherche d'authentification et de contacts, et comment configurer l'accès à différents domaines de répertoire : LDAP, Active Directory, NIS, fichiers de configuration BSD et NetInfo.
- le chapitre 8, "Maintenance et résolution des problèmes" explique comment contrôler les services Open Directory, visualiser et modifier directement les données des répertoires à l'aide de l'Inspecteur et effectuer d'autres opérations de maintenance de répertoire. Ce chapitre donne également des solutions à certains problèmes que vous pourriez rencontrer.
- l'Annexe "Données de répertoire Mac OS X" présente la liste des extensions Open Directory au schéma LDAP et spécifie les types d'enregistrements et d'attributs standard de Mac OS X.
- le glossaire définit les termes utilisés dans ce guide.

Remarque : étant donné qu'Apple publie régulièrement de nouvelles versions et mises à jour de ses logiciels, les illustrations de ce document peuvent être différentes de celles qui s'affichent à l'écran.

Utilisation de ce guide

Les chapitres de ce guide sont classés dans l'ordre correspondant probablement le mieux à vos besoins de configuration et de gestion d'Open Directory sur votre serveur.

- Lisez le chapitre 1 jusqu'au le chapitre 3 pour vous familiariser avec les concepts d'Open Directory : services de répertoires, politiques de recherche et authentification.
- Lisez le chapitre 4 lorsque vous êtes prêt à planifier les services de répertoires et l'authentification des mots de passe pour votre réseau.
- Après cette étape de planification, utilisez les instructions du chapitre 5 pour configurer les services Open Directory.
- Lorsque vous avez besoin de définir des politiques de mot de passe ou de modifier les réglages de mot de passe d'un compte d'utilisateur, reportez-vous aux instructions du chapitre 6.
- Si vous devez configurer ou modifier la façon dont un ordinateur Mac OS X ou Mac OS X Server accède à des domaines de répertoire, suivez les instructions du chapitre 7.
- Pour la maintenance courante des services de répertoires et d'authentification, consultez le chapitre 8.

Utilisation de l'aide à l'écran

Vous pouvez afficher des instructions et d'autres informations utiles sur la suite serveur en utilisant l'aide à l'écran.

Sur un ordinateur sous Mac OS X Server, vous pouvez accéder à l'aide à l'écran après avoir ouvert Gestionnaire de groupe de travail ou Admin Serveur. À partir du menu d'aide, sélectionnez l'une des options :

- *Aide Gestionnaire de groupe de travail* ou *Aide Admin Serveur* affiche des informations sur l'application.
- *Aide Mac OS X Server* affiche la page d'aide principale du serveur, à partir de laquelle vous pouvez rechercher des informations sur le serveur.
- *Documentation* vous permet d'accéder au site www.apple.com/fr/server/documentation, à partir duquel vous pouvez télécharger la documentation du serveur.

Vous pouvez également accéder à l'aide à l'écran à partir du Finder ou d'autres applications d'un serveur ou d'un ordinateur administrateur. (Un ordinateur administrateur est un ordinateur Mac OS X sur lequel des logiciels d'administration de serveur sont installés.) Utilisez le menu Aide pour ouvrir Visualisation Aide, puis choisissez Bibliothèque > Aide Mac OS X Server.

Pour consulter les toutes dernières rubriques d'aide, assurez-vous que l'ordinateur serveur ou administrateur est connecté à Internet lorsque vous utilisez Visualisation Aide. Visualisation Aide extrait et met en cache automatiquement les toutes dernières rubriques d'aide sur Internet concernant le serveur. Lorsque vous n'êtes pas connecté à Internet, Visualisation Aide affiche les rubriques d'aide mises en cache.

La suite Mac OS X Server

La documentation de Mac OS X Server comprend une série de guides présentant les services offerts ainsi que les instructions relatives à leur configuration, leur gestion et leur dépannage. Tous les guides sont disponibles au format PDF via : www.apple.com/fr/server/documentation.

Ce guide ...	explique comment :
Mac OS X Server Premiers contacts avec la version 10.4 ou ultérieure	installer Mac OS X Server et le configurer pour la première fois.
Mac OS X Server Mise à niveau et migration vers la version 10.4 ou ultérieure	utiliser les données et réglages des services actuellement utilisés sur les versions antérieures du serveur.
Mac OS X Server Gestion utilisateur pour la version 10.4 ou ultérieure	créer et gérer les utilisateurs, groupes et listes d'ordinateurs ; configurer les préférences gérées des clients Mac OS X.
Mac OS X Server Administration du service de fichiers pour la version 10.4 ou ultérieure	partager des volumes ou dossiers de serveur sélectionnés parmi les clients du serveur via les protocoles suivants : AFP, NFS, FTP et SMB/CIFS.
Mac OS X Server Administration du service d'impression pour la version 10.4 ou ultérieure	héberger les imprimantes partagées et gérer les files d'attente et travaux d'impression associés.
Mac OS X Server Administration de mises à jour de logiciels et d'images de système pour la version 10.4 ou ultérieure	utiliser NetBoot et Installation en réseau pour créer des images disque à partir desquelles les ordinateurs Macintosh peuvent démarrer sur le réseau ; configurer un serveur de mise à jour de logiciels pour la mise à jour d'ordinateurs clients via le réseau.
Mac OS X Server Administration du service de courrier pour la version 10.4 ou ultérieure	installer, configurer et administrer les services de courrier sur le serveur.
Mac OS X Server Administration de technologies Web pour la version 10.4 ou ultérieure	configurer et gérer un serveur Web, dont WebDAV, WebMail, et les modules Web.
Mac OS X Server Administration de services de réseaux pour la version 10.4 ou ultérieure	installer, configurer et administrer DHCP, DNS, VPN, NTP, coupe-feu IP et services NAT sur le serveur.
Mac OS X Server Administration d'Open Directory pour la version 10.4 ou ultérieure	gérer les services de répertoires et d'authentification.

Ce guide ...	explique comment :
Mac OS X Server Administration du Serveur Enchaînement QuickTime pour la version 10.4 ou ultérieure	configurer et gérer les services d'enchaînement QuickTime.
Mac OS X Server Administration des services Windows pour la version 10.4 ou ultérieure	configurer et gérer des services tels que PDC, BDC, fichiers et impression pour les utilisateurs d'ordinateurs Windows.
Mac OS X Server Migration à partir de Windows NT pour la version 10.4 ou ultérieure	déplacer des comptes, des dossiers partagés et des services à partir de serveurs Windows NT vers Mac OS X Server.
Mac OS X Server Administration du serveur d'applications Java pour la version 10.4 ou ultérieure	configurer et administrer un serveur d'applications JBoss sur Mac OS X Server.
Mac OS X Server Administration de la ligne de commande pour la version 10.4 ou ultérieure	utiliser les commandes et les fichiers de configuration pour exécuter les tâches d'administration du serveur via l'interpréteur de commandes UNIX.
Mac OS X Server Administration des services de collaboration pour la version 10.4 ou ultérieure	configurer et gérer Weblog, la discussion en ligne et d'autres services qui facilitent les interactions entre utilisateurs.
Mac OS X Server Administration de la haute disponibilité pour la version 10.4 ou ultérieure	gérer le basculement, l'agrégation des liens, l'équilibrage de charge et d'autres configurations matérielles et logicielles pour garantir la haute disponibilité des services de Mac OS X Server
Mac OS X Server Administration d'Xgrid pour la version 10.4 ou ultérieure	gérer des clusters de calcul Xserve à l'aide de l'application Xgrid.
Mac OS X Server Glossaire : inclut la terminologie pour Mac OS X Server, Xserve, Xserve RAID et Xsan	interpréter les termes utilisés pour les produits de serveur et les produits de stockage.

Obtention de mises à jour de documentation

Apple publie régulièrement de nouvelles rubriques d'aide à l'écran, des guides révisés et des documents de solutions. Les nouvelles rubriques d'aide incluent des mises à jour des guides les plus récents.

- Pour afficher de nouvelles rubriques d'aide à l'écran, assurez-vous que votre ordinateur serveur ou administrateur est connecté à Internet et cliquez sur le lien Informations de dernière minute dans la page d'aide principale de Mac OS X Server.
- Pour télécharger les guides et documents de solutions les plus récents au format PDF, rendez-vous à la page Web de documentation de Mac OS X Server : www.apple.com/fr/server/documentation.

Obtention d'informations supplémentaires

Pour plus d'informations, consultez les ressources suivantes :

Documents Ouvrez-moi—mises à jour importantes et informations spécifiques. Recherchez-les sur les disques du serveur.

Site Web de Mac OS X Server (www.apple.com/fr/macosx/server)—passerelle vers des informations détaillées sur des produits et technologies.

Site Web Service & Support AppleCare (www.apple.com/fr/support)—accès à des centaines d'articles provenant de l'organisation d'assistance d'Apple.

Formation des clients Apple (train.apple.com)—cours en salle et autoformations afin de développer vos compétences en termes d'administration de serveur.

Groupes de discussion Apple (discussions.info.apple.com)—moyen de partager des questions, des connaissances et des conseils avec d'autres administrateurs.

Répertoire de liste de diffusion Apple (www.lists.apple.com)—abonnez-vous à des listes de diffusion afin de pouvoir communiquer par courrier électronique avec d'autres administrateurs.

Site Web d'OpenLDAP (www.openldap.org)—découvrez le logiciel open source utilisé par Open Directory pour fournir le service de répertoires LDAP.

Site Web de Kerberos MIT (web.mit.edu/kerberos/www)—obtenez des informations élémentaires et des spécifications sur les protocoles utilisés par Open Directory pour fournir une authentification par signature unique robuste.

Site Web de Berkeley DB (www.sleepycat.com)—consultez des descriptions de fonctionnalités et de la documentation technique sur la base de données open source utilisée par Open Directory pour stocker les données des répertoires LDAP.

RFC3377, "Lightweight Directory Access Protocol (v3): Spécification technique" (www.rfc-editor.org/rfc/rfc3377.txt)—accédez à huit autres documents RFC (Request for Comment) qui contiennent des informations d'ensemble et des spécifications détaillées sur le protocole LDAPv3.

Service de répertoire avec Open Directory

1

Un service de répertoire est un lieu de stockage centralisé d'informations concernant les utilisateurs d'ordinateurs et les ressources réseau d'une organisation.

Le fait de centraliser les données administratives en un seul endroit présente plusieurs avantages :

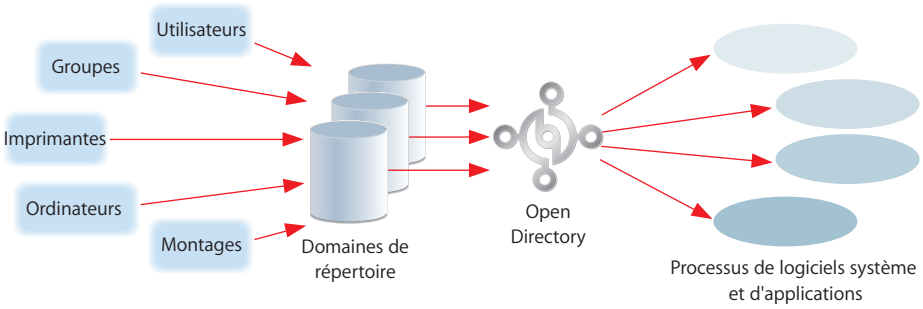
- Réduction du nombre de données à saisir.
- Tous les clients et les services réseau disposent d'informations cohérentes en ce qui concerne les utilisateurs et les ressources.
- L'administration des utilisateurs et des ressources est simplifiée.
- Fournit des informations d'identification, d'authentification et d'autorisation à d'autres services de réseau.

Dans les écoles ou les entreprises par exemple, ils sont parfaits pour gérer les utilisateurs et les ressources informatiques. Même une organisation de moins de dix personnes peut bénéficier des avantages du déploiement d'un service de répertoire.

Les services de répertoires peuvent offrir deux types d'avantages. Ils simplifient d'une part l'administration du système et du réseau, et d'autre part l'usage du réseau pour les utilisateurs. Grâce aux services de répertoire, les administrateurs peuvent conserver des informations sur tous les utilisateurs, comme, par exemple, leur nom, leur mot de passe les emplacements des répertoires de départ réseau, de façon centrale plutôt que sur les différents ordinateurs. Les services de répertoire permettent aussi de centraliser les informations concernant les imprimantes, les ordinateurs et les autres ressources en réseau. La centralisation des informations concernant les utilisateurs et les ressources peut réduire la charge de travail que représente la gestion des informations pour l'administrateur réseau. Et chaque utilisateur dispose d'un compte d'utilisateur centralisé pour la connexion à tout ordinateur autorisé sur le réseau. Avec le service de répertoire et le service de fichiers centralisés et configurés pour héberger les répertoires de départ réseau, un utilisateur obtient partout les mêmes répertoire de départ, bureau personnalisé et préférences individuelles, quel que soit l'ordinateur sur lequel il se connecte. L'utilisateur peut donc toujours accéder à ces fichiers personnels et localiser en toute simplicité les ressources réseau autorisées en vue de les utiliser.

Services et domaines de répertoire

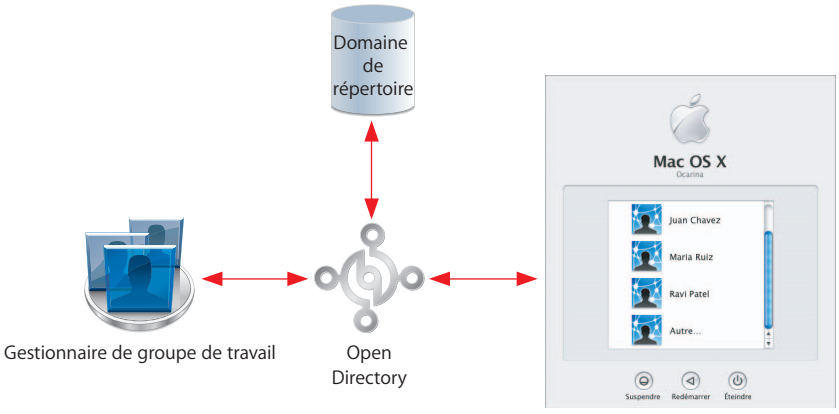
Le service de répertoire agit comme un intermédiaire entre les processus d'application et de logiciel système, qui ont besoin d'informations sur les utilisateurs et les ressources, et les *directory domains* qui stockent les informations. Sous Mac OS X et Mac OS X Server, c'est Open Directory qui fournit les services de répertoire. Open Directory peut accéder aux informations d'un ou plusieurs domaines de répertoire.



Un domaine de répertoire stocke des informations dans une base de données spécialisée et optimisée pour traiter un grand nombre de requêtes d'informations ainsi que pour les trouver et les récupérer rapidement.

Les processus exécutés sous ordinateurs Mac OS X utilisent les services Open Directory pour enregistrer des informations dans les domaines de répertoire. Si par exemple vous créez un compte d'utilisateur à l'aide de Gestionnaire de groupe de travail, cette application demande à Open Directory de stocker le nom de l'utilisateur et les autres informations du compte dans un domaine de répertoire. Bien entendu, vous pouvez ensuite afficher les informations des comptes d'utilisateur à l'aide de Gestionnaire de groupe de travail qui demande à Open Directory de récupérer les informations d'utilisateur à partir d'un domaine de répertoire.

D’autres processus de logiciels système et d’applications peuvent également accéder aux informations des comptes d’utilisateur stockées dans des domaines de répertoire. Quand un utilisateur ouvre une session sur un ordinateur Mac OS X, le processus d’ouverture de session utilise les services Open Directory pour valider le nom d’utilisateur et le mot de passe.

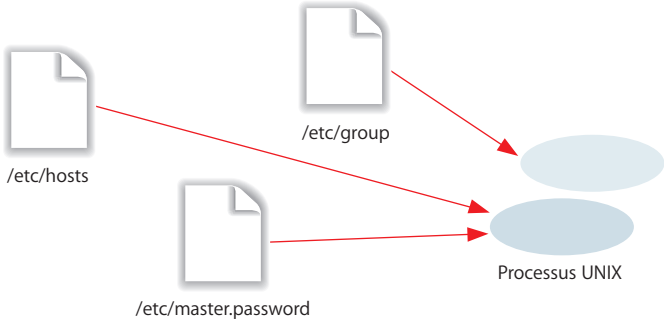


Point de vue historique

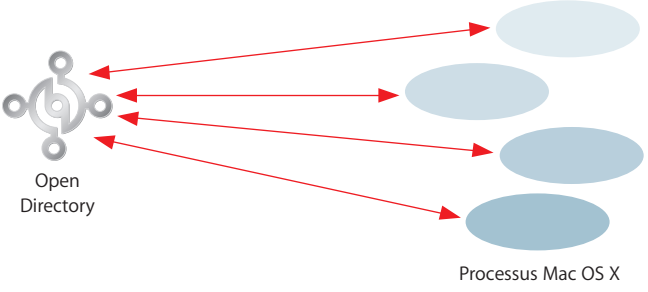
Tout comme Mac OS X, Open Directory trouve ses origines dans UNIX. En effet, Open Directory fournit l’accès aux données administratives que les systèmes UNIX conservent généralement dans des fichiers de configuration, ce qui requiert un travail de maintenance plus méticuleux (certains systèmes UNIX reposent toujours sur des fichiers de configuration). Open Directory consolide ces données, puis les répartit pour faciliter les accès comme la maintenance.

Consolidation des données

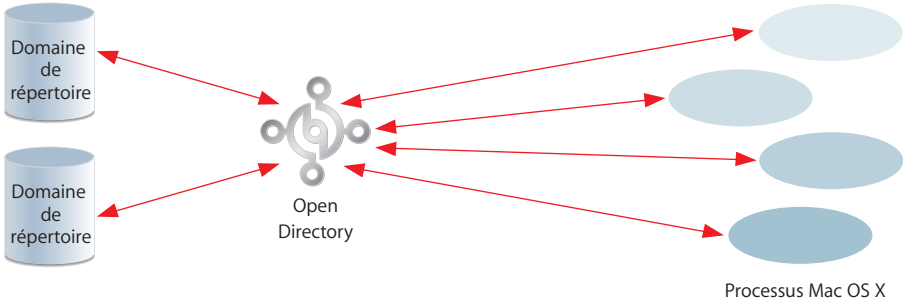
Depuis des années, les systèmes UNIX stockent les informations administratives dans une série de fichiers située dans le répertoire "/etc". Ce schéma exige que chaque ordinateur UNIX dispose de sa propre série de fichiers. Ainsi, les processus exécutés sur un ordinateur UNIX lisent ses fichiers, lorsqu'ils ont besoin d'informations administratives. Si vous maîtrisez l'environnement UNIX, vous connaissez sans aucun doute les fichiers du répertoire /etc : group, hosts, hosts.equiv, master.passwd et bien d'autres. Ainsi, un processus UNIX ayant besoin d'un mot de passe d'utilisateur consultera le fichier /etc/master.passwd. Le fichier /etc/master.passwd contient un enregistrement pour chaque compte d'utilisateur. Un autre processus UNIX nécessitant des informations sur les groupes utilise plutôt le fichier /etc/group.



Open Directory consolide les informations administratives, ce qui simplifie les interactions entre les processus et les données administratives qu'ils créent et utilisent.



Les processus n'ont désormais plus besoin de savoir où et comment les données administratives sont stockées. Open Directory s'occupe d'obtenir ces données pour leur compte. Si un processus doit connaître l'emplacement du répertoire de départ d'un utilisateur, il fait simplement en sorte qu'Open Directory obtienne cette information. Open Directory localise les informations recherchées, puis les renvoie, évitant ainsi au processus tous les détails concernant le stockage des informations. Si vous avez configuré Open Directory pour accéder aux données administratives dans plusieurs directory domains, Open Directory les consulte automatiquement en cas de besoin.



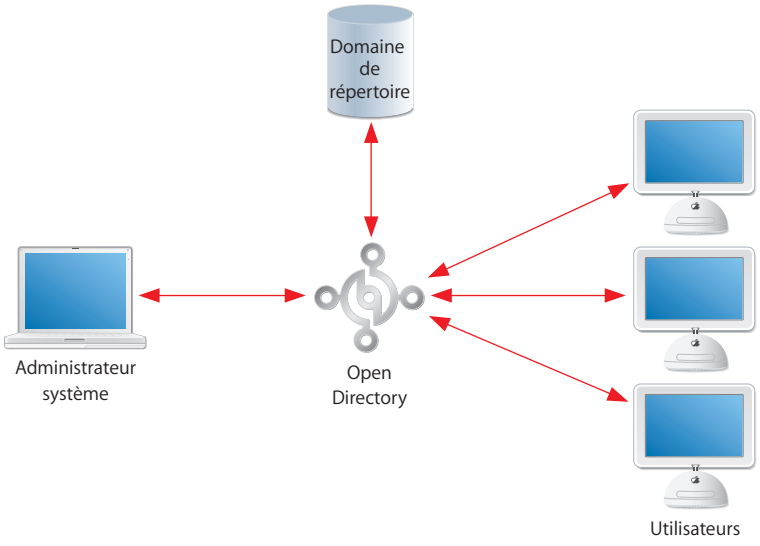
Certaines des données stockées dans un directory domain sont identiques à celles stockées dans les fichiers de configuration UNIX. Par exemple, l'emplacement du répertoire de départ, le nom réel, l'identifiant d'utilisateur et l'identifiant de groupe sont stockés dans l'enregistrement d'utilisateur d'un directory domain plutôt que dans le fichier /etc/passwd standard. Toutefois, un directory domain stocke beaucoup d'informations supplémentaires pour gérer des fonctions propres à Mac OS X comme la prise en charge de la gestion d'ordinateurs clients Mac OS X.

Répartition des données

Autre caractéristique des fichiers de configuration UNIX, les données administratives qu'ils contiennent sont disponibles uniquement sur l'ordinateur sur lequel elles sont stockées. Chaque ordinateur comporte donc ses propres fichiers de configuration UNIX. Avec les fichiers de configuration UNIX, tout ordinateur sur lequel un utilisateur envisage de travailler doit posséder les réglages du compte de cet utilisateur. De manière plus générale, tout ordinateur doit donc posséder les réglages des comptes des utilisateurs autorisés à les utiliser. Pour configurer les réglages de réseau d'un ordinateur, l'administrateur doit se déplacer jusqu'à cet ordinateur, puis entrer directement l'adresse IP et toute information identifiant cet ordinateur sur le réseau.

De même, lorsque des informations sur un utilisateur ou le réseau doivent être modifiées dans des fichiers de configuration UNIX, l'administrateur doit apporter ces modifications sur l'ordinateur sur lequel sont situés ces fichiers. Certains changements, comme les réglages de réseau, nécessitent que l'administrateur procède aux mêmes opérations sur plusieurs ordinateurs. Cette approche devient de plus en plus compliquée alors que les réseaux gagnent en taille et en complexité.

Open Directory résout ce problème en vous permettant de stocker des données administratives dans un domaine de répertoire qui peut être géré par un administrateur réseau à partir d'un emplacement unique. Open Directory vous permet de répartir ces informations, afin qu'elles soient accessibles en réseau pour tous les ordinateurs qui en ont besoin et pour l'administrateur qui les gère.



Utilisation des données des répertoires

Open Directory permet de regrouper et de gérer aisément les informations sur le réseau dans un directory domain, mais ces informations n'ont de valeur que si les processus du logiciel système et des applications exécutés sur les ordinateurs du réseau y accèdent réellement.

Voici quelques exemples d'utilisation des données de répertoire par le logiciel système et les applications Mac OS X :

- **Ouverture de session :** comme nous l'avons déjà mentionné, Gestionnaire de groupe de travail peut créer des enregistrements d'utilisateurs dans un directory domain et ces enregistrements peuvent servir à authentifier des utilisateurs ouvrant une session sur des ordinateurs Mac OS X et Windows. Lorsqu'un utilisateur saisit un nom et un mot de passe dans la fenêtre d'ouverture de session Mac OS X, le processus d'ouverture de session demande à Open Directory d'authentifier ce nom et ce mot de passe. Open Directory utilise le nom pour trouver l'enregistrement du compte de l'utilisateur dans un directory domain et valide ensuite le mot de passe à l'aide d'informations supplémentaires fournies par l'enregistrement de l'utilisateur.

- **Accès aux dossiers et aux fichiers :** une fois qu'il a ouvert une session, l'utilisateur peut accéder aux dossiers et aux fichiers. Mac OS X utilise d'autres données provenant de l'enregistrement d'utilisateur pour déterminer les autorisations d'accès de l'utilisateur pour chaque fichier ou dossier.
- **Répertoires de départ :** chaque enregistrement d'utilisateur d'un directory domain stocke l'emplacement du répertoire de départ de l'utilisateur concerné, également appelé "dossier de départ". Il s'agit de l'endroit où sont stockés les fichiers, dossiers et préférences de l'utilisateur Le répertoire de départ d'un utilisateur peut être situé sur l'ordinateur sur lequel il travaille ou sur un serveur de fichiers de réseau.
- **Montage automatique de points de partage :** les points de montage peuvent être configurés pour le montage automatique (ils apparaissent automatiquement) dans le dossier /Network (le globe Réseau) des fenêtres du Finder des ordinateurs clients. Les informations concernant ces points de partage à monter automatiquement sont stockées dans un domaine de répertoire. Les *points de partage* sont des dossiers, des disques ou des partitions de disque rendus accessibles sur le réseau.
- **Réglage des comptes de messagerie :** chaque enregistrement d'utilisateur d'un domaine de répertoire indique si l'utilisateur concerné dispose du service de messagerie et, le cas échéant, spécifie les protocoles de courrier à utiliser, le mode de présentation des messages entrants, l'activation éventuelle d'une alerte en cas de réception de message, etc.
- **Utilisation des ressources :** les quotas de disque, d'impression et de courrier peuvent être stockés dans chaque enregistrement d'utilisateur d'un domaine de répertoire.
- **Informations sur les clients gérés :** l'administrateur peut gérer l'environnement Mac OS X des utilisateurs dont les comptes sont stockés dans un domaine de répertoire. L'administrateur choisit les réglages de préférences imposés qui sont stockés dans le domaine de répertoire et qui sont prioritaires par rapport aux préférences personnelles des utilisateurs.
- **Gestion de groupes :** outre des enregistrements d'utilisateurs, un domaine de répertoire contient également des enregistrements de groupes.. Chaque fiche de groupe affecte tous les utilisateurs membres de ce groupe. Les informations contenues dans les fiches de groupes indiquent les réglages des préférences des membres. Les enregistrements de groupe permettent également de déterminer l'accès aux fichiers, aux dossiers et aux ordinateurs.
- **Présentations de réseau gérées** l'administrateur peut configurer des présentations personnalisées que les utilisateurs voient lorsqu'ils sélectionnent l'icône Réseau dans la barre latérale d'une fenêtre du Finder. Comme ces présentations de réseau gérées sont stockées dans un domaine de répertoire, elles sont automatiquement disponibles lorsqu'un utilisateur se connecte.

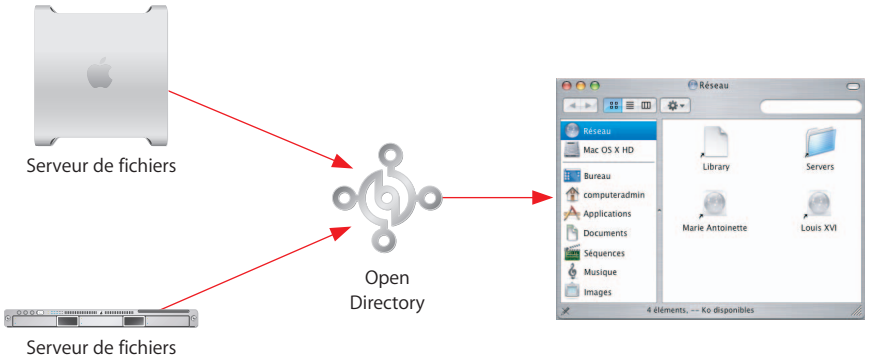
Accès aux services de répertoires

Open Directory peut accéder aux domaines de répertoire pour les types suivants de services de répertoires :

- Lightweight Directory Access Protocol (LDAP), une norme commune dans les environnements mixtes de systèmes Macintosh, UNIX et Windows. LDAP est le service de répertoire natif pour les répertoires partagés de Mac OS X Server.
- NetInfo, le service de répertoire du domaine de répertoire local sur tout système Mac OS X. Il s'agit du service de répertoire hérité de Mac OS X Server.
- Active Directory, le service de répertoire des serveurs Microsoft Windows 2000 et 2003.
- Network Information System (NIS), le service de répertoire de nombreux serveurs UNIX.
- Fichiers plats BSD, service de répertoire hérité des systèmes UNIX.

Détection de services de réseau

Open Directory offre bien plus que des données administratives stockées dans des répertoires. Il permet entre autres d'obtenir des informations sur les services disponibles sur le réseau. Open Directory est par exemple en mesure de fournir des informations sur les serveurs de fichiers accessibles.

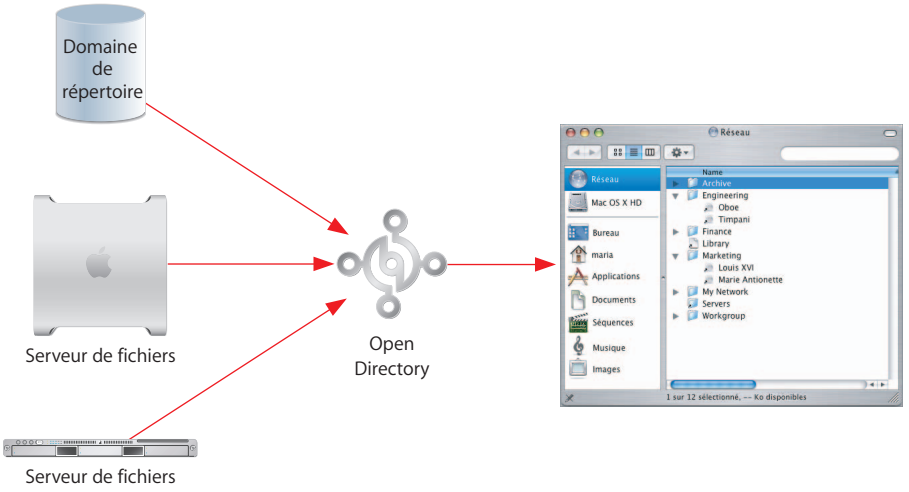


Open Directory peut détecter des services de réseau, afin de faire connaître leur existence et leur emplacement. Pour leur part, les services s'identifient au moyen de protocoles standard. Open Directory accepte les protocoles de détection de services suivants :

- Bonjour, le protocole d'Apple qui utilise le DNS multidiffusion pour détecter le partage de fichiers, d'imprimantes, de discussion en ligne, de musique et d'autres services sur les réseaux IP.
- AppleTalk, protocole hérité pour la détection de services réseau tels que les services de fichiers, d'impression, etc.
- Service Location Protocol (SLP), un protocole standard ouvert pour la détection de services de fichiers et d'impression sur les réseaux IP.
- Server Message Block/Common Internet File System (SMB/CIFS), le protocole utilisé par Microsoft Windows pour les services de fichiers, d'impression et pour d'autres services.

En fait, Open Directory peut fournir des informations sur les services de réseau, aussi bien à partir des protocoles de détection de services que des domaines de répertoire. Pour ce faire, Open Directory demande simplement à toutes ses sources le type d'information exigé par un processus Mac OS X. Les sources disposant du type d'information demandé le fournissent à Open Directory qui recueille toutes les informations fournies et les transmet au processus Mac OS X qui les a demandées.

Si Open Directory recherche par exemple des informations sur les serveurs de fichiers, ceux présents sur le réseau répondent via les protocoles de détection de services avec leurs propres informations. Un domaine de répertoire contenant des informations relativement statiques sur certains serveurs de fichiers répond également à cette requête. Open Directory collecte alors toutes les informations provenant des protocoles de détection de services et des domaines de répertoire.



Dans le cas où Open Directory recherche des informations sur un utilisateur, les protocoles de détection de services ne sont pas en mesure de répondre, car ils ne disposent d'aucune information concernant les utilisateurs (En théorie, AppleTalk, Bonjour, SMB/CIFS et SLP pourraient fournir des informations sur les utilisateurs, mais ils ne disposent en réalité d'aucune information à fournir sur ces derniers). Les informations collectées par Open Directory proviennent donc d'autres sources, les domaines de répertoire.

Au sein d'un domaine de répertoire

Les informations d'un domaine de répertoire sont organisées d'après le *type d'enregistrement*. Les types d'enregistrement sont des catégories spécifiques d'informations, comme, par exemple, les utilisateurs, les groupes et les ordinateurs. Un domaine de répertoire peut contenir un nombre quelconque d'enregistrements, quel que soit leur type. Chaque enregistrement est constitué d'un ensemble d'attributs et chaque attribut comporte une ou plusieurs valeurs. Si vous imaginez un type d'enregistrement comme une feuille de calcul dédiée à une certaine catégorie d'informations, les enregistrements sont alors les lignes de la feuille, les attributs sont les colonnes et chaque cellule contient une ou plusieurs valeurs.

Par exemple, lorsque vous définissez un compte d'utilisateur à l'aide de Gestionnaire de groupe de travail, vous créez un enregistrement d'utilisateur (un enregistrement de type utilisateur). Les réglages définis pour ce compte d'utilisateur (son nom abrégé, son nom complet, l'emplacement de son répertoire de départ, etc.) deviennent des valeurs des attributs qui figurent dans l'enregistrement. La fiche d'utilisateur comme les valeurs de ses attributs sont stockées dans un domaine de répertoire.

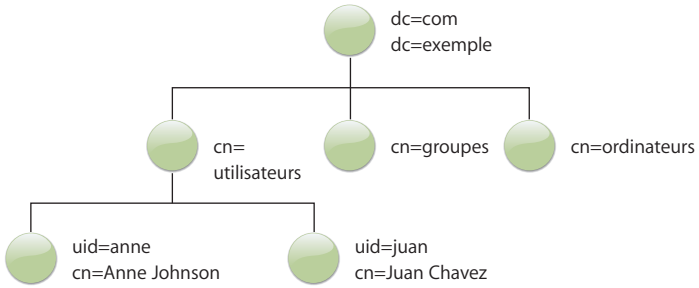
Dans certains services de répertoire, comme, par exemple, LDAP et Active Directory, les informations de répertoire sont organisées par *classe d'objets*. Comme les types d'enregistrement, les classes d'objets définissent des catégories d'informations. Une classe d'objets définit des objets d'informations similaires appelés *entrées* en spécifiant les attributs qu'une entrée peut ou doit contenir. Pour une classe d'objets particulière, un domaine de répertoire peut contenir plusieurs entrées et chaque entrée peut contenir plusieurs attributs. Certains attributs ont une seule valeur, d'autres en ont plusieurs. Par exemple, la classe d'objets inetOrgPerson définit les entrées qui contiennent des attributs d'utilisateur. La classe inetOrgPerson est une classe LDAP standard définie par le document RFC 2798. D'autres classes d'objets et attributs LDAP standard sont définis par le document RFC 2307. Les classes d'objets et les attributs par défaut d'Open Directory se fondent sur ces documents RFC.

L'ensemble des attributs et des types d'enregistrements (ou classes d'objets) définissent la structure des informations d'un domaine de répertoire. Cette structure est appelée *schéma* du domaine de répertoire.

Structure des informations de répertoire LDAP

Dans un répertoire LDAP, les entrées sont organisées dans une structure arborescente hiérarchique. Dans certains répertoires LDAP, cette structure est basée sur des frontières géographiques et organisationnelles. D'une façon plus générale, la structure est basée sur les noms de domaine Internet.

Dans une organisation de répertoire simple, les entrées représentant les utilisateurs, les groupes, les ordinateurs et les autres classes d'objets sont immédiatement sous le niveau racine de la hiérarchie.



Une entrée est référencée par son *nom distinctif* (DN, Distinguished Name), qui est construit à partir du nom de l'entrée proprement dite, appelé le *nom distinctif relatif* (RND, Relative Distinguished Name), et d'une concaténation des noms des entrées ancêtres. Par exemple, l'entrée d'Anne Jacques pourrait avoir le RDN "uid=anne" et le "uid=anne, cn=utilisateurs, dc=exemple, dc=com."

Le service LDAP extrait les données en faisant une recherche dans la hiérarchie d'entrées. La recherche peut commencer à n'importe quelle entrée. L'entrée à laquelle la recherche commence est appelée la *base de recherche*. Vous pouvez spécifier une base de recherche en donnant le nom distinctif d'une entrée dans le répertoire LDAP. Par exemple, la base de recherche "cn=utilisateurs, dc=exemple, dc=com" spécifie que le service LDAP commencera la recherche à l'entrée dont l'attribut "cn" a la valeur "utilisateurs".

Vous pouvez aussi spécifier dans combien de niveaux de la hiérarchie LDAP sous la base de recherche il faut chercher. L'étendue de recherche peut contenir toutes les sous-branches sous la base de recherche ou uniquement le premier niveau d'entrée sous la base de recherche. Si vous utilisez des outils de ligne de commande pour faire une recherche dans un répertoire LDAP, vous pouvez aussi restreindre l'étendue de la recherche à la seule entrée de la base de recherche.

Domaines de répertoire locaux et partagés

L'emplacement de stockage des informations concernant les utilisateurs et autres données administratives nécessaires à votre serveur est déterminé par le fait que ces données doivent parfois être partagées. Ces informations peuvent être stockées dans le domaine de répertoire local du serveur ou dans un domaine de répertoire partagé.

À propos du domaine de répertoire local

Tout ordinateur Mac OS X dispose d'un domaine de répertoire local. Les données administratives contenues dans ce domaine local sont visibles *uniquement* par les applications et le logiciel système exécutés sur l'ordinateur hébergeant le domaine en question. Il s'agit du premier domaine consulté lorsque l'utilisateur ouvre une session ou exécute certaines opérations nécessitant des données stockées dans un domaine de répertoire.

Lorsqu'un utilisateur ouvre une session sur un ordinateur Mac OS X, Open Directory recherche l'enregistrement de cet utilisateur dans le domaine de répertoire local de l'ordinateur. S'il contient cette fiche (et que l'utilisateur a entré un mot de passe correct), la connexion se poursuit et l'utilisateur a alors accès à l'ordinateur.

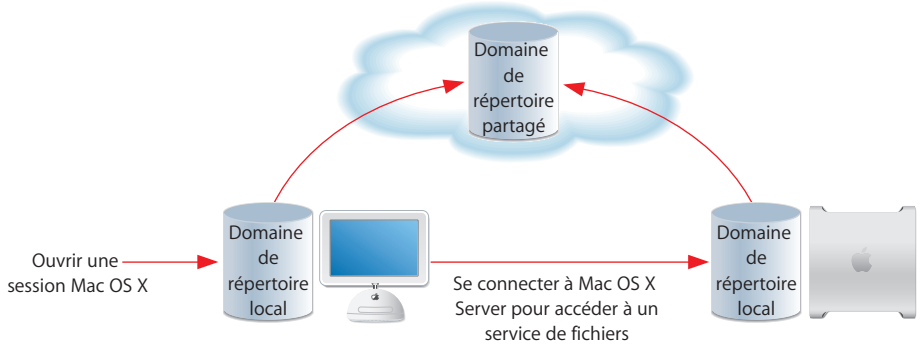
Après l'ouverture de session, l'utilisateur peut choisir "Se connecter à un serveur" dans le menu Aller, puis se connecter à un serveur Mac OS X Server pour accéder à un service de fichiers. Dans ce cas, Open Directory sur le serveur recherche la fiche de cet utilisateur dans le domaine de répertoire local du serveur. Si ce domaine contient cette fiche (et que l'utilisateur a entré un mot de passe correct), le serveur octroie à l'utilisateur l'accès aux services de fichiers.

Lorsque vous configurez pour la première fois un ordinateur Mac OS X, son domaine de répertoire local est automatiquement créé et rempli avec des enregistrements. Par exemple, une fiche d'utilisateur est créée pour l'utilisateur qui s'est chargé de l'installation. Elle contient le nom d'utilisateur et le mot de passe saisis au cours de l a configuration, ainsi que d'autres informations, telles qu'un identifiant unique pour l'utilisateur et l'emplacement de son répertoire de départ.

À propos des domaines de répertoire partagés

Même si sur tout ordinateur Mac OS X, Open Directory peut stocker des données administratives dans le domaine de répertoire local de l'ordinateur, son atout majeur est de permettre à plusieurs ordinateurs Mac OS X de partager des données administratives en les stockant dans des domaines de répertoire partagés. Lorsqu'un ordinateur est configuré pour utiliser un domaine partagé, toutes les données administratives contenues dans ce domaine sont également visibles par les applications et le logiciel système de cet ordinateur.

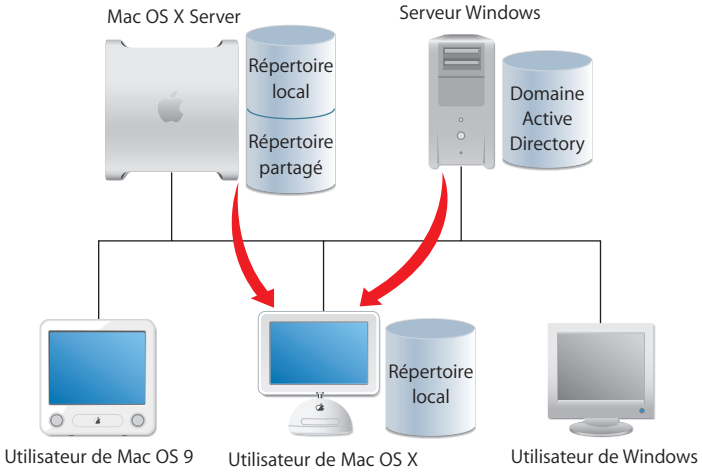
Si Open Directory ne trouve pas l'enregistrement d'un utilisateur dans le domaine local d'un ordinateur Mac OS X, il peut effectuer une recherche dans tous les domaines partagés auxquels cet ordinateur a accès. Dans l'exemple suivant, l'utilisateur peut accéder aux deux ordinateurs, car le domaine partagé, accessible à partir des deux ordinateurs, contient un enregistrement pour cet utilisateur.



Les domaines partagés se trouvent généralement sur des serveurs parce que les informations de domaines de répertoire contiennent des informations extrêmement importantes telles les données d'authentification des utilisateurs. L'accès aux serveurs est généralement très restreint pour protéger les données qu'ils contiennent. En outre, les données de répertoires doivent demeurer disponibles. Les serveurs disposent souvent de fonctions matérielles supplémentaires qui augmentent leur fiabilité et ils bénéficient habituellement de dispositifs d'alimentation électrique sans interruption.

Données partagées dans des domaines de répertoire existants

Certaines organisations (les universités ou les multinationales par exemple) conservent les informations sur leurs utilisateurs et d'autres données administratives dans des domaines de répertoire situés sur des serveurs UNIX ou Windows. Open Directory peut être configuré pour effectuer une recherche dans ces domaines non-Apple aussi bien que dans les domaines Open Directory partagés de systèmes Mac OS X Server.



L'ordre dans lequel Mac OS X effectue des recherches dans les domaines de répertoire est configurable. La politique de recherche détermine l'ordre dans lequel Mac OS X effectue les recherches dans les domaines de répertoire. Le prochain chapitre traite des politiques de recherche.

Politiques de recherche Open Directory

2

Chaque ordinateur dispose d'une politique de recherche qui spécifie un ou plusieurs domaines de répertoire et l'ordre dans lequel Open Directory y effectue ses recherches.

Chaque ordinateur Mac OS X a une *politique de recherche* qui spécifie les domaines de répertoire auxquels Open Directory peut accéder, comme le répertoire local de l'ordinateur et un répertoire partagé particulier. La politique de recherche spécifie également l'ordre dans lequel Open Directory accède aux domaines de répertoire. Open Directory recherche tour à tour dans chaque domaine de répertoire et s'arrête lorsqu'il trouve un élément correspondant. Ainsi, Open Directory stoppe la recherche d'un enregistrement d'utilisateur lorsqu'il trouve un enregistrement dont le nom d'utilisateur correspond au nom recherché.

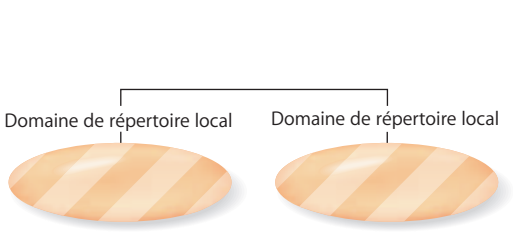
Une politique de recherche est aussi appelée un *chemin de recherche*.

Niveaux de politique de recherche

Une politique de recherche peut inclure le répertoire local seul, le répertoire local et un répertoire partagé ou le répertoire local et plusieurs répertoires partagés. Sur un réseau comportant un répertoire partagé, plusieurs ordinateurs accèdent généralement au répertoire partagé. Cette organisation est une structure arborescente, le répertoire partagé étant situé au sommet et les répertoires locaux se trouvant en bas.

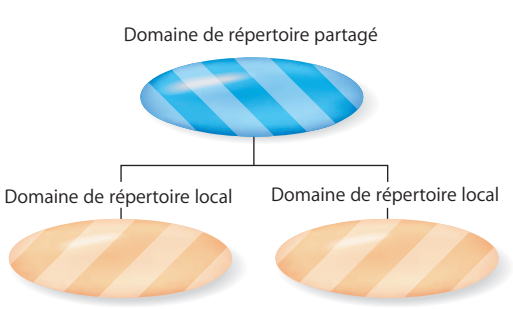
Politique de recherche de répertoire local

La politique de recherche la plus simple se compose uniquement du répertoire local d'un ordinateur. Dans ce cas, Open Directory recherche les données d'utilisateur et autres données administratives uniquement dans le domaine de répertoire local de chaque ordinateur. Si un serveur du réseau héberge un répertoire partagé, Open Directory n'y recherche pas d'informations d'utilisateur ou de données administratives car le répertoire partagé ne fait pas partie de la politique de recherche de l'ordinateur.

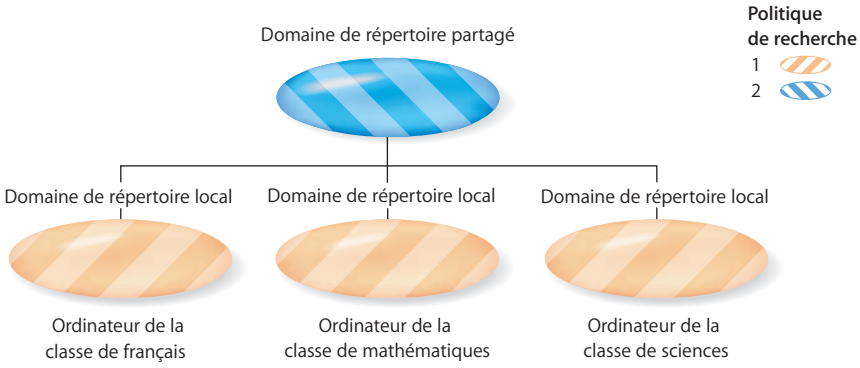


Politiques de recherche à deux niveaux

Si un des serveurs du réseau héberge un répertoire partagé, tous les ordinateurs du réseau peuvent inclure le répertoire partagé dans leurs politiques de recherche. Dans ce cas, Open Directory recherche les informations d'utilisateur et autres données administratives en commençant par le répertoire local. Si Open Directory ne trouve pas les informations dont il a besoin dans le répertoire local, il va chercher dans le répertoire partagé.

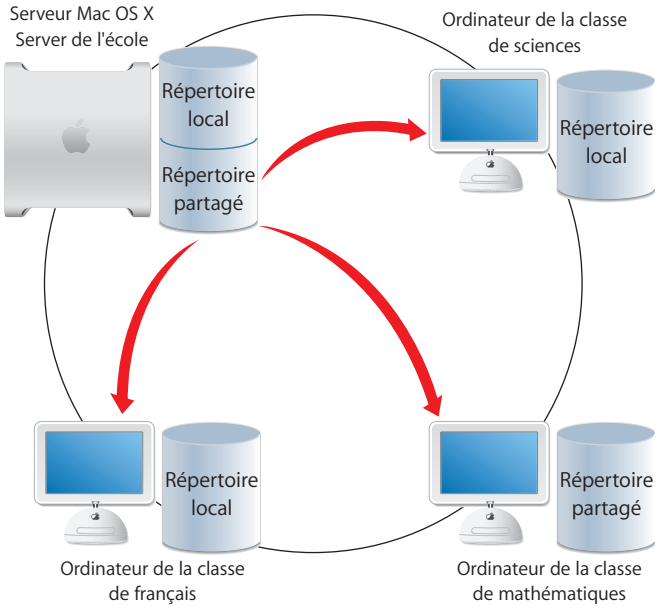


Voici un exemple d'utilisation de politique de recherche à deux niveaux :



Chaque classe (français, mathématiques, sciences) possède son propre ordinateur. Les étudiants de chaque classe sont définis en tant qu'utilisateurs du domaine local de l'ordinateur de cette classe. Ces trois domaines locaux partagent un même domaine, dans lequel sont définis tous les professeurs. Les professeurs, en tant que membres du domaine partagé, peuvent ouvrir une session sur n'importe quel ordinateur des classes. Les étudiants de chaque domaine local ne peuvent ouvrir une session que sur l'ordinateur où se trouve leur compte local.

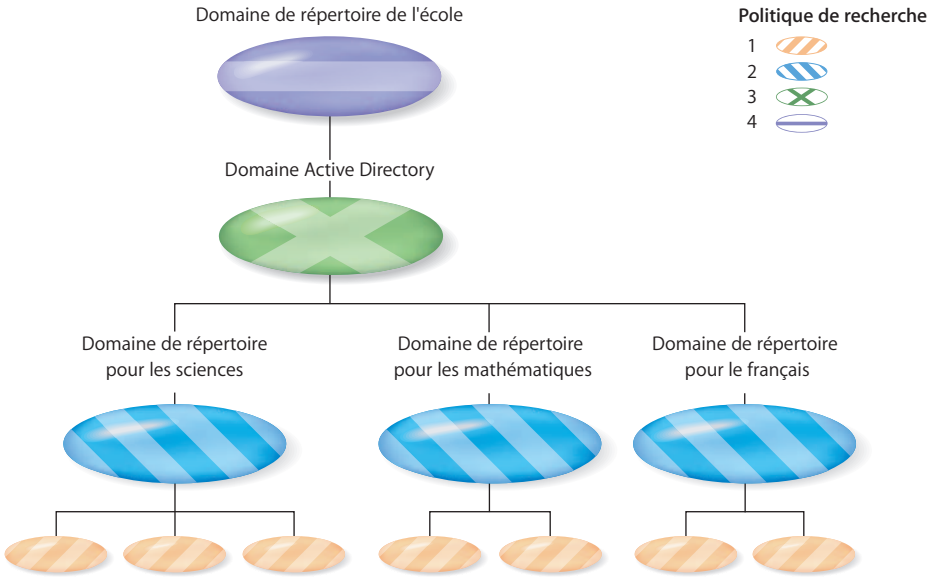
Alors que les domaines locaux résident chacun sur leurs ordinateurs respectifs, un domaine partagé se trouve sur un serveur accessible à partir de l'ordinateur d'un domaine local. Lorsqu'un professeur ouvre une session sur n'importe quel ordinateur des trois classes et qu'il est introuvable dans le domaine local, Open Directory recherche dans le domaine partagé. Dans cet exemple, il existe un seul domaine partagé, mais des réseaux plus complexes peuvent en contenir davantage.



Politiques de recherche multiniveaux

Si plusieurs serveurs du réseau hébergent un répertoire partagé, les ordinateurs du réseau peuvent inclure plusieurs répertoires partagés dans leurs politiques de recherche. Comme dans les politiques de recherche plus simples, Open Directory recherche toujours les informations d'utilisateur et autres données administratives en commençant par le répertoire local. Si Open Directory ne trouve pas les informations dont il a besoin dans le répertoire local, il les recherche tour à tour dans chaque répertoire partagé, dans l'ordre spécifié par la politique de recherche.

Voici un exemple d'utilisation de plusieurs répertoires partagés :



Chaque classe (français, mathématiques, sciences) possède un serveur qui héberge un domaine de répertoire partagé. La politique de recherche de chaque ordinateur de classe spécifie le domaine local de cet ordinateur, le domaine partagé de la classe et le domaine partagé de l'école. Les étudiants de chaque classe sont définis en tant qu'utilisateurs du domaine partagé du serveur de cette classe, ce qui les autorise à ouvrir une session sur tout ordinateur de leur classe. Les professeurs sont définis dans le domaine partagé du serveur de l'école, ce qui les autorise à ouvrir une session sur n'importe quel ordinateur de classe.

Il est possible d'affecter la totalité d'un réseau ou juste un groupe d'ordinateurs, en choisissant le domaine dans lequel seront définies les données administratives. Plus le niveau des données administratives dans une politique de recherche est élevé, moins il est nécessaire de les modifier au fur et à mesure de l'évolution des utilisateurs et des ressources système. Pour les administrateurs de services de répertoire, l'aspect le plus important est sans doute la planification des domaines de répertoire et des politiques de recherche. Ces éléments doivent refléter les ressources que vous souhaitez partager, les utilisateurs entre lesquels vous souhaitez les partager et même le mode de gestion de vos données de répertoire.

Politiques de recherche automatiques

Les ordinateursMac OS X peuvent être configurés pour définir leurs politiques de recherche automatiquement. Une politique de recherche automatique se compose de trois éléments, dont deux sont facultatifs :

- Domaine de répertoire local
- Domaines NetInfo partagés (facultatif)
- Répertoire LDAP partagé (facultatif)

La politique de recherche automatique d'un ordinateur commence toujours par son domaine de répertoire local. Lorsqu'un ordinateur Mac OS X n'est pas connecté à un réseau, l'ordinateur recherche les comptes d'utilisateur et autres données administratives uniquement dans son domaine de répertoire local.

La politique de recherche automatique détermine ensuite si l'ordinateur est configuré pour lier les domaines NetInfo partagés. L'ordinateur peut être lié à un domaine NetInfo partagé qui, à son tour, peut être lié à un autre domaine NetInfo partagé, etc. La liaison NetInfo, si elle existe, constitue la seconde partie sur laquelle porte la politique de recherche automatique. Pour plus d'informations, consultez la section "À propos de la liaison NetInfo" à la page 171.

Enfin, un ordinateur doté d'une politique de recherche automatique peut se lier à un répertoire LDAP partagé. Lorsque l'ordinateur démarre, il peut obtenir l'adresse d'un serveur de répertoire LDAP à partir d'un service DHCP. Le service DHCP de Mac OS X Server peut fournir une adresse de serveur LDAP de même qu'il fournit les adresses de serveurs DNS et d'un routeur. (Un service DHCP non-Apple peut également fournir une adresse de serveur LDAP ; cette caractéristique est connue sous le nom de DHCP option 95.)

Pour que le service DHCP de Mac OS X Server fournisse à ses clients une adresse de serveur LDAP particulière pour leurs politiques de recherche automatiques, vous devez configurer les options LDAP du service DHCP. Pour plus d'instructions, reportez-vous au chapitre DHCP du guide d'administration de services réseau.

Pour qu'un ordinateur Mac OS X obtienne l'adresse d'un serveur LDAP à partir du service DHCP :

- L'ordinateur doit être configuré pour utiliser une politique de recherche automatique. Cela inclut l'activation de l'option permettant d'ajouter des répertoires LDAP fournis par le DHCP. Consultez les sections "Configuration de politiques de recherche" à la page 126 et "Activation ou désactivation d'un répertoire LDAP fourni via DHCP" à la page 131.
- Les préférences Réseau de l'ordinateur doivent être configurées pour utiliser DHCP ou DHCP avec une adresse IP manuelle. Mac OS X est initialement configuré pour utiliser DHCP. Pour plus d'informations sur les réglages des préférences Réseau, consultez l'Aide Mac.

Une politique de recherche automatique offre confort et souplesse, particulièrement pour les ordinateurs portables. Lorsqu'un ordinateur doté d'une politique de recherche automatique est déconnecté du réseau, connecté à un autre réseau ou placé sur un autre sous-réseau, la politique de recherche automatique peut changer. Si l'ordinateur est déconnecté du réseau, il utilise son domaine de répertoire local. Si l'ordinateur est connecté à un réseau ou sous-réseau différent, il peut automatiquement changer sa liaison NetInfo et obtenir une adresse de serveur LDAP à partir du service DHCP du sous-réseau actuel. Avec une politique de recherche automatique, il n'est pas nécessaire de reconfigurer un ordinateur afin qu'il puisse obtenir les services de répertoires et d'authentification dans son nouvel emplacement.

Important : si vous configurez Mac OS X pour qu'il utilise une politique de recherche automatique d'authentification et un serveur LDAP fourni par DHCP ou un domaine NetInfo fourni par DHCP, vous augmenterez le risque de voir un attaquant prendre le contrôle de votre ordinateur. Le risque est encore plus élevé si votre ordinateur est configuré pour se connecter à réseau un sans fil. Pour plus de détails, consultez la rubrique "Protection d'ordinateurs contre un serveur DHCP malveillant" à la page 130

Politiques de recherche personnalisées

Si vous ne voulez pas qu'un ordinateur Mac OS X utilise la politique de recherche automatique fournie par DHCP, vous pouvez définir une politique de recherche personnalisée pour cet ordinateur. Par exemple, une politique de recherche personnalisée pourrait spécifier qu'il faut rechercher dans un domaine Active Directory avant de rechercher dans un domaine de répertoire d'un serveur Open Directory. Cela permettrait aux utilisateurs de se connecter à l'aide d'enregistrements d'utilisateur provenant du domaine Active Directory et d'avoir leurs préférences gérées par groupe et des fiches d'ordinateur provenant du domaine Open Directory.

Une politique de recherche personnalisée ne fonctionne généralement pas dans plusieurs emplacements de réseau, ni lorsque l'ordinateur n'est pas connecté à un réseau, car elle se base sur la disponibilité de domaines de répertoire spécifiques sur un réseau en particulier. Si un ordinateur portable est déconnecté de son réseau habituel, il n'aura plus accès aux domaines de répertoire partagés de sa propre politique de recherche personnalisée. L'ordinateur déconnecté aura toujours accès à son propre domaine de répertoire local car ce dernier est le premier domaine de répertoire dans toutes les politiques de recherche. L'utilisateur de l'ordinateur portable pourra se connecter à l'aide d'un enregistrement d'utilisateur du domaine de répertoire local, qui peut contenir des comptes d'utilisateur mobiles. Ceux-ci mettent en miroir les comptes d'utilisateur provenant du domaine de répertoire partagé auquel l'ordinateur portable accède lorsqu'il est connecté à son réseau habituel.

Politiques de recherche d'authentification et de contacts

Un ordinateur Mac OS X possède en réalité plusieurs politiques de recherche. Il possède une politique de recherche pour trouver des informations d'authentification et une autre politique de recherche pour trouver des informations de contacts. Open Directory utilise la politique de recherche d'authentification pour localiser et récupérer les données d'authentification d'utilisateur et d'autres données administratives à partir des domaines de répertoire. Il utilise la politique de recherche de contacts pour localiser et récupérer les noms, adresses et autres informations de contact à partir des domaines de répertoire. Le Carnet d'adresses de Mac OS X utilise ces informations de contact. D'autres applications peuvent être programmées pour les exploiter.

Chaque politique de recherche peut être automatique, personnalisée ou exclusivement locale.

Authentification Open Directory

3

Open Directory offre plusieurs options d'authentification des utilisateurs dont les comptes sont stockés dans des domaines de répertoire de Mac OS X Server, y compris Kerberos et les méthodes d'authentification traditionnelles requises par les services de réseau.

Open Directory peut authentifier les utilisateurs à l'aide :

- de l'authentification Kerberos pour la signature unique ;
- de méthodes d'authentification traditionnelles et d'un mot de passe stocké de façon sécurisée dans la base de données du serveur de mots de passe Open Directory ;
- de méthodes d'authentification traditionnelles et d'un mot de passe shadow stocké dans un fichier de mots de passe sécurisé pour chaque utilisateur ;
- d'un mot de passe crypté stocké directement dans le compte de l'utilisateur, pour une compatibilité descendante avec les systèmes hérités ;
- d'un serveur LDAP non Apple pour une authentification par liaison LDAP.

De plus, Open Directory permet de configurer une politique de mot de passe pour tous les utilisateurs ainsi que des politiques de mot de passe spécifiques pour chacun des utilisateurs, telles que l'arrivée à expiration automatique et la longueur minimale des mots de passe. (Les politiques de mot de passe ne s'appliquent ni aux administrateurs, ni à l'authentification par mot de passe crypté, ni à l'authentification par liaison LDAP.)

Types de mots de passe

Chaque compte d'utilisateur a un type de mot de passe qui détermine la façon dont le compte d'utilisateur est authentifié. Dans un domaine de répertoire local, le type de mot de passe par défaut est le mot de passe shadow. Sur un serveur mis à niveau à partir de Mac OS X Server 10.3, les comptes d'utilisateur du domaine de répertoire local peuvent aussi disposer d'un mot de passe de type Open Directory.

Pour les comptes d'utilisateur du répertoire LDAP de Mac OS X Server, le type de mot de passe par défaut est le type Open Directory. Les comptes d'utilisateur du répertoire LDAP peuvent aussi disposer d'un mot de passe de type mot de passe crypté.

Authentification et autorisation

Les services tels que la fenêtre de connexion et le service de fichiers Apple nécessitent une authentification de l'utilisateur à partir d'Open Directory. *L'authentification* fait partie du processus par lequel un service détermine s'il doit accorder à un utilisateur l'accès à une ressource. Généralement, ce processus nécessite également une *autorisation*. L'authentification prouve l'identité de l'utilisateur, tandis que l'autorisation détermine ce que l'utilisateur authentifié a le droit de faire. Un utilisateur s'authentifie généralement en fournissant un nom et un mot de passe valides. Un service peut alors autoriser l'utilisateur authentifié à accéder à des ressources spécifiques. Par exemple, le service de fichiers autorise l'accès complet aux dossiers et fichiers dont l'utilisateur authentifié est le possesseur.

Lorsque vous utilisez une carte de crédit, vous faites l'expérience de processus d'authentification et d'autorisation. Le commerçant vous identifie (authentification) en comparant votre signature sur la facture avec celle qui figure au dos de votre carte de crédit. Il soumet alors votre numéro de carte de crédit à la banque qui autorise le paiement en fonction du solde de votre compte et d'une limite de crédit autorisé.

Open Directory authentifie les comptes d'utilisateur et les listes de contrôle d'accès de service (SACL : "service access control list") autorisent l'utilisation de services. Si Open Directory vous authentifie, la SACL pour la fenêtre de connexion détermine si vous pouvez ouvrir une session, la SACL pour le service AFP détermine si vous pouvez vous connecter pour le service de fichiers, et ainsi de suite. Certains services déterminent aussi si un utilisateur est autorisé à accéder à des ressources particulières. Cette autorisation peut nécessiter l'extraction d'informations de compte d'utilisateur supplémentaires à partir du domaine de répertoire. Par exemple, le service AFP a besoin de l'identifiant d'utilisateur et d'informations sur l'adhésion de groupe pour déterminer les dossiers et les fichiers que l'utilisateur est autorisé à lire et/ou à écrire.

Mots de passe Open Directory

Lorsqu'un compte d'utilisateur dispose d'un type de mot de passe d'Open Directory, l'utilisateur peut être authentifié via Kerberos ou via le serveur de mots de passe Open Directory. Kerberos est un système d'authentification réseau qui utilise des références émises par un serveur sécurisé. Le serveur de mots de passe Open Directory prend en charge les méthodes d'authentification de mots de passe traditionnelles que certains clients de services de réseau requièrent. (Kerberos n'est pas disponible sur certains serveurs Open Directory, tels qu'un serveur mis à niveau possédant un répertoire NetInfo partagé plutôt qu'un répertoire LDAP).

Ni Kerberos ni le serveur de mots de passe Open Directory ne stockent le mot de passe dans le compte d'utilisateur. Tant Kerberos que le serveur de mots de passe Open Directory stockent les mots de passe dans des bases de données sécurisées en dehors du domaine de répertoire et n'autorisent jamais la lecture des mots de passe. Les mots de passe ne peuvent être que définis et vérifiés. Des utilisateurs malveillants peuvent tenter de se connecter via le réseau dans l'espoir d'accéder à Kerberos et au serveur de mots de passe Open Directory. L'examen de l'historique d'Open Directory permet de détecter ces tentatives d'accès infructueuses. (Consultez la section "Affichage des états et des historiques Open Directory" à la page 178.)

Les comptes d'utilisateur dans les domaines de répertoire suivants peuvent disposer de mots de passe Open Directory :

- Le répertoire LDAP de Mac OS X Server
- Le domaine de répertoire local de Mac OS X Server mis à niveau à partir des versions 10.2–10.3
- Un répertoire NetInfo partagé d'un serveur mis à niveau à partir de ou utilisant toujours Mac OS X Server 10.2

Remarque : les mots de passe Open Directory ne peuvent pas être utilisés pour ouvrir une session dans Mac OS X version 10.1 ou antérieure. Les utilisateurs qui doivent ouvrir une session à l'aide de la fenêtre de connexion de Mac OS X 10.1 ou antérieur doivent être configurés pour utiliser des mots de passe cryptés. Le type de mot de passe n'a pas d'importance pour les autres services. Par exemple, un utilisateur de Mac OS X 10.1 pourrait s'authentifier auprès du service de fichiers Apple à l'aide d'un mot de passe Open Directory.

Mots de passe shadow

Les mots de passe shadow prennent en charge les mêmes méthodes d'authentification traditionnelles que le serveur de mots de passe Open Directory. Ces méthodes d'authentification sont utilisées pour envoyer des mots de passe shadow via le réseau sous une forme brouillée ou hachée.

Un mot de passe shadow est stocké sous forme de plusieurs empreintes dans un fichier situé sur le même ordinateur que le domaine de répertoire accueillant le compte d'utilisateur. Etant donné que le mot de passe n'est pas stocké dans le compte d'utilisateur, sa capture via le réseau s'avère difficile. Chaque mot de passe shadow d'utilisateur est stocké dans un fichier différent, appelé fichier de mots de passe shadow. Seul le compte d'utilisateur racine est autorisé à lire ces fichiers.

Seuls les comptes d'utilisateur qui sont stockés dans le répertoire local d'un ordinateur peuvent disposer d'un mot de passe shadow. Les comptes d'utilisateur qui sont stockés dans un répertoire partagé ne peuvent en bénéficier.

Les mots de passe shadow fournissent également une authentification cachée pour les comptes d'utilisateur mobiles. Pour obtenir des informations complètes sur les comptes d'utilisateur mobiles, consultez le guide de gestion des utilisateurs.

Mots de passe cryptés

Un mot de passe crypté est stocké sous la forme d'une valeur cryptée, ou condensé numérique, dans le compte d'utilisateur. Cette stratégie, historiquement appelée authentification de base (Basic), est principalement compatible avec les logiciels qui nécessitent un accès direct aux enregistrements d'utilisateur. Par exemple, Mac OS X version 10.1 et les versions antérieures s'attendent à trouver un mot de passe crypté stocké dans le compte d'utilisateur.

L'authentification cryptée ne prend en charge que les mots de passe d'une longueur maximale de huit octets (huit caractères ASCII). Si un mot de passe plus long est saisi dans le compte d'un utilisateur, seuls les huit premiers octets sont utilisés pour la validation du mot de passe crypté. Les mots de passe shadow et Open Directory ne sont pas soumis à cette limite de longueur.

Pour une transmission sécurisée des mots de passe via un réseau, les mots de passe cryptés peuvent fonctionner avec la méthode d'authentification DHX.

Attaques hors ligne sur des mots de passe

Du fait que les mots de passe cryptés sont enregistrés directement dans les comptes d'utilisateur, ils sont susceptibles d'être craqués. Les comptes d'utilisateur qui se trouvent dans un domaine de répertoire partagé sont accessibles sur le réseau. N'importe quelle personne connectée au réseau et disposant de Gestionnaire de groupe de travail ou sachant utiliser les outils à lignes de commandes peut lire le contenu des comptes d'utilisateur, y compris les mots de passe qui y sont enregistrés. Notez que les mots de passe Open Directory et les mots de passe shadow ne sont pas stockés dans les comptes d'utilisateur ; ils ne peuvent donc pas être lus à partir des domaines de répertoire.

Un attaquant malveillant ou un pirate informatique pourrait utiliser Gestionnaire de groupe de travail ou des commandes UNIX pour copier des enregistrements d'utilisateur dans un fichier. Le pirate peut ensuite transférer ce fichier vers un autre système et utiliser différentes techniques pour décoder les mots de passe cryptés stockés dans les enregistrements d'utilisateur. Après avoir décodé un mot de passe crypté, le pirate peut se connecter incognito avec un nom d'utilisateur et un mot de passe crypté valides.

Avec ce type d'attaque "hors ligne", il n'est pas nécessaire d'effectuer plusieurs tentatives de connexion successives pour accéder à un système.

Un moyen très efficace pour contrer le craquage de mots de passe consiste à utiliser de bons mots de passe. Les mots de passe doivent contenir des lettres, des chiffres et des symboles et former des combinaisons difficiles à deviner par les utilisateurs non autorisés. Ils ne doivent pas être constitués de mots réels. Les bons mots de passe associent des chiffres et des symboles (comme # ou $). Ils peuvent également être composés en juxtaposant la première lettre de tous les mots d'une phrase particulière. Utilisez une combinaison de lettres minuscules et majuscules.

Important : les mots de passe shadow et les mots de passe Open Directory sont beaucoup moins sujets à l'attaque hors ligne car ils ne sont pas stockés dans les enregistrements d'utilisateur. Les mots de passe shadow sont stockés dans des fichiers séparés, uniquement lisibles par une personne qui connaît le mot de passe de l'utilisateur racine (appelé aussi administrateur système). Les mots de passe Open Directory sont enregistrés de manière sûre dans le centre de distribution de clés Kerberos et dans la base de données du serveur de mots de passe Open Directory. Le mot de passe Open Directory d'un utilisateur ne peut être lu par d'autres utilisateurs, pas même par un utilisateur disposant d'autorisations d'administrateur pour l'authentification Open Directory. (Cet administrateur ne peut changer que les mots de passe Open Directory et les politiques de mot de passe).

Les mots de passe cryptés ne sont pas considérés comme sécurisés. Il est recommandé de ne les utiliser que pour les comptes d'utilisateur qui doivent être compatibles avec des clients UNIX qui les requièrent ou des clients sous Mac OS X 10.1. Comme ils sont stockés dans les comptes d'utilisateur, ils sont aussi accessibles et susceptibles d'être la cible d'attaques hors ligne (consultez la section "Attaques hors ligne sur des mots de passe"). Bien que stockés sous une forme encodée, ils sont relativement faciles à décoder.

Comment les mots de passe cryptés sont cryptés

Les mots de passe cryptés ne sont pas stockés en clair ; ils sont dissimulés et rendus illisibles par le cryptage. Le procédé de cryptage d'un mot de passe crypté consiste à introduire le mot de passe en clair et un nombre aléatoire dans une fonction mathématique (appelée fonction de hachage unidirectionnelle). Une fonction de hachage unidirectionnelle génère toujours la même valeur cryptée à partir de données en entrée spécifiques, mais ne peut être utilisée pour recréer le mot de passe original à partir des données en sortie cryptées qu'elle génère.

Pour valider un mot de passe à l'aide de la valeur cryptée, Mac OS X applique la fonction au mot de passe tapé par l'utilisateur et la compare à la valeur stockée dans le compte d'utilisateur ou le fichier shadow. Si les valeurs se correspondent, le mot de passe est considéré valide.

Détermination de l'option d'authentification à utiliser

Pour authentifier un utilisateur, Open Directory doit d'abord déterminer l'option d'authentification à utiliser : Kerberos, le serveur de mots de passe Open Directory, le mot de passe shadow ou le mot de passe crypté. Le compte de l'utilisateur contient les informations spécifiant l'option d'authentification à utiliser. Ces informations portent le nom d'*attribut d'autorité d'authentification*. Open Directory se sert du nom fourni par l'utilisateur pour trouver le compte de l'utilisateur dans le domaine de répertoire. Open Directory consulte alors l'attribut d'autorité d'authentification présent dans le compte de l'utilisateur pour connaître l'option d'authentification à appliquer.

Vous pouvez changer l'attribut d'autorité d'authentification d'un utilisateur en changeant le type de mot de passe dans la sous-fenêtre Avancé de Gestionnaire de groupe de travail, comme illustré dans le tableau qui suit. Pour plus de détails, consultez la section "Modification du type de mot de passe d'un utilisateur" à la page 106.

Type de mot de passe	Autorité d'authentification	Attribut dans l'enregistrement d'utilisateur
Open Directory	Serveur de mots de passe Open Directory et/ou Kerberos[1]	L'un ou l'autre, ou les deux : • ;ApplePasswordServer; • ;Kerberosv5;
Mot de passe shadow	Fichier de mots de passe de chaque utilisateur, lisible uniquement par l'utilisateur root	L'un ou l'autre : • ;ShadowHash;[2] • ;ShadowHash;<*liste des méthodes d'authentification activées*>
Mot de passe crypté	Mot de passe encodé dans l'enregistrement d'utilisateur	L'un ou l'autre : • ;basic; • pas d'attribut du tout

[1] Les comptes d'utilisateur de Mac OS X Server 10.2 doivent être réinitialisés pour qu'ils contiennent l'attribut d'autorité d'authentification Kerberos. Consultez la section "Activation de l'authentification Kerberos par signature unique pour un utilisateur" à la page 110.
[2] Si l'attribut qui figure dans l'enregistrement d'utilisateur est ;ShadowHash; sans liste de méthodes d'authentification activées, ce sont les méthodes d'authentification par défaut qui sont activées. La liste des méthodes d'authentification par défaut est différente pour Mac OS X Server et Mac OS X.

L'attribut d'autorité d'authentification peut spécifier plusieurs options d'authentification. Par exemple, un compte d'utilisateur avec un mot de passe de type Open Directory possède normalement un attribut d'autorité d'authentification qui spécifie tant Kerberos que le serveur de mots de passe Open Directory.

Un compte d'utilisateur ne doit pas nécessairement contenir un attribut d'autorité d'authentification. Dans ce cas, Mac OS X Server suppose qu'un mot de passe crypté est enregistré dans le compte d'utilisateur. Ainsi, les comptes d'utilisateur créés à l'aide de la version 10.1 ou des versions antérieures de Mac OS X contiennent un mot de passe crypté mais pas d'attribut d'autorité d'authentification.

Politiques de mot de passe

Open Directory applique les politiques de mot de passe pour les utilisateurs dont le type de mot de passe est Open Directory ou Mot de passe Shadow. Une politique de mot de passe d'utilisateur peut, par exemple, spécifier un délai d'expiration du mot de passe. Si, au moment où l'utilisateur se connecte, Open Directory constate que le mot de passe a expiré, l'utilisateur devra remplacer ce mot de passe. Open Directory pourra alors authentifier l'utilisateur.

Les politiques de mot de passe peuvent désactiver un compte d'utilisateur à une date donnée, après un certain nombre de jours, après une période d'inactivité ou après un certain nombre de tentatives de connexion infructueuses. Elles peuvent aussi exiger que le mot de passe soit composé au minimum d'un certain nombre de caractères, qu'il contienne au moins une lettre ou un chiffre, qu'il soit différent du nom d'utilisateur, qu'il diffère des mots de passe précédemment choisis ou qu'il soit modifié régulièrement.

La politique de mot de passe pour un compte d'utilisateur mobile est d'application lorsque le compte est utilisé aussi bien lorsqu'il est déconnecté du réseau que lorsqu'il est connecté au réseau. La politique de mot de passe d'un compte d'utilisateur mobile est mise en mémoire cache pour son utilisation hors ligne. Pour en savoir plus sur l es comptes d'utilisateur mobiles, consultez le guide de gestion des utilisateurs.

Les politiques de mot de passe n'affectent pas les comptes d'administrateur. Les administrateurs sont exclus des politiques de mot de passe car ils peuvent modifier ces politiques comme ils le souhaitent. De plus, appliquer des politiques de mot de passe à des administrateurs pourrait en faire la cible d'attaques par déni de service.

Kerberos et le serveur de mots de passe Open Directory maintiennent les politiques de mot de passe séparément. Un serveur Open Directory synchronise les règles de politique de mot de passe Kerberos avec les règles de politique de mot de passe du serveur de mots de passe Open Directory.

Authentification par signature unique

Mac OS X Server utilise Kerberos pour l'authentification par *signature unique*, ce qui permet aux utilisateurs de ne pas devoir taper un nom d'utilisateur et un mot de passe différents pour chacun des services. Avec la signature unique, un utilisateur tape toujours un nom d'utilisateur et un mot de passe dans la fenêtre de connexion. Par la suite, il n'a plus besoin de saisir un nom et un mot de passe pour le service de fichiers Apple, le service de courrier ou d'autres services faisant appel à l'authentification Kerberos. Pour tirer parti de la fonction de signature unique, les utilisateurs et les services doivent être *kerbérisés*, c'est-à-dire configurés pour l'authentification Kerberos, et utiliser le même serveur de centre de distribution de clés Kerberos.

Les comptes d'utilisateur qui résident dans un répertoire LDAP de Mac OS X Server et qui possèdent un mot de passe de type Open Directory utilisent le centre de distribution de clés intégré du serveur. Ces comptes d'utilisateur sont automatiquement configurés pour Kerberos et la signature unique. Les services kerbérisés de ce serveur utilisent également le centre de distribution de clés intégré du serveur et sont automatiquement configurés pour la signature unique. Ce centre de distribution de clés Mac OS X Server peut aussi authentifier les utilisateurs pour les services fournis par d'autres serveurs. Pour que des serveurs supplémentaires sous Mac OS X Server utilisent le centre de distribution de clés de Mac OS X Server, très peu de configuration est nécessaire.

Authentification Kerberos

Kerberos est un protocole d'authentification en réseau développé par le MIT en vue de fournir une authentification et des communications sûres en réseaux ouverts, tels qu'Internet. Il porte le nom du chien à trois têtes qui gardait l'accès au monde souterrain dans la mythologie grecque.

Kerberos fournit des preuves de l'identité aux deux parties. Il vous permet de prouver qui vous êtes aux services de réseau que vous souhaitez utiliser. Il prouve aussi à vos applications que les services de réseau sont authentiques, et non pastiches. Comme d'autres systèmes d'authentification, Kerberos ne fournit pas d'autorisation. Chaque service de réseau détermine lui-même ce qu'il vous autorise à faire en fonction de l'identité prouvée.

Kerberos permet à un client et à un serveur de s'identifier mutuellement sans ambiguïté de façon bien plus sûre que les méthodes d'authentification de mot de passe par défi et réponse déployées habituellement. Kerberos fournit aussi un environnement de signature unique dans lequel les utilisateurs ne doivent s'authentifier qu'une fois par jour, par semaine ou par période de temps, ce qui réduit la charge liée à l'authentification pour les utilisateurs.

Mac OS X Server offre une prise en charge intégrée de Kerberos que vraiment tout le monde peut déployer. En fait, le déploiement de Kerberos est à ce point automatique que les utilisateurs et les administrateurs ne remarqueront peut-être même pas qu'il est déployé. Mac OS X 10.3 et ultérieur utilisent Kerberos automatiquement lorsque quelqu'un se connecte à l'aide d'un compte configuré pour l'authentification Open Directory et lorsque c'est le réglage par défaut pour les comptes d'utilisateur dans le répertoire LDAP de Mac OS X Server. D'autres services fournis par le serveur de répertoire LDAP comme, par exemple, les services AFP et ceux de courrier électronique, utilisent aussi Kerberos automatiquement. Si votre réseau comporte des serveurs supplémentaires sous Mac OS X Server 10.4, il est aisé de les joindre au serveur Kerberos ; la plupart de leurs services utilisent alors Kerberos automatiquement. D'un autre côté, si votre réseau dispose déjà d'un système Kerberos comme, par exemple, Microsoft Active Directory, vous pouvez configurer vos ordinateurs Mac OS X Server et Mac OS X pour qu'ils l'utilisent pour l'authentification.

Mac OS X Server et Mac OS X 10.3 et 10.4 prennent en charge Kerberos 5.

Surmonter les obstacles du déploiement de Kerberos

Jusqu'il y a peu, Kerberos n'était qu'une technologie destinée aux universités et à certains sites gouvernementaux. Si Kerberos est si génial, pourquoi n'est-il pas déployé plus largement ? Réponse : des obstacles à l'adoption devaient être surmontés.

Mac OS X et Mac OS X Server 10.3 et ultérieur éliminent les obstacles historiques suivants à l'adoption de Kerberos.

- Un administrateur devait configurer un centre de distribution de clés Kerberos (KDC, Key Distribution Center). Ce dernier n'était pas facile à déployer ni à administrer. Il fallait être costaud.
- Il n'y avait pas d'intégration standard avec un système de répertoire. Kerberos ne fait que de l'authentification, il ne stocke pas de données de compte d'utilisateur comme, par exemple, l'identifiant d'utilisateur (UID), l'emplacement du répertoire de départ ou l'adhésion de groupe. L'administrateur devait arriver à comprendre comment intégrer Kerberos à un système de répertoire.
- Tous les serveurs devaient être inscrits au centre de distribution de clés Kerberos. Cela ajoutait une étape supplémentaire au processus de configuration du serveur.
- Après avoir configuré un serveur Kerberos, l'administrateur devait se rendre sur tous les ordinateurs clients et tous les configurer pour l'utilisation de Kerberos. Ce n'était pas difficile à faire, mais cela prenait beaucoup de temps et nécessitait la modification de fichiers de configuration et l'utilisation d'outils de ligne de commande.
- Il fallait disposer d'une suite d'applications kerbérisées (logiciels serveur et client). Certaines des applications de base sont disponibles, mais les porter et les adapter pour qu'elles fonctionnent dans votre environnement n'était pas chose aisée.
- Tous les protocoles de réseau utilisés pour l'authentification client-serveur ne prennent pas en charge Kerberos. Certains protocoles de réseau nécessitent toujours des méthodes d'authentification défi-réponse traditionnelles et il n'y a pas de façon standard d'intégrer Kerberos à ces méthodes d'authentification réseau patrimoniales.
- Le client Kerberos prend en charge le basculement de sorte que, si un centre de distribution de clés est hors ligne, il peut utiliser une réplique, mais l'administrateur devait arriver à comprendre comment configurer une réplique Kerberos.
- Les outils d'administration n'ont jamais été intégrés. Les outils pour la création et la modification de comptes d'utilisateur dans le domaine de répertoire ne savaient rien de Kerberos et les outils Kerberos ne savaient rien des comptes d'utilisateur dans les répertoires. Configurer un enregistrement d'utilisateur était une opération spécifique au site, qui dépendait de la façon dont le centre de distribution de clés était intégré au système de répertoire.

Expérience en matière de signature unique

Kerberos est un système de références ou un système à base de tickets. L'utilisateur se connecte une fois au système Kerberos et reçoit un ticket avec une certaine durée de vie. Pendant la durée de vie de ce ticket, l'utilisateur ne doit jamais se réauthentifier pour accéder à un service kerbérisé. Le logiciel client kerbérisé de l'utilisateur, comme, par exemple, l'application Mail de Mac OS X, présente automatiquement un ticket Kerberos valide pour authentifier l'utilisateur pour un service kerbérisé. C'est cela la signature unique.

Un ticket Kerberos, c'est comme une carte de presse pour un festival de jazz qui se tient dans différentes boîtes de nuit sur trois jours. Vous devez prouver votre identité une fois pour obtenir la carte de presse. Jusqu'à son expiration, il suffit de la montrer à une des boîtes de nuit pour obtenir un ticket pour un spectacle. Toutes les boîtes de nuit participantes acceptent votre carte de presse sans vous demander de prouver à nouveau votre identité.

Authentification sécurisée

Bien qu'intrinsèquement Internet ne soit pas sécurisé, de nombreux protocoles d'authentification ne fournissent pas de véritable sécurité. Les pirates informatiques peuvent utiliser des outils logiciels tout prêts pour intercepter les mots de passe qui transitent par un réseau. De nombreuses applications envoient, en effet, les mots de passe en clair. Ces derniers sont prêts à l'emploi dès qu'ils sont interceptés. Même les mots de passe cryptés ne sont pas tout à fait sûrs. S'il dispose de temps et de puissance de calcul, un pirate peut aussi craquer les mots de passe cryptés.

Vous pouvez utiliser un coupe-feu pour isoler les mots de passe qui transitent sur votre réseau privé, mais ce n'est pas la panacée. Un coupe-feu ne protège pas contre les personnes mécontentes ou malveillantes venant de l'intérieur.

Kerberos a été conçu pour solutionner les problèmes de sécurité de réseau. Il ne transmet jamais le mot de passe de l'utilisateur par le réseau et ne l'enregistre jamais dans la mémoire ni sur le disque de l'ordinateur de l'utilisateur. De cette façon, même si les références Kerberos sont craquées ou compromises, l'attaquant ne connaîtra pas le mot de passe original et ne pourra, le cas échéant, compromettre qu'une petite partie du réseau et non l'ensemble du réseau.

En plus d'une gestion des mots de passe plus efficace, Kerberos procède aussi à une authentification mutuelle. Le client s'authentifie auprès du service et le service s'authentifie auprès du client. Une attaque "man-in-the-middle" ou de mystification est impossible lorsque vous utilisez des services kerbérisés. Les utilisateurs peuvent donc faire confiance aux services auxquels ils accèdent.

Prêt à aller au-delà des mots de passe

L'authentification réseau est une opération délicate. Pour déployer une nouvelle méthode d'authentification réseau, il faut que le client et le serveur se mettent d'accord sur la méthode d'authentification à utiliser. Alors qu'il est possible pour n'importe quel processus client-serveur de se mettre d'accord sur une méthode d'authentification personnalisée, obtenir une large adoption d'une multitude de protocoles réseau, de plateformes et de clients est presque impossible.

Par exemple, imaginez que vous souhaitiez déployer des cartes à puce intelligentes comme méthode d'authentification réseau. Sans Kerberos, vous devriez modifier chaque protocole client-serveur pour qu'il prenne en charge la nouvelle méthode. La liste des protocoles est longue : SMTP, POP, IMAP, AFP, SMB, HTTP, FTP, IPP, SSH, QuickTime Streaming, DNS, LDAP, Netinfo, RPC, NFS, AFS, WebDAV, LPR et ainsi de suite. Si l'on considère tous les logiciels qui font de l'authentification réseau, déployer une nouvelle méthode d'authentification parmi l'ensemble des protocoles réseau est une tâche titanesque. Alors que cela semble faisable pour les logiciels d'un seul et unique fournisseur, il est peu probable que vous arriviez à convaincre tous les fournisseurs de modifier leur logiciel client pour qu'il utilise votre nouvelle méthode d'authentification par cartes à puce intelligentes. De plus, vous souhaiterez probablement aussi que votre méthode d'authentification par cartes à puce intelligentes fonctionne sur plusieurs plateformes : Mac OS X, Windows et UNIX.

À cause de la conception de Kerberos, un protocole binaire client-serveur qui prend en charge Kerberos ne sait même pas comment l'utilisateur prouve son identité : à l'aide d'une paire nom d'utilisateur-mot de passe, d'une carte à puce intelligente et d'un numéro d'identification personnel, ou de toute autre méthode. C'est pourquoi il vous suffit de changer le client Kerberos et le serveur Kerberos pour qu'ils acceptent une nouvelle preuve d'identité comme, par exemple, une carte à puce intelligente, pour que l'ensemble de votre réseau Kerberos adopte la nouvelle méthode de preuve d'identité, sans que vous deviez déployer de nouvelles versions des logiciels client et serveur.

Authentification multiplateforme

Kerberos est disponible sur les principales plateformes, y compris Mac OS X, Windows, Linux et d'autres variantes d'UNIX.

Authentification centralisée

Kerberos fournit une autorité d'authentification centrale pour le réseau. Tous les services et clients pour lesquels Kerberos est activé sur le réseau utilisent cette autorité centrale. Les administrateurs peuvent vérifier et contrôler les politiques et les opérations d'authentification de façon centralisée.

Services kerbérisés

Kerberos peut authentifier des utilisateurs pour les services suivants de Mac OS X Server :

- Fenêtre de connexion
- Service de courrier
- Service de fichiers AFP
- Service de fichiers FTP
- Service de fichiers SMB/CIFS (en tant que membre d'un royaume Kerberos Active Directory)
- Service VPN
- Service Web Apache
- Service de répertoire LDAP

Ces services ont été "kerbérisés", qu'ils tournent ou pas. Seuls ces services peuvent utiliser Kerberos pour authentifier un utilisateur. Mac OS X Server contient des outils de ligne de commande pour kerbériser des services supplémentaires qui sont compatibles avec Kerberos MIT. Pour plus d'informations, consultez le chapitre consacré à Open Directory du guide de l'administration en ligne de commande.

Principaux et royaumes Kerberos

Les services kerbérisés sont configurés pour authentifier les principaux connus d'un royaume Kerberos donné. Un royaume Kerberos peut être considéré comme une base de données ou un domaine d'authentification Kerberos spécifique contenant des données de validation pour les utilisateurs, les services et parfois les serveurs (tous appelés "principaux"). Par exemple, un royaume contient des clés secrètes de principaux qui résultent d'une fonction unidirectionnelle appliquée à des mots de passe. Les principaux de service sont généralement basés sur des secrets générés de façon aléatoires plutôt que sur des mots de passe.

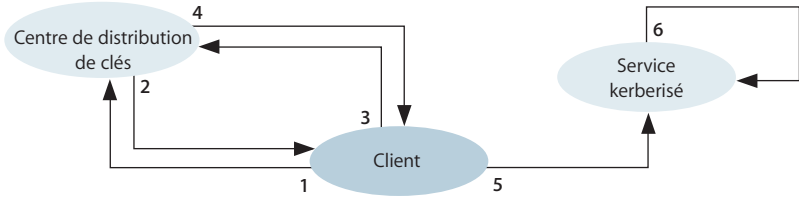
Des exemples de royaumes et de noms principaux sont fournis ci-après. Vous remarquerez que les noms de royaumes sont, par convention, en lettres capitales afin de les différencier des noms de domaines DNS :

- Royaume : MONROYAUME.EXEMPLE.COM
- Utilisateur principal : jsanchez@MONROYAUME.EXEMPLE.COM
- Service principal : serveurafp/autrenom.exemple.com@MONROYAUME.EXEMPLE.COM

Processus d'authentification Kerberos

L'authentification Kerberos se fait en plusieurs étapes. Lors de la première étape, le client obtient des références servant à demander l'accès aux services kerbérisés. Lors de la deuxième phase, le client requiert l'authentification pour un service donné. Lors de la dernière étape, le client présente les références au service.

L'illustration suivante schématise ces activités. Remarquez que, sur ce schéma, le service et le client peuvent constituer soit la même entité (la fenêtre de connexion, par exemple), soit deux entrées différentes (par exemple un client de courrier et le serveur de courrier).



1 Le client s'authentifie auprès d'un centre de distribution de clés (KDC), qui interagit avec des royaumes pour accéder aux données d'authentification. Ce n'est qu'à cette étape que les mots de passe et les informations de politique de mot de passe qui y sont associées doivent être vérifiées.

2 Le centre de distribution de clés délivre au client un ticket d'octroi de ticket, référence dont le client a besoin pour utiliser des services kerbérisés. Ce ticket est valide pour une durée paramétrable, mais peut être annulé avant l'expiration du délai. Ils sont placés sur le client jusqu'à leur expiration.

3 Le client contacte le centre de distribution de clés avec le ticket d'octroi de ticket lorsqu'il souhaite utiliser un service kerbérisé donné.

4 Le centre délivre un ticket pour ce service.

5 Le client présente le ticket au service.

6 Le service authentifie le client en vérifiant que le ticket est valide.

Après avoir authentifié le client, le service détermine si le client est autorisé à utiliser le service. Kerberos ne fait qu'authentifier les clients, il ne les autorise pas à utiliser des services. Par exemple, de nombreux services utilisent les listes de contrôle d'accès à un service de Mac OS X Server pour déterminer si un client est autorisé à utiliser le service.

Notez que Kerberos n'envoie jamais de mot de passe ni d'information de politique de mot de passe à aucun service. Une fois qu'un ticket d'octroi de ticket a été obtenu, il est inutile de fournir des informations de mot de passe.

La notion de temps est très importante pour Kerberos. Si le client et le centre de distribution de clés ne sont pas synchronisés à quelques minutes près, le client ne réussira pas à s'authentifier avec le centre. Les informations concernant la date, l'heure et le fuseau horaire doivent être correctes sur le serveur du centre de distribution de clés et chez les clients. Il est recommandé qu'ils utilisent tous le même service d'horloge réseau pour que leurs horloges restent synchronisées.

Pour plus d'informations sur Kerberos, rendez-vous sur le site Web de Kerberos MIT :

web.mit.edu/kerberos/www/index.html

Méthodes d'authentification par serveur de mots de passe Open Directory et par mot de passe shadow

À des fins de compatibilité avec différents services, Mac OS X Server peut utiliser une variété de méthodes d'authentification pour valider les mots de passe Open Directory et les mots de passe shadow. Pour les mots de passe Open Directory, Mac OS X Server utilise la méthode standard Simple Authentication and Security Layer (SASL) pour négocier une méthode d'authentification entre un client et un service. Pour les mots de passe shadow, l'utilisation de SASL dépend du protocole de réseau.

Méthode d'authentification	Sécurité du réseau	Sécurité du stockage	Utilise
APOP	Crypté, avec solution de secours à texte en clair	Texte en clair	Service de courrier POP
CRAM-MD5	Crypté, avec solution de secours à texte en clair	Crypté	Service de courrier IMAP, service LDAP
DHX	Crypté	Crypté	Service de fichiers AFP, administration Open Directory
Digest-MD5	Crypté	Crypté	Fenêtre de connexion, service de courrier électronique
MS-CHAPv2	Crypté	Crypté	Service VPN
NTLMv1 et NTLMv2	Crypté	Crypté	Services SMB/CIFS (Windows NT/98 ou ultérieur)
LAN Manager	Crypté	Crypté	Services SMB/CIFS (Windows 95)
WebDAV-Digest	Crypté	Texte en clair	Service de fichiers WebDAV (iDisk)

Open Directory doit gérer de nombreuses méthodes d'authentification différentes car chaque service requérant l'authentification utilise des méthodes particulières. Les services de fichiers utilisent un ensemble de méthodes d'authentification, le service Web en utilise un autre, le service de courrier encore un autre, etc.

Certaines méthodes d'authentification sont plus sûres. Les méthodes les plus sûres utilisent des algorithmes plus robustes pour encoder les données transmises entre le client et le serveur. Les méthodes d'authentification les plus sûres stockent en outre des mots de passe cryptés, appelés condensés numériques, difficiles à récupérer à partir du serveur. Les méthodes les moins sûres stockent les mots de passe en clair, ce qui les rend faciles à récupérer.

Personne, pas même un administrateur ni un utilisateur racine, ne peut récupérer des mots de passe cryptés en les lisant dans la base de données. Un administrateur peut utiliser Gestionnaire de groupe de travail pour définir le mot de passe d'un utilisateur, mais il ne peut lire aucun mot de passe d'utilisateur.

Remarque : si vous connectez Mac OS X Server 10.4 ou ultérieur à un domaine de répertoire de Mac OS X Server 10.3 ou antérieur, sachez que les utilisateurs définis dans le domaine de répertoire le plus ancien ne peuvent être authentifiés par la méthode MS-CHAPv2. Cette méthode peut s'avérer nécessaire pour authentifier de façon sûre certains utilisateurs Windows pour les services Windows de Mac OS X Server 10.4 et ultérieur. Le serveur de mots de passe Open Directory dans Mac OS X Server 10.4 et ultérieur prend en charge l'authentification NTLMv2, mais le serveur de mots de passe dans Mac OS X Server 10.3 et antérieur ne prend pas en charge NTLMv2.

De la même façon, si vous connectez Mac OS X Server 10.3 ou ultérieur à un domaine de répertoire de Mac OS X Server 10.2 ou antérieur, les utilisateurs définis dans le domaine de répertoire le plus ancien ne peuvent être authentifiés par la méthode MS-CHAPv2. Cette méthode peut s'avérer nécessaire pour authentifier de façon sûre des utilisateurs pour le service VPN de Mac OS X Server 10.3 et ultérieur. Le serveur de mots de passe Open Directory dans Mac OS X Server 10.3 et ultérieur prend en charge l'authentification MS-CHAPv2, mais le serveur de mots de passe de Mac OS X Server 10.2 et antérieur ne prend pas en charge MS-CHAPv2.

Désactivation des méthodes d'authentification Open Directory

Les méthodes d'authentification peuvent être désactivées de manière sélective afin de rendre plus sûr le stockage des mots de passe Open Directory sur le serveur. Par exemple, si aucun client n'utilise les services Windows, vous pouvez désactiver les méthodes d'authentification NTLMv1, NTLMv2 et LAN Manager afin d'empêcher le stockage de mots de passe sur le serveur à l'aide de ces méthodes. Ainsi, toute personne qui accéderait à votre base de données de mots de passe ne pourrait pas exploiter les vulnérabilités de ces méthodes d'authentification pour craquer des mots de passe.

Important : si vous désactivez une méthode d'authentification, son condensé numérique sera supprimé de la base de données de mots de passe à la prochaine authentification de l'utilisateur. Si vous activez une méthode d'authentification qui était désactivée, chaque mot de passe Open Directory doit être réinitialisé pour ajouter le condensé numérique de la méthode nouvellement activée à la base de données de mots de passe. Les utilisateurs peuvent réinitialiser leurs propres mots de passe ou un administrateur de répertoire peut le faire pour eux.

Désactiver une méthode d'authentification rend la base de données du serveur de mots de passe Open Directory plus sûre au cas où un utilisateur malveillant aurait accès physiquement à un serveur Open Directory (maître ou réplique) ou à un support contenant une copie de sauvegarde du maître Open Directory. Une personne qui arriverait à accéder à la base de données de mots de passe peut tenter de craquer le mot de passe d'un utilisateur en attaquant le condensé numérique ou le texte récupérable stocké dans la base de données de mots de passe à l'aide de n'importe quelle méthode d'authentification. Rien ne sera stocké dans la base de données de mots de passe par une méthode d'authentification désactivée, ce qui laisse une voie de pénétration de moins ouverte à un pirate qui aurait accès physiquement au serveur Open Directory ou à une copie de sauvegarde de ce dernier.

Les condensés numériques stockés dans la base de données de mots de passe par certaines méthodes d'authentification sont plus faciles à craquer que d'autres. Les méthodes d'authentification récupérables stockent en réalité du texte en clair, c'est-à-dire parfaitement lisible. Désactiver les méthodes d'authentification qui stockent du texte en clair ou des condensés numériques plus faibles augmentera plus la sécurité de la base de données de mots de passe que désactiver des méthodes qui stockent des condensés numériques plus forts.

Si vous pensez que vos maîtres, vos répliques et vos copies de sauvegarde Open Directory sont en sécurité, vous pouvez sélectionner toutes les méthodes d'authentification. Si vous vous faites du souci à propos de la sécurité physique d'un serveur Open Directory ou de ses supports de copies de sauvegarde, désactivez certaines méthodes.

Remarque : désactiver des méthodes d'authentification n'améliore pas la sécurité des mots de passe pendant qu'ils transitent par le réseau. Seule la sécurité de la base de données de mots de passe est concernée. En fait, désactiver certaines méthodes d'authentification peut contraindre certains clients à configurer leur logiciel pour qu'il envoie les mots de passe par le réseau sous la forme de texte en clair, ce qui risque de compromettre la sécurité des mots de passe d'une autre façon.

Désactivation des méthodes d'authentification de mots de passe shadow

Les méthodes d'authentification peuvent être désactivées de manière sélective afin de rendre plus sûr le stockage des mots de passe dans des fichiers de mots de passe shadow. Par exemple, si un utilisateur n'utilise ni le service de courrier électronique ni le service Web, vous pouvez désactiver les méthodes WebDAV-Digest et APOP pour cet utilisateur. Ainsi, toute personne qui accéderait aux fichiers de mots de passe shadow sur un serveur ne pourrait pas récupérer le mot de passe de l'utilisateur.

Important : si vous désactivez une méthode d'authentification de mots de passe shadow, son condensé numérique sera supprimé du fichier de mots de passe de l'utilisateur à la prochaine authentification de l'utilisateur. Si vous activez une méthode d'authentification qui était désactivée, le condensé numérique de la méthode nouvellement activée sera ajouté au fichier de mots de passe shadow de l'utilisateur à la prochaine authentification de l'utilisateur pour un service qui peut utiliser un mot de passe en clair comme, par exemple, la fenêtre de connexion ou AFP. D'un autre côté, le mot de passe de l'utilisateur peut être réinitialisé pour ajouter le condensé numérique de la méthode nouvellement activée. Les utilisateurs peuvent réinitialiser leurs propres mots de passe ou un administrateur de répertoire peut le faire pour eux.

Désactiver une méthode d'authentification rend le mot de passe shadow plus sûr au cas où un utilisateur malveillant aurait accès physiquement aux fichiers de mots de passe shadow d'un serveur ou à un support contenant une copie de sauvegarde des fichiers de mots de passe shadow. Une personne qui arriverait à accéder aux fichiers de mots de passe peut tenter de craquer le mot de passe d'un utilisateur en attaquant le condensé numérique ou le texte récupérable stocké dans la base de données de mots de passe à l'aide de n'importe quelle méthode d'authentification. Rien ne sera stocké par une méthode d'authentification désactivée, ce qui laisse une voie de pénétration de moins ouverte à un pirate qui aurait accès physiquement au fichier de mots de passe shadow ou à une copie de sauvegarde de ce dernier.

Les condensés numériques stockés par certaines méthodes d'authentification sont plus faciles à craquer que d'autres. Avec les méthodes d'authentification récupérables, le mot de passe en clair original peut être reconstruit à partir de ce qui est stocké dans le fichier. Désactiver les méthodes d'authentification qui stockent des condensés numériques récupérables ou plus faibles augmentera plus la sécurité du fichier de mots de passe shadow que désactiver des méthodes qui stockent des condensés numériques plus forts.

Si vous pensez que les fichiers de mots de passe shadow et les copies de sauvegarde de ces derniers d'un serveur sont en sécurité, vous pouvez sélectionner toutes les méthodes d'authentification. Si vous vous faites du souci à propos de la sécurité physique du serveur ou de ses supports de copies de sauvegarde, désactivez certaines méthodes.

Remarque : désactiver des méthodes d'authentification n'améliore pas la sécurité des mots de passe pendant qu'ils transitent par le réseau ; seule la sécurité du stockage des mots de passe est concernée. En fait, désactiver certaines méthodes d'authentification peut contraindre certains clients à configurer leur logiciel pour qu'il envoie les mots de passe par le réseau sous la forme de texte en clair, ce qui risque de compromettre la sécurité des mots de passe d'une autre façon.

Contenu de la base de données du serveur de mots de passe Open Directory

Le serveur de mots de passe Open Directory tient à jour une base de données d'authentification distincte du domaine de répertoire de . Open Directory restreint très fort l'accès à la base de données d'authentification.

Le serveur de mots de passe Open Directory stocke les informations suivantes dans sa base de données d'authentification pour chaque compte d'utilisateur possédant un mot de passe de type Open Directory.

- L'identifiant de mot de passe de l'utilisateur, une valeur 128 bits attribuée lors de la création du mot de passe. Il est également enregistré dans l'enregistrement de l'utilisateur, dans le domaine de répertoire, et est utilisé comme clé d'accès à l'enregistrement d'utilisateur dans la base de données du serveur de mot de passe Open Directory.
- Le mot de passe stocké sous une forme récupérable (en clair) ou sous la forme d'un condensé numérique (crypté). La forme varie en fonction de la méthode d'authentification. Un mot de passe récupérable est enregistré pour les méthodes d'authentification APOP et WebDAV. Pour toutes les autres méthodes, l'enregistrement se fait sous la forme d'un mot de passe crypté. Si aucune méthode d'authentification exigeant un mot de passe en clair n'est activée, la base de données d'authentification d'Open Directory enregistre les mots de passe sous forme cryptée uniquement.
- Le nom abrégé de l'utilisateur (utilisé dans les messages d'historiques consultables dans Admin Serveur).
- Des données de politique de mot de passe.
- Des horodatages et autres informations sur l'utilisation comme, par exemple, l'heure de la dernière connexion, l'heure de la dernière validation échouée, le nombre de validations échouées et des informations de réplication.

Authentification par liaison LDAP

Pour les comptes d'utilisateur qui résident dans un répertoire LDAP sur un serveur non Apple, Open Directory tente d'utiliser l'authentification par liaison LDAP. Open Directory envoie au serveur de répertoire LDAP le nom et le mot de passe fournis par l'utilisateur en cours d'authentification. L'authentification est réussie si le serveur LDAP trouve un enregistrement d'utilisateur et un mot de passe correspondants.

L'authentification par liaison LDAP peut être peu sûre si le service de répertoire LDAP et la connexion de l'ordinateur client à ce dernier sont configurés pour autoriser l'envoi de mots de passe en clair sur le réseau. Open Directory tente d'utiliser une méthode d'authentification sûre avec le répertoire LDAP. Si le répertoire ne prend pas en charge la liaison LDAP sécurisée et si la connexion LDAPv3 du client autorise l'envoi d'un mot de passe en clair, Open Directory va se rabattre sur la liaison LDAP simple. Dans ce cas, vous pouvez sécuriser cette authentification en configurant un accès au répertoire LDAP à l'aide du protocole SSL (Secure Sockets Layer). SSL sécurise l'accès en cryptant toutes les communications avec le répertoire LDAP. Pour plus d'informations, consultez les sections "Modification de la politique de sécurité pour une connexion LDAP" à la page 142 et "Modification des réglages de connexion d'un répertoire LDAP" à la page 141.

Gestionnaire d'authentification

Mac OS X Server gère les utilisateurs qui ont été configurés pour employer la technologie héritée Gestionnaire d'authentification de Mac OS X Server versions 10.0 à 10.2.

Gestionnaire d'authentification est une technologie héritée pour la validation sécurisée des mots de passe des utilisateurs suivants :

- Utilisateurs de services Windows (y compris gestion de SMB-NT, SMB-LM et CRAM-MD5)
- Utilisateurs de services de fichiers Apple dont les ordinateurs Mac OS 8 n'ont pas été mis à niveau avec le logiciel client AFP version 3.8.3 ou plus
- Utilisateurs devant s'authentifier pour le service de courrier à l'aide d'APOP ou de CRAM-MD5

Le Gestionnaire d'authentification ne fonctionne qu'avec les comptes d'utilisateur qui ont été créés dans un domaine NetInfo de Mac OS X Server 10.0–10.2. Le Gestionnaire d'authentification doit avoir été activé pour le domaine NetInfo.

Lorsque vous mettez à niveau un serveur vers Mac OS X Server 10.4 à partir d'une version antérieure dans laquelle le Gestionnaire d'authentification est activé, ce dernier demeure activé. Les utilisateurs existants peuvent conserver leurs mots de passe. Un compte d'utilisateur existant utilise Gestionnaire d'authentification si le compte se trouve dans un domaine NetInfo pour lequel Gestionnaire d'authentification a été activé et si le compte est configuré pour utiliser un mot de passe crypté. Chaque compte d'utilisateur existant dans le domaine de répertoire local du serveur, qui est un domaine NetInfo, est converti automatiquement d'un mot de passe crypté en un mot de passe shadow lorsque l'utilisateur ou l'administrateur change le mot de passe ou lorsque l'utilisateur s'authentifie pour un service qui peut utiliser une méthode d'authentification récupérable.

Après la mise à niveau d'un serveur vers Mac OS X Server 10.4, vous pouvez modifier les comptes d'utilisateur existants pour s'authentifier à l'aide d'Open Directory. Si le serveur mis à niveau dispose d'un domaine NetInfo partagé et si vous le migrez vers un répertoire LDAP, tous les comptes d'utilisateur sont automatiquement convertis en des mots de passe Open Directory.

Les mots de passe Open Directory et les mots de passe shadow sont plus sûrs que les mots de passe cryptés. Tant les mots de passe Open Directory que les mots de passe shadow peuvent être utilisés pour le service de fichiers Windows. Les mots de passe Open Directory sont requis pour la connexion à des domaines à partir de postes de travail Windows vers un contrôleur de domaine principal Mac OS X Server. Les nouveaux comptes d'utilisateur créés dans le répertoire LDAP de Mac OS X Server 10.4 sont configurés pour utiliser l'authentification Open Directory.

Planification Open Directory

4

Tout comme l'installation électrique ou les canalisations d'un bâtiment, les services de répertoire d'un réseau doivent être planifiés à l'avance plutôt qu'improvisés au gré des circonstances.

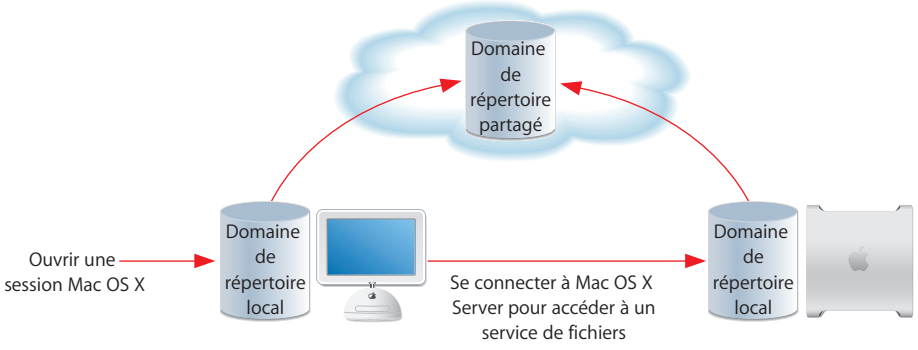
Le stockage d'informations dans des domaines de répertoire partagés améliore le contrôle du réseau, permet à un nombre plus important d'utilisateurs d'accéder aux informations et simplifie la gestion des informations. Toutefois, le niveau de contrôle et de convivialité dépend de l'effort consacré à la planification de vos domaines partagés. L'objectif de la planification d'un domaine de répertoire est de concevoir la disposition de domaines partagés la plus simple qui fournit à vos utilisateurs Mac OS X un accès aisé aux ressources réseau dont ils ont besoin *et* minimise le temps consacré à la gestion des enregistrements d'utilisateurs et d'autres données administratives.

Ce chapitre fournit des indications générales pour la planification des services Open Directory et décrit les outils nécessaires pour les gérer.

Directives générales de planification

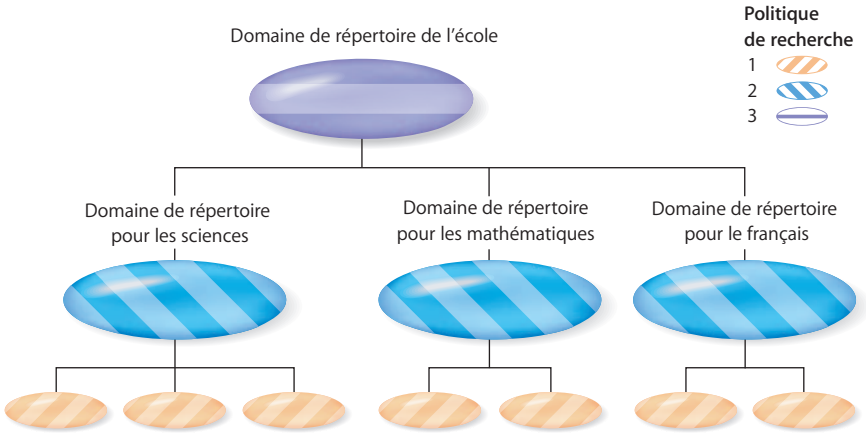
Si vous n'avez pas besoin de partager des informations sur les utilisateurs et les ressources entre plusieurs ordinateurs Mac OS X, la planification de domaines de répertoire présente peu d'intérêt car tout est accessible à partir de domaines de répertoire locaux. Assurez-vous simplement que toutes les personnes qui doivent utiliser un certain ordinateur Mac OS X disposent de comptes d'utilisateur sur ce dernier. Ces comptes d'utilisateur résident dans le domaine de répertoire local, sur l'ordinateur. De plus, toute personne qui a besoin d'utiliser le service de fichiers, le service de courrier ou tout autre service qui requiert une authentification de Mac OS X Server, aura besoin d'un compte d'utilisateur dans le domaine de répertoire local du serveur. Avec cette disposition, chaque utilisateur dispose de deux comptes : un pour se connecter à un ordinateur et un pour accéder aux services de Mac OS X Server.

Pour partager des informations entre des ordinateurs et des serveurs Mac OS X, vous devez configurer au moins un domaine de répertoire partagé. Avec cette disposition, chaque utilisateur n'a besoin que d'un seul compte dans le domaine de répertoire partagé. Avec ce compte unique, l'utilisateur peut se connecter à Mac OS X sur tout ordinateur configuré pour accéder au domaine de répertoire partagé. L'utilisateur peut aussi utiliser le même compte pour accéder à des services de tout Mac OS X Server configuré pour accéder au domaine de répertoire partagé.



Dans de nombreuses organisations, un domaine de répertoire partagé unique convient parfaitement. Il permet à des centaines de milliers d'utilisateurs et à des milliers d'ordinateurs de partager les mêmes ressources, comme, par exemple, les mêmes files d'attente d'impression, points de partage pour répertoires de départ, points de partage pour applications et points de partage pour documents. La réplication du domaine de répertoire partagé peut augmenter les capacités ou les performance du système de répertoire en permettant à plusieurs serveurs de traiter la charge du système de répertoire pour le réseau.

Pour des réseaux plus grand et plus complexes, il peut être utile de mettre en place des domaines de répertoire partagés supplémentaires.



Contrôle de l'accès aux données

Avec un domaine de répertoire unique, vous pouvez gérer les préférences des clients et les présentations de réseau pour isoler certains services de réseau tout en rendant d'autres services disponibles à tous les utilisateurs. Par exemple, vous pourriez configurer une présentation de réseau de sorte que les points de partage contenant les applications et les fichiers de comptabilité ne soient visibles que par les ordinateurs du département de la comptabilité. Vous pourriez configurer une autre présentation de réseau gérée de sorte que les points de partage contenant les logiciels et les documents d'édition ne soient visibles que par les rédacteurs techniques. Si vous souhaitez que tous les employés aient accès aux dossiers Boîte de dépôt des autres, il suffit d'inclure le point de partage contenant les dossiers Boîte de dépôt dans toutes les présentations de réseau gérées. Pour en savoir plus sur les clients gérés et les présentations de réseau gérées, consultez le guide de gestion des utilisateurs.

Si votre réseau comprend plusieurs domaines de répertoire partagés, vous pouvez ne rendre les informations des différents répertoires disponibles que pour certains ordinateurs du réseau. Par exemple, les étudiants possédant des comptes d'utilisateur dans le domaine de répertoire des sciences ne pourraient se connecter que sur les ordinateurs dont les politiques de recherche contiennent le domaine des sciences.

Si vous souhaitez que tous les ordinateurs aient accès à certaines données administratives, stockez ces dernières dans un domaine de répertoire partagé inclus dans les politiques de recherche de tous les ordinateurs. Pour que certaines données ne soient accessibles qu'à certains ordinateurs, stockez-les dans un domaine de répertoire partagé qui ne soit inclus que dans la politique de recherche des ordinateurs concernés.

Simplification des modifications des données de répertoires

Si vous avez besoin de plusieurs domaines de répertoire partagés, organisez vos politiques de recherches de manière à minimiser le nombre de changements d'emplacement de stockage des données. Il est également conseillé d'élaborer un plan de gestion des événements en cours tels que :

- L'arrivée de nouveaux utilisateurs dans votre organisation et le départ d'anciens utilisateurs
- L'ajout, l'amélioration ou le remplacement de serveurs de fichiers
- Le déplacement d'imprimantes

Essayez de faire en sorte que chaque domaine de répertoire soit applicable à l'ensemble des ordinateurs l'utilisant, de manière à ne pas devoir modifier ni ajouter d'informations dans plusieurs domaines. Dans l'exemple de domaines partagés à plusieurs niveaux ci-dessus, l'ajout d'un nouvel étudiant au domaine partagé d'une classe permet à l'étudiant d'ouvrir une session à partir de n'importe quel ordinateur de la classe. Au fur et à mesure du recrutement ou du départ de formateurs, l'administrateur peut mettre à jour les informations d'utilisateurs en modifiant simplement le domaine partagé de l'école.

Si votre hiérarchie de domaines de répertoire est complexe ou étendue et appartient à un réseau géré par plusieurs administrateurs, vous devez élaborer des stratégies visant à minimiser les conflits. Par exemple, vous pouvez prédéfinir des gammes d'identifiants d'utilisateurs (Id. Util.) afin d'empêcher un accès accidentel à des fichiers. (Pour plus d'informations, lisez le chapitre sur la configuration des comptes dans le guide de gestion des utilisateurs.)

Évaluation des besoins en matière de répertoires et d'authentification

Outre le mode de répartition des différentes données de répertoires entre les différents domaines, vous devez également tenir compte des capacités de chaque domaine de répertoire. Différents facteurs affectent la taille maximale d'un domaine de répertoire. Parmi ces facteurs, on peut citer les performances de la base de données qui stocke les informations de répertoire. Le domaine de répertoire LDAP de Mac OS X Server utilise la base de données Berkeley DB, qui reste performante avec 200 000 enregistrements. Bien entendu, un serveur hébergeant un domaine de répertoire de cette taille a tout intérêt à disposer d'un espace disque suffisant pour stocker tous les enregistrements.

Le nombre de connexions gérées par un service de répertoire est plus difficile à évaluer car les connexions des services de répertoires surviennent dans un contexte qui englobe les connexions de l'ensemble des services fournis par ce serveur. Sous Mac OS X Server, un serveur dédié à Open Directory peut accepter au maximum 1000 connexions d'ordinateurs clients simultanées.

Le serveur Open Directory est toutefois en mesure de fournir des services LDAP et d'authentification à un nombre plus élevé d'ordinateurs clients car ces derniers ne font pas tous appel à ces services en même temps. Chaque ordinateur client se connecte au répertoire LDAP pendant une durée maximum de deux minutes et les connexions au serveur de mots de passe Open Directory sont encore plus brèves. Un serveur Open Directory est capable de prendre en charge bien plus que 1000 ordinateurs clients, parce qu'il est probable que seule une fraction des ordinateurs clients susceptibles d'établir une connexion avec Open Directory cherche effectivement à établir une connexion au même moment. Il peut néanmoins s'avérer difficile d'évaluer leur nombre, autrement dit le pourcentage d'ordinateurs clients effectuant une connexion au même moment. Ainsi, un ordinateur client utilisé à longueur de journée par une même personne qui travaille sur des fichiers d'images n'aura que rarement besoin des services Open Directory. En revanche, les nombreux utilisateurs d'un ordinateur situé dans un laboratoire ouvrent et ferment des sessions tout au long de la journée, chacun d'entre eux utilisant différents réglages de préférences de client géré. Un tel ordinateur représente une charge relativement lourde pour les services Open Directory.

En général, l'utilisation d'Open Directory est proportionnelle au nombre d'ouvertures et de fermetures de sessions. Ces activités sont habituellement majoritaires dans les services de répertoires et d'authentification de n'importe quel système. Plus les utilisateurs ouvrent et ferment des sessions, moins le serveur Open Directory (ou tout autre serveur de répertoires et d'authentification) pourra gérer d'ordinateurs clients. Si les ouvertures et fermetures de sessions sont très fréquentes, vous devrez ajouter des serveurs Open Directory. En revanche, si les sessions de travail sont plus longues et que les ouvertures de session sont plus rares, vous pourrez vous contenter d'un plus petit nombre de serveurs Open Directory.

Identification de serveurs pour l'hébergement de domaines partagés

Si vous avez besoin de plusieurs domaines partagés, identifiez les serveurs appelés à héberger ces domaines. Les domaines partagés concernent de nombreux utilisateurs, il est donc conseillé de les placer sur des ordinateurs Mac OS X Server présentant les caractéristiques suivantes :

- Accès physique limité
- Accès réseau limité
- Installation de technologies à haute disponibilité telles que les systèmes d'alimentation sans coupure

Sélectionnez des ordinateurs qui ne seront pas fréquemment remplacés et qui sont dotés des capacités adéquates pour accueillir un nombre grandissant de domaines de répertoire. Bien qu'il soit possible de déplacer un domaine partagé après sa configuration, vous devrez peut-être reconfigurer les politiques de recherche des ordinateurs qui se lient à ce domaine partagé, de sorte que leurs utilisateurs puissent continuer à y ouvrir des sessions.

Duplication de services Open Directory

Mac OS X Server gère la duplication du service de répertoire LDAP, du serveur de mots de passe Open Directory et du centre de distribution de clés Kerberos.

La duplication de vos services de répertoires et d'authentification vous permet :

- De rapprocher les informations de répertoires d'un groupe d'utilisateurs au sein d'un réseau distribué géographiquement, ce qui améliore les performances des services de répertoires et d'authentification pour ces utilisateurs.
- D'obtenir la redondance des services, afin que les utilisateurs ne soient que très peu affectés en cas de défaillance ou d'inaccessibilité d'un système de répertoire.

L'un des serveurs dispose d'une copie principale du domaine de répertoire LDAP partagé, du serveur de mots de passe Open Directory et du centre de distribution de clés Kerberos. Ce serveur est appelé maître Open Directory. Chaque réplique Open Directory constitue un serveur distinct contenant une copie du répertoire LDAP maître, du serveur de mots de passe Open Directory et du centre de distribution de clés Kerberos.

L'accès au répertoire LDAP sur une réplique s'effectue en lecture seule. Les modifications des enregistrements d'utilisateur et à d'autres informations du répertoire LDAP ne peuvent être apportées que sur le maître Open Directory.

Le maître Open Directory répercute automatiquement sur ses répliques tout changement apporté au répertoire LDAP. Le maître peut mettre ses répliques à jour soit dès qu'une modification survient, soit à intervalles de temps programmés. L'option des intervalles de temps programmés est la meilleure si les répliques sont connectées au maître par l'intermédiaire d'un réseau à faible débit.

Les mots de passe et les politiques de mots de passe peuvent être modifiés sur n'importe quelle réplique. Si le mot de passe ou la politique de mot de passe d'un utilisateur est modifié sur plusieurs répliques, c'est la modification la plus récente qui prévaut.

La mise à jour des répliques dépend de la synchronisation des horloges du maître et de toutes les répliques. Si les horloges des répliques et du maître affichent des différences importantes, la mise à jour risque d'être quelque peu arbitraire. Les informations de date, d'heure et de fuseau horaire doivent être correctes sur le maître et les répliques et elles doivent, si possible, utiliser le même service d'horloge réseau pour demeurer synchronisées.

Évitez de n'avoir qu'une seule réplique à une des deux extrémités d'un lien réseau lent. Si une réplique est séparée de toutes les autres répliques par un lien réseau lent et si cette réplique tombe en panne, les clients de la réplique vont basculer vers une réplique qui se trouve à l'autre extrémité du lien réseau lent. Leurs services de répertoire s'en trouveraient certainement fortement ralentis.

Si votre réseau contient un mélange de versions 10.3 et de versions 10.4 de Mac OS X Server, sachez qu'une version ne peut pas être la réplique d'un maître de l'autre version. Un maître Open Directory de version 10.4 ne peut pas se répliquer vers Mac OS X Server 10.3. De même, un maître Open Directory sous Mac OS X Server version 10.3 ne peut pas se répliquer vers Mac OS X Server 10.4.

	Maître sous Mac OS X Server 10.4	Maître sous Mac OS X Server 10.3
Réplique sous Mac OS X Server 10.4	Oui	Non
Réplique sous Mac OS X Server 10.3	Non	Oui

Répartition de la charge dans les petits, moyens et grands environnements

N'utilisez pas de logiciel de répartition de la charge de services de tiers avec des serveurs Open Directory. Un logiciel de répartition de la charge pourrait provoquer des problèmes imprévisibles sur les clients Open Directory. Il pourrait, par exemple, interférer avec la répartition de la charge et le basculement automatiques de Mac OS X et Mac OS X Server. Les clients Mac OS X recherchent automatiquement le serveur Open Directory disponible le plus proche, qu'il s'agisse du maître ou d'une réplique. Le maître ou la réplique Open Directory le plus proche d'un client est celui qui répond le plus rapidement à la demande de connexion Open Directory du client.

Réplication dans un campus comprenant plusieurs bâtiments

Quand un réseau s'étend sur plusieurs bâtiments, les connexions entre bâtiments peuvent s'avérer plus lentes qu'au sein de chaque bâtiment. Il peut arriver également que les connexions entre bâtiments soient saturées. Ces situations peuvent nuire aux performances des ordinateurs qui bénéficient de services Open Directory provenant d'un serveur situé dans un autre bâtiment. Par conséquent, il est recommandé d'installer une réplique Open Directory dans chaque bâtiment. Selon vos besoins, il peut même s'avérer intéressant d'installer une réplique Open Directory à chacun des étages d'un bâtiment qui en compte plusieurs. Chaque réplique offre ainsi des services de répertoires et d'authentification efficaces aux ordinateurs clients situés à proximité. Les ordinateurs clients n'ont plus besoin d'établir de connexion avec un serveur Open Directory via la ligne plus lente qui relie les bâtiments entre eux.

L'augmentation du nombre de répliques présente toutefois un désavantage. Les répliques communiquent entre elles et avec le maître via le réseau. Ces communications représentent une charge pour le réseau, qui augmente en proportion du nombre de répliques. L'ajout d'un trop grand nombre de répliques peut en fait accroître le trafic entre bâtiments (du fait des mises à jour de répliques) plus qu'il ne réduit les communications clientes Open Directory.

Par conséquent, lors du choix du nombre de répliques, il faut tenir compte de l'importance de l'utilisation des services Open Directory par les ordinateurs clients. Si les ordinateurs clients n'ont en moyenne que relativement peu recours aux services Open Directory et que vos bâtiments sont reliés entre eux par des connexions rapides (Ethernet à 100 Mbits/s, par exemple), vous n'avez sans doute pas besoin d'installer une réplique dans chaque bâtiment.

Vous pouvez réduire la charge des communications entre répliques et maître Open Directory en programmant la fréquence de mise à jour des répliques par le maître Open Directory. Ainsi, il n'est peut-être pas nécessaire que les répliques soient mises à jour à chaque modification apportée au maître. En choisissant une fréquence de mise à jour moins élevée, vous améliorez les performances du réseau.

Utilisation d'un maître ou d'une réplique Open Directory avec NAT

Si votre réseau dispose d'un serveur Open Directory du côté du réseau privé d'un routeur (ou d'une passerelle), y compris le routeur NAT de Mac OS X Server, seuls les ordinateurs qui se trouvent du côté du réseau privé du routeur NAT peuvent se connecter au domaine de répertoire LDAP du serveur Open Directory. Les ordinateurs qui se trouvent du côté du réseau public du routeur NAT ne peuvent pas se connecter au domaine de répertoire LDAP d'un maître ou d'une réplique Open Directory qui se trouve du côté du réseau privé.

Si un serveur Open Directory se trouve du côté du réseau public d'un routeur NAT, les ordinateurs qui se trouvent du côté du réseau privé et du côté du réseau public du routeur NAT peuvent se connecter au répertoire LDAP du serveur Open Directory.

Évitement de conflits Kerberos avec plusieurs répertoires

Si vous configurez un maître Open Directory sur un réseau qui dispose déjà d'un domaine Active Directory, votre réseau disposera de deux royaumes Kerberos. Il disposera, en effet, d'un royaume Kerberos Open Directory et d'un royaume Kerberos Active Directory. Pour des raisons pratiques, les autres serveurs sur le réseau ne peuvent utiliser qu'un des royaumes Kerberos. Lorsque vous configurez un serveur de fichiers, un serveur de courrier ou tout autre serveur qui peut utiliser l'authentification Kerberos, vous devez donc choisir un des royaumes Kerberos.

Mac OS X Server doit appartenir au même royaume Kerberos que ses utilisateurs clients. Le royaume Kerberos n'a qu'un serveur Kerberos faisant autorité. Ce serveur Kerberos prend toutes les responsabilités pour l'authentification Kerberos au sein du royaume. En effet, le serveur Kerberos ne peut authentifier des clients et des serveurs qu'au sein de son royaume. Le serveur Kerberos ne peut pas authentifier des clients ou des services qui appartiennent à un autre royaume.

Seuls les comptes d'utilisateur du royaume Kerberos choisi pourront bénéficier de la signature unique. Les comptes d'utilisateur de l'autre royaume pourront toujours s'authentifier, mais ils ne bénéficieront pas de la signature unique.

Si vous configurez un serveur pour qu'il accède à plusieurs systèmes de répertoire disposant chacun de leur propre royaume Kerberos, réfléchissez bien aux comptes d'utilisateur qui utiliseront des services kerbérisés. Vous devez connaître l'intention qui peut présider l'accès à deux services de répertoire. Vous devez connecter le serveur au royaume dont le domaine de répertoire compagnon contient les comptes d'utilisateur que vous souhaitez voir utiliser Kerberos et bénéficier de la signature unique.

Par exemple, il se peut que vous souhaitiez configurer l'accès à un royaume Active Directory pour ses enregistrements d'utilisateur et un répertoire LDAP Open Directory pour les enregistrements et les attributs Mac OS X qui ne sont pas dans Active Directory, comme, par exemple, les enregistrements de groupe et d'ordinateur. D'autres serveurs pourraient se connecter au royaume Kerberos Active Directory ou au royaume Kerberos Open Directory. Dans ce cas, il est recommandé que ces autres serveurs se connectent au royaume Kerberos Active Directory afin que les comptes d'utilisateur Active Directory bénéficient de la signature unique. Si vous avez aussi des comptes d'utilisateur dans le répertoire LDAP du serveur Open Directory, les utilisateurs peuvent toujours s'authentifier avec ces derniers. Mais les comptes d'utilisateur Open Directory n'utiliseront pas Kerberos et ne bénéficieront pas de la signature unique ; ils utiliseront des méthodes d'authentification du serveur de mots de passe Open Directory. Vous pourriez mettre tous les utilisateurs Mac dans le domaine Open Directory et tous les utilisateurs Windows dans le domaine Active Directory ; ils pourraient tous s'authentifier. Mais un seul des deux groupes d'utilisateurs pourrait utiliser Kerberos.

Important : un problème sérieux survient si vous configurez un maître ou une réplique Open Directory pour qu'il puisse aussi accéder à un domaine Active Directory. Dans ce cas, le royaume Kerberos Open Directory et le royaume Kerberos Active Directory tentent d'utiliser les mêmes fichiers de configuration sur le serveur Open Directory, ce qui perturbera probablement l'authentification Kerberos Open Directory. C'est pourquoi il vaut mieux ne pas configurer un maître ou une réplique Open Directory pour qu'il accède aussi à un domaine Active Directory ou à tout autre domaine de répertoire ayant un royaume Kerberos.

Pour éviter tout conflit de fichiers de configuration Kerberos, n'utilisez pas de serveur Open Directory comme station de travail pour la gestion des utilisateurs dans le domaine de répertoire d'un autre serveur Kerberos, comme, par exemple, dans un domaine Active Directory. Utilisez plutôt un ordinateur administrateur (un ordinateur Mac OS X sur lequel les outils d'administration de serveur sont installés) configuré pour accéder à tous les domaines de répertoire d'intérêt. Si vous devez utiliser un serveur Open Directory pour gérer les utilisateurs du domaine de répertoire d'un autre serveur, assurez-vous que l'autre domaine de répertoire ne fait pas partie de la politique de recherche d'authentification du serveur Open Directory.

Pour éviter un conflit de fichiers de configuration Kerberos, n'utilisez pas non plus un serveur Open Directory pour fournir des services qui doivent accéder au domaine de répertoire d'un autre serveur Kerberos. Par exemple, si vous devez configurer le service de fichiers AFP pour qu'il accède tant à Open Directory qu'à Active Directory, n'utilisez pas un serveur Open Directory pour fournir le service de fichiers. Utilisez un autre serveur et connectez-le au royaume Kerberos de l'un ou de l'autre service de répertoire.

En théorie, les serveurs et les clients peuvent appartenir à deux royaumes Kerberos, comme, par exemple, à un royaume Open Directory et à un royaume Active Directory. L'authentification Kerberos multiroyaume requiert toutefois une configuration très avancée, qui comprend notamment la configuration des serveurs et des clients Kerberos pour l'authentification interroyaume, la révision du logiciel des services kerbérisés afin qu'il puisse appartenir à plusieurs royaumes, etc. La description de ces procédures avancées dépasse le cadre de ce guide.

Amélioration des performances et de la redondance

Vous pouvez améliorer les performances des services Open Directory en ajoutant de la mémoire au serveur et en limitant les services qu'il fournit. Cette stratégie est également valable pour tous les autres services de Mac OS X Server. Plus vous limitez le nombre de services offerts par un serveur, meilleures sont ses performances.

Au-delà de cette stratégie générale, vous pouvez aussi améliorer les performances des serveurs Open Directory en plaçant la base de données LDAP sur un volume qui lui est propre et les historiques Open Directory sur un autre volume.

Si vous prévoyez de placer des répliques d'un maître Open Directory sur votre réseau, vous pouvez améliorer les performances du réseau en réduisant la fréquence de mise à jour des répliques. Une réduction de la fréquence de mise à jour signifie que les répliques contiennent des données de répertoires moins actuelles. Vous devez donc trouver un compromis entre performances du réseau et exactitude des répertoires des répliques.

Pour accroître la redondance des services Open Directory, vous pouvez installer des serveurs supplémentaires comme répliques Open Directory. Une autre stratégie de redondance consiste à utiliser des serveurs équipés de systèmes RAID pour les services Open Directory.

Sécurité d'Open Directory

Avec Mac OS X Server, un serveur disposant d'un domaine de répertoire LDAP partagé fournit aussi l'authentification Open Directory. Les données d'authentification stockées par Open Directory sont particulièrement sensibles. Ces données d'authentification comprennent la base de données du serveur de mots de passe Open Directory ainsi que la base de données Kerberos extrêmement sensible. Par conséquent, vous devez vous assurer que le maître Open Directory et toutes les répliques Open Directory sont bien protégés :

- La sécurité physique d'un serveur maître ou réplique Open Directory est essentielle. Ces serveurs doivent se trouver dans des pièces fermées à clé. Ne laissez jamais de session ouverte sur ces serveurs.
- Gardez en lieu sûr les supports de sauvegarde de la base de données du serveur de mots de passe Open Directory et de la base de données Kerberos. Le fait de placer vos serveurs Open Directory dans une pièce fermée à clé ne protégera pas la bande de sauvegarde que vous laissez sur votre bureau tous les soirs.
- Évitez si possible d'utiliser les serveurs Open Directory, maître ou répliques, pour d'autres services. S'il vous est impossible de consacrer exclusivement vos serveurs aux rôles de maîtres ou de répliques Open Directory, essayez au moins de limiter le nombre d'autres services qu'ils fournissent. L'un de ces autres services pourrait comporter une faille de sécurité permettant un accès illicite aux bases de données Kerberos ou du serveur de mots de passe Open Directory. L'emploi de serveurs dédiés aux services Open Directory est une solution idéale mais pas obligatoire.
- Configurez des listes de contrôle d'accès aux services (SACL) pour la fenêtre de connexion et SSH afin de déterminer quels utilisateurs peuvent se connecter à un maître ou à une réplique Open Directory.
- Évitez d'utiliser un volume RAID partagé avec d'autres ordinateurs comme volume de démarrage d'un serveur qui est maître ou réplique Open Directory. Une faille de sécurité sur l'un des autres ordinateurs représente une menace potentielle pour la sécurité des informations d'authentification Open Directory.
- Configurez le service de coupe-feu IP pour qu'il bloque tous les ports à l'exception de ceux utilisés pour les protocoles de répertoires, d'authentification et d'administration.

- Le serveur de mots de passe Open Directory utilise les ports 106 et 3659.
- Le centre de distribution de clés Kerberos utilise le port TCP/UDP 88 et le port TCP/UDP 749 est utilisé pour l'administration Kerberos.
- Le répertoire partagé LDAP utilise le port TCP 389 pour les connexions normales et le port TCP 636 pour les connexions SSL.
- Lorsque vous créez une réplique Open Directory, le port 22 doit être ouvert entre le maître et la future réplique. C'est le port utilisé pour les transferts de données Secure Shell (SSH), le protocole utilisé pour transférer une copie complète et à jour de la base de données LDAP. Après la configuration initiale de la réplique, seul le port LDAP (389 ou 636) est utilisé pour la réplication.
- Gestionnaire de groupe de travail utilise les ports TCP 311 et 625.
- Admin Serveur utilise le port TCP 311.
- SMB/CIFS utilise les ports TCP/UDP 137, 138, 139 et 445.

- Équipez l'ordinateur maître Open Directory d'un système d'alimentation sans coupure (onduleur).

En résumé, la solution pratique la plus sûre consiste à dédier exclusivement chaque serveur maître ou réplique Open Directory aux services Open Directory. Installez sur chacun de ces serveurs un coupe-feu afin qu'ils n'acceptent que les protocoles d'accès aux répertoires, d'authentification et d'administration : LDAP, serveur de mots de passe, Kerberos, Gestionnaire de groupe de travail et Gestionnaire du serveur. Protégez physiquement chaque serveur Open Directory ainsi que leurs supports de sauvegarde.

La réplication de données de répertoire et d'authentification sur le réseau représente un risque minime pour la sécurité. En effet, les données de mot de passe sont répliquées de façon sécurisée à l'aide de clés aléatoires négociées lors de chaque session de réplication. La partie du trafic de duplication concernant l'authentification (le serveur de mots de passe Open Directory et le centre de distribution de clés Kerberos) est entièrement cryptée. Pour plus de sécurité, vous pouvez configurer les connexions réseau entre serveurs Open Directory afin qu'elles utilisent des commutateurs réseau plutôt que des concentrateurs. Ainsi, le trafic de duplication d'authentification sera limité aux segments de réseau fiables.

Outils pour la gestion des services de répertoire Open Directory

Les applications Admin Serveur, Format de répertoire et Gestionnaire de groupe de travail fournissent des interfaces graphiques pour la gestion des services Open Directory sous Mac OS X Server. De plus, vous pouvez gérer les services Open Directory à partir de la ligne de commandes de Terminal. Gestionnaire NetInfo est aussi disponible pour les domaines NetInfo hérités (vous pouvez aussi utiliser l'Inspecteur de Gestionnaire de groupe de travail).

Toutes ces applications sont livrées avec Mac OS X Server et peuvent être installées sur un autre ordinateur sous Mac OS X 10.4 ou ultérieur pour faire de cet ordinateur un ordinateur administrateur. Pour plus d'informations sur la configuration d'un ordinateur administrateur, lisez le chapitre sur l'administration de serveur dans le guide Premiers contacts.

Admin Serveur

L'application Admin Serveur donne accès à des outils destinés à la configuration, la gestion et le contrôle des services Open Directory et d'autres services. Admin serveur vous permet de :

- Configurer Mac OS X Server en tant que maître ou réplique Open Directory, en tant que serveur connecté à un système de répertoire ou en tant que serveur autonome ne comportant qu'un répertoire local. Pour obtenir des instructions, consultez le chapitre 5, "Configuration des services Open Directory"
- Configurer des systèmes Mac OS X Server supplémentaires de telle manière qu'ils puissent utiliser le centre de distribution de clés Kerberos d'un maître ou d'une réplique Open Directory. Pour obtenir des instructions, consultez le chapitre 5.
- Faire migrer de NetInfo vers LDAP le domaine de répertoire partagé d'un serveur mis à niveau. Pour obtenir des instructions, consultez le chapitre 5.
- Configurer les options LDAP d'un maître Open Directory. Pour obtenir des instructions, consultez le chapitre 5.
- Configurer le service DHCP pour qu'il fournisse l'adresse d'un serveur LDAP à des ordinateurs Mac OS X utilisant des politiques de recherche automatiques. Pour plus de détails, consultez le chapitre du guide d'administration de services réseau consacré au DHCP.
- Définir des politiques de mot de passe s'appliquant à tous les utilisateurs qui ne disposent pas de politique de mot de passe particulières. Pour plus de détails, consultez le chapitre 6, "Gestion de l'authentification d'utilisateur" Pour définir des politiques de mot de passe, utilisez Gestionnaire de groupe de travail. Voir à ce propos le chapitre 6.
- Contrôler les services Open Directory. Pour obtenir des instructions, consultez le chapitre 8, "Maintenance et résolution des problèmes".

Consultez le chapitre sur l'administration de serveurs dans le guide Premiers contacts pour obtenir des informations élémentaires sur l'utilisation d'Admin Serveur, y compris sur les sujets suivants :

- Ouverture de l'application Admin Serveur et authentification
- Utilisation de serveurs spécifiques
- Administration des services
- Contrôle de l'accès aux services
- Utilisation de SSL pour l'administration à distance des serveurs
- Personnalisation de l'environnement d'Admin Serveur

Admin Serveur est installé dans le dossier /Applications/Server/.

Format de répertoire

Format de répertoire détermine comment un ordinateur Mac OS X utilise les services de répertoire, détecte les services de réseau et recherchent des informations d'authentification et de contacts dans les services de répertoire. Format de répertoire vous permet de :

- Configurer l'accès à des répertoires LDAP, à un domaine Active Directory, à un domaine NIS et à des domaines NetInfo.
- Configurer le mappage de données pour les répertoires LDAP.
- Définir des politiques de recherche d'informations d'authentification et de contacts dans plusieurs services de répertoire.
- Activer ou désactiver les différents types de services de répertoires et de détection de services de réseau.

Format de répertoire peut se connecter à d'autres serveurs sur votre réseau afin que vous puissiez les configurer à distance.

Pour plus d'informations sur l'utilisation de Format de répertoire, lisez le chapitre 7, "Gestion de Format de répertoire"

Format de répertoire est installé, sur tous les ordinateurs Mac OS X, dans le dossier /Applications/Utilitaires/.

Gestionnaire de groupe de travail

L'application Gestionnaire de groupe de travail permet une gestion complète des clients de Mac OS X Server. Gestionnaire de groupe de travail vous permet de :

- Configurer et gérer les comptes d'utilisateur, de groupe et les listes d'ordinateurs. Pour obtenir des instructions sur la gestion de l'authentification des utilisateurs, consultez le chapitre 6, "Gestion de l'authentification d'utilisateur" Pour obtenir des instructions sur d'autres rubriques liées à la gestion des utilisateurs, des groupes et des ordinateurs, consultez le guide de gestion des utilisateurs et le guide d'administration des services Windows.

- Gérer les points de partage pour le service de fichiers et les répertoires de départ des utilisateurs. Pour obtenir des instructions, consultez le chapitre consacré aux points de partage dans le guide d'administration de services de fichiers, le chapitre consacré aux répertoires de départ dans le guide de gestion des utilisateurs et le chapitre consacré à la gestion des services Windows dans le guide d'administration des services Windows.
- Contrôler ce que les utilisateurs Mac OS X voient lorsqu'ils sélectionnent le globe Réseau dans une barre latérale du Finder. Pour obtenir des instructions, consultez le chapitre consacré à la gestion des présentations de réseau dans le guide de gestion des utilisateurs.
- Visionner des entrées de répertoire sous une forme brute à l'aide de l'Inspecteur. Pour obtenir des instructions, consultez la section "Affichage et modification directs des données de répertoire" à la page 179.

Consultez le chapitre consacré à l'administration de serveurs dans le guide Premiers contacts pour obtenir des informations élémentaires sur l'utilisation de Gestionnaire de groupe de travail, y compris sur les sujets suivants :

- Ouverture et authentification dans Gestionnaire de groupe de travail
- Administration des comptes
- Personnalisation de l'environnement de Gestionnaire de groupe de travail

Gestionnaire de groupe de travail se trouve dans le dossier /Applications/Server/.

Outils de ligne de commande

Toute une série d'outils de ligne de commande est disponible pour les administrateurs qui préfèrent utiliser l'administration de serveur à l'aide de commandes. Pour la gestion de serveur à distance, soumettez les commandes dans une session Secure Shell (SSH). Vous pouvez taper des commandes sur des serveurs et des ordinateurs Mac OS X à l'aide de l'application Terminal qui se trouve dans le dossier /Applications/Utilitaires/. Pour plus de détails, consultez le guide de l'administration en ligne de commande.

Gestionnaire NetInfo

Gestionnaire NetInfo permet d'afficher et de modifier des enregistrements, des attributs et des valeurs dans les domaines NetInfo hérités, sur les ordinateurs qui utilisent encore ou ont été mis à niveau à partir de Mac OS X Server version 10.2 ou antérieure. Ces mêmes tâches peuvent être effectuées à l'aide de l'Inspecteur dans Gestionnaire de groupe de travail. Vous pouvez aussi utiliser le Gestionnaire NetInfo pour gérer une hiérarchie NetInfo héritée ou sauvegarder et restaurer un domaine NetInfo hérité.

Le Gestionnaire NetInfo se trouve dans le dossier /Applications/Utilitaires/.

Configuration des services Open Directory

5

Vous pouvez utiliser Admin Serveur pour configurer le rôle Open Directory d'un serveur, le service d'authentification Kerberos par signature unique, les options LDAP et migrer de NetInfo vers LDAP.

Les services Open Directory (services de répertoires et d'authentification) constituent une partie essentielle de l'infrastructure d'un réseau. Ces services affectent considérablement les autres services et utilisateurs du réseau. C'est pourquoi Open Directory doit être configuré correctement dès le début.

Présentation générale de la configuration

Résumé des tâches principales à réaliser pour configurer les services Open Directory. Consultez les pages mentionnées pour obtenir des informations détaillées sur chaque étape.

Étape 1: Avant de commencer, élaborez un programme
Consultez la section "Avant de commencer" à la page 80 pour obtenir la liste des éléments à prendre en considération avant de configurer Open Directory sur Mac OS Server.

Étape 2: Configurez des serveurs autonomes
Si vous souhaitez configurer des serveurs qui ne recevront pas d'informations d'authentification ou d'autres informations administratives d'un service de répertoires, consultez la section "Configuration d'un serveur autonome" à la page 81.

Étape 3: Configurez un maître Open Directory
Si vous souhaitez configurer un serveur pour qu'il fournisse des services de répertoire et d'authentification, consultez les sections "Compatibilité entre maître et répliques Open Directory" à la page 82 et "Configuration d'un maître Open Directory" à la page 83.

Étape 4: Configurez les répliques de votre maître Open Directory
Si vous souhaitez configurer un ou plusieurs serveurs pour qu'ils fournissent des services de répertoire de basculement et d'authentification ou des services de répertoire à distance et d'authentification pour l'interaction rapide entre clients sur des réseaux distribués, consultez la section "Configuration d'une réplique Open Directory" à la page 85.

Étape 5: Configurez les serveurs qui se connectent à d'autres systèmes de répertoire

Si vous disposez de serveurs de fichiers ou d'autres serveurs qui doivent accéder à des services de répertoire et d'authentification, consultez la section "Configuration d'une connexion à un système de répertoire" à la page 88.

Étape 6: Configurez l'authentification Kerberos par signature unique

Si vous avez configuré un maître Open Directory, vous pouvez configurer d'autres serveurs pour qu'ils se connectent à son royaume Kerberos. Si vous configurez un maître Open Directory sans Kerberos, vous pouvez configurer Kerberos plus tard. Pour obtenir des instructions, consultez la section "Configuration de l'authentification Kerberos par signature unique" à la page 90.

Étape 7: Migrez les serveurs mis à niveau de NetInfo vers LDAP

Si vous disposez de serveurs qui ont été mis à niveau à partir de Mac OS Server 10.2 et utilisent toujours des domaines de répertoire NetInfo partagés, vous pouvez les faire migrer vers LDAP. Consultez les sections "Migration d'un domaine de répertoire de NetInfo vers LDAP" à la page 99 et "Désactivation de NetInfo après la migration vers LDAP" à la page 102.

Étape 8: Configurez Format de répertoire sur les ordinateurs clients

Si vous avez configuré un maître Open Directory, vous devez configurer les ordinateurs clients pour qu'ils accèdent à son domaine de répertoire. Vous pouvez aussi configurer les ordinateurs clients pour qu'ils accèdent à d'autres services de répertoire comme, par exemple, Microsoft Active Directory. Consultez le chapitre 7, "Gestion de Format de répertoire"

Étape 9: Expliquez aux utilisateurs comment se connecter

Consultez la section "Explication de la façon de se connecter aux utilisateurs" à la page 85.

Avant de commencer

Avant de configurer des services Open Directory pour la première fois :

- Comprenez les utilisations des données de répertoire et évaluez vos besoins en répertoires.

  Identifiez les services qui nécessitent des données issues de domaines de répertoire et déterminez quels utilisateurs auront besoin d'accéder à ces services.

  Les utilisateurs dont les informations peuvent être aisément gérées sur un serveur doivent être définis dans le répertoire LDAP partagé d'un Mac OS Server qui est un maître Open Directory. Certains de ces utilisateurs seront plutôt définis dans des domaines de répertoire d'autres serveurs, tels qu'un domaine Active Directory sur un serveur Windows.

  Ces concepts sont présentés au chapitre 1, "Service de répertoire avec Open Directory"

- Évaluez s'il vous faut plusieurs domaines partagés. Si c'est le cas, choisissez les utilisateurs à définir dans chaque domaine partagé. Pour plus d'informations, consultez les sections "Politiques de recherche multiniveaux" à la page 36 et "Simplification des modifications des données de répertoires" à la page 66.
- Déterminez quelles sont les options d'authentification nécessaires aux utilisateurs. Pour obtenir les descriptions des options disponibles, consultez le chapitre 3, "Authentification Open Directory"
- Décidez si vous allez utiliser ou non des répliques de votre maître Open Directory. Le chapitre 4, "Planification Open Directory" propose quelques recommandations.
- Choisissez les administrateurs de serveur avec beaucoup de soin. Ne donnez un mot de passe d'administrateur qu'aux personnes en qui vous avez entière confiance. Limitez au maximum le nombre d'administrateurs. N'attribuez à aucun utilisateur
- de droits d'accès d'administrateur pour procéder à des tâches mineures, telle que la modification de réglages dans une fiche d'utilisateur.

Important : les informations de répertoire font autorité ; elles ont une incidence vitale sur toute personne dont l'ordinateur les utilise.

Configuration d'Open Directory à l'aide de l'Assistant du serveur

La configuration initiale d'Open Directory a lieu lorsque vous utilisez l'Assistant du serveur pendant l'installation de Mac OS Server. Pour obtenir des instructions sur l'utilisation de l'Assistant du serveur, consultez le guide Premiers contacts.

Gestion d'Open Directory sur un serveur distant

Vous pouvez installer Admin Serveur sur un ordinateur sous Mac OS X 10.4 ou ultérieur et l'utiliser pour gérer Open Directory sur n'importe quel serveur sur votre réseau local ou au-delà. Vous pouvez aussi gérer Open Directory à distance en vous servant des outils à ligne de commande sur un ordinateur Mac OS X ou sur un ordinateur non-Macintosh. Pour plus d'informations, consultez le chapitre du guide Premiers contacts consacré à l'administration de serveur.

Configuration d'un serveur autonome

A l'aide d'Admin Serveur, vous pouvez configurer Mac OS Server pour utiliser uniquement le domaine de répertoire local du serveur. Le serveur ne fournit aucune information sur les répertoires aux autres ordinateurs et n'en obtient pas d'un système existant. (Le domaine de répertoire local ne peut être partagé.)

Important : si vous modifiez Mac OS Server pour obtenir des informations de répertoires uniquement à partir de son domaine de répertoire local, les enregistrements d'utilisateurs et les autres informations que le serveur avait auparavant récupéré sur un domaine de répertoire partagé deviendront inaccessibles :

- Les enregistrements d'utilisateur et les autres informations qui figurent dans le domaine de répertoire partagé seront supprimés.
- Les fichiers et dossiers du serveur peuvent devenir inaccessibles aux utilisateurs dont les comptes se trouvent dans le domaine de répertoire partagé.
- Si le serveur était un maître Open Directory et si d'autres serveurs y étaient connectés :
  - Des services risquent d'être interrompus sur les serveurs connectés si les comptes d'utilisateur et les autres informations du domaine de répertoire partagé deviennent inaccessibles.
  - Les utilisateurs dont les comptes se trouvent dans le domaine de répertoire partagé peuvent ne plus pouvoir accéder aux fichiers et dossiers situés sur le maître Open Directory et sur les autres serveurs qui étaient connectés à son domaine de répertoire LDAP partagé.
  - Vous pouvez archiver une copie des données de répertoire et d'authentification du maître Open Directory avant de le transformer en serveur autonome. Pour obtenir des instructions, consultez la section "Archivage d'un maître Open Directory" à la page 186. Vous pouvez aussi exporter des utilisateurs, des groupes et des listes d'ordinateurs à partir du maître Open Directory avant de le transformer en serveur autonome. Consultez le guide de gestion des utilisateurs pour en savoir plus.

Pour configurer un serveur afin qu'il utilise uniquement son propre domaine de répertoire local non partagé :

1. Ouvrez Admin Serveur et sélectionnez Open Directory pour un des serveurs de la liste Ordinateurs et services.
2. Cliquez sur Réglages (vers le bas de la fenêtre), puis cliquez sur Général (vers le haut).
3. Sélectionnez Serveur autonome dans le menu local Rôle.
4. Si vous êtes sûr que les utilisateurs et les services n'ont plus besoin d'accéder aux données de répertoire enregistrées dans le domaine de répertoire partagé que le serveur a hébergé ou auquel il était connecté, cliquez sur Enregistrer.

Compatibilité entre maître et répliques Open Directory

Le maître Open Directory et ses répliques doivent utiliser la même version de Mac OS Server.

- Un maître Open Directory sous Mac OS Server 10.4 ne peut pas se répliquer vers Mac OS Server 10.3.
- Mac OS Server 10.4 ne peut pas être une réplique d'un maître Open Directory sous Mac OS Server 10.3.
- Un maître Open Directory sous Mac OS Server 10.4 ne peut pas se répliquer vers une réplique Open Directory sous Mac OS Server 10.4.

Si vous disposez d'un maître et de répliques Open Directory qui utilisent Mac OS Server 10.3, vous devez les mettre à niveau ensemble vers 10.4. Mettez d'abord à niveau le maître, puis les répliques. Les clients du maître et des répliques continueront à recevoir des services de répertoire et d'authentification pendant la mise à niveau. Pendant la mise à niveau du maître, ses clients basculeront automatiquement vers la réplique la plus proche. Pendant la mise à niveau des différentes répliques, les clients basculeront vers le maître mis à niveau.

La mise à niveau d'un maître Open Directory à partir de Mac OS Server 10.3 vers 10.4 rompra des liens avec les répliques existantes. Après la mise à niveau d'une réplique Open Directory vers Mac OS Server 10.4, celle-ci sera un serveur autonome ; vous devrez la retransformer à nouveau en réplique. Consultez le guide de migration et de mise à niveau pour obtenir des instructions sur la mise à niveau vers Mac OS Server 10.4.

Configuration d'un maître Open Directory

A l'aide d'Admin Serveur, vous pouvez configurer Mac OS Server comme maître Open Directory afin qu'il puisse fournir des informations de répertoires et d'authentification à d'autres systèmes. Mac OS Server fournit des informations de répertoires en hébergeant un domaine de répertoire LDAP partagé. De plus, le serveur authentifie les utilisateurs dont les comptes sont enregistrés dans le domaine de répertoire LDAP partagé.

Un maître Open Directory dispose d'un serveur de mots de passe Open Directory qui prend en charge toutes les méthodes d'authentification conventionnelles requises par les services Mac OS Server. De plus, un maître Open Directory peut fournir l'authentification Kerberos pour la signature unique.

Si vous souhaitez que le maître Open Directory fournisse l'authentification Kerberos pour la signature unique, le DNS doit être disponible sur le réseau et doit être configuré correctement pour résoudre le nom DNS complet du serveur du maître Open Directory et le convertir en son adresse IP. DNS doit aussi être configuré pour résoudre l'adresse IP et la convertir dans le nom DNS complet du serveur .

Important : si vous transformez une réplique Open Directory en un maître Open Directory, la procédure à suivre dépend de savoir si la réplique doit remplacer le maître pour devenir un maître supplémentaire.

- Si vous souhaitez promouvoir une réplique pour qu'elle remplace un maître non opérationnel, suivez les instructions qui figurent dans la section "Promotion d'une réplique Open Directory" à la page 183 plutôt que les instructions ci-dessous.
- Si vous souhaitez transformer une réplique en un maître supplémentaire, mettez d'abord la réplique hors service comme décrit dans la rubrique "Mise hors service d'une réplique Open Directory" à la page 185. Transformez-la ensuite en maître en suivant les étapes décrites.

Remarque : si Mac OS Server était connecté à un système de répertoire et que vous l'avez transformé en maître Open Directory, il reste connecté à l'autre système de répertoire. Le serveur recherchera les fiches d'utilisateur et d'autres informations dans son domaine de répertoire LDAP partagé avant de rechercher dans d'autres systèmes de répertoire auxquels il est connecté.

Pour configurer un serveur en maître Open Directory :

1. Ouvrez Admin Serveur et sélectionnez Open Directory pour ce serveur dans la liste Ordinateurs et services.
2. Cliquez sur Réglages (vers le bas de la fenêtre), puis cliquez sur Général (vers le haut).
3. Si l'option Rôle est réglée sur Réplique Open Directory et que vous souhaitez créer un nouveau maître Open Directory, vous devez changer le Rôle en Serveur autonome et cliquer sur Enregistrer.

   Si vous ne transformez pas une réplique Open Directory en serveur autonome avant d'en faire un maître, vous promouvrez la réplique en maître au lieu de créer un nouveau maître. Pour plus de détails, consultez la section "Promotion d'une réplique Open Directory" à la page 183
4. Sélectionnez Maître Open Directory dans le menu local Rôle et saisissez les informations demandées.

   Nom, nom abrégé, identifiant d'utilisateur, mot de passe : vous devez créer un nouveau compte d'utilisateur pour l'administrateur principal du répertoire LDAP. Ce compte n'est pas une copie du compte d'administrateur dans le domaine de répertoire local du serveur. Il est recommandé d'utiliser, pour l'administrateur de répertoire LDAP, des noms et un identifiant d'utilisateur différents des noms et des identifiants d'utilisateur des comptes d'utilisateur qui figurent dans le domaine de répertoire local.

   Royaume Kerberos : ce champ est préréglé pour être identique au nom DNS du serveur converti en lettres majuscules. Il s'agit d'une convention pour nommer les royaumes Kerberos. Vous pouvez saisir un autre nom, si nécessaire.

   Base de recherche : ce champ est préréglé sur un suffixe de base de recherche pour le nouveau répertoire LDAP, dérivé de la partie réservée au domaine du nom DNS du serveur. Vous pouvez saisir un autre suffixe de base de recherche ou laissez le champ vide. Si vous laissez ce champ vide, c'est le suffixe de base de recherche par défaut du répertoire LDAP qui sera utilisé.
5. Cliquez sur OK, puis sur Enregistrer.

   Vous pouvez confirmer que le maître Open Directory fonctionne correctement en cliquant sur Aperçu (dans le bas de la fenêtre Admin Serveur, avec Open Directory sélectionné dans la liste Ordinateurs et services). L'état de tous les éléments listés dans la sous-fenêtre de vue d'ensemble d'Open Directory doit être "En service". Si Kerberos reste arrêté alors que vous souhaitez le démarrer, consultez la section "Kerberos est arrêté sur un maître ou une réplique Open Directory" à la page 188.

Après avoir configuré un ordinateur Mac OS Server pour qu'il soit un maître Open Directory, vous pouvez modifier sa politique de liaison, sa politique de sécurité, sa politique de mot de passe, la fréquence de réplication et des options de protocole LDAP. Pour obtenir des instructions, consultez la section "Définition d'options pour un maître ou une réplique Open Directory" à la page 95.

Vous pouvez configurer d'autres ordinateurs sous Mac OS X ou Mac OS Server pour qu'ils accèdent au domaine de répertoire LDAP partagé du serveur. Pour obtenir des instructions, consultez la section "Accès à des répertoires LDAP" à la page 130.

Explication de la façon de se connecter aux utilisateurs

Lorsqu'un ordinateur Mac OS X est connecté à un domaine de répertoire et est configuré pour qu'il affiche une liste d'utilisateurs dans la fenêtre de connexion Mac OS X, la liste peut contenir "Autre". Expliquez aux utilisateurs qui ne se sont jamais connectés à l'aide d'un compte réseau qu'ils doivent cliquer sur Autre, puis entrer le nom du compte et le mot de passe.

Les utilisateurs peuvent configurer leur ordinateurs pour que ces derniers n'affichent pas une liste d'utilisateurs dans la fenêtre de connexion. Les utilisateurs changent ce réglage en cliquant sur Options de connexion dans la sous-fenêtre Comptes des Préférences Système.

Vous pouvez faire en sorte que la fenêtre de connexion d'un ordinateur affiche la liste des utilisateurs du réseau ou n'affiche pas de liste en gérant les préférences des ordinateurs. Utilisez Gestionnaire de groupe de travail pour configurer des réglages de préférences de connexion pour le compte de liste d'ordinateurs qui contient l'ordinateur. Pour gérer des ordinateurs qui ne font pas partie d'un compte de liste d'ordinateurs particulier, configurez des réglages de préférences de connexion pour le compte Ordinateurs hôtes. Pour plus d'instructions, consultez le guide de gestion des utilisateurs.

Configuration d'une réplique Open Directory

A l'aide d'Admin Serveur, vous pouvez configurer Mac OS Server comme réplique d'un maître Open Directory afin qu'il puisse fournir les mêmes informations de répertoires et d'authentification que le maître à d'autres systèmes. Le serveur réplique héberge une copie en lecture seule du domaine de répertoire LDAP du maître. Le serveur réplique héberge aussi une copie en lecture/écriture du serveur de mots de passe Open Directory et du centre de distribution de clés Kerberos (KDC).

Les répliques Open Directory peuvent offrir les avantages suivants :

- Dans un réseau étendu (WAN) de réseaux locaux (LAN) interconnectés par des liaisons lentes, les répliques situées sur les réseaux locaux peuvent fournir aux serveurs et aux ordinateurs clients un accès rapide aux comptes d'utilisateur et aux autres informations de répertoires.

- Une réplique fournit la redondance. En cas de défaillance du maître Open Directory, les ordinateurs qui lui sont connectés basculent automatiquement vers une réplique située à proximité. Ce basculement automatique est une fonctionnalité de Mac OS X et de Mac OS Server 10.3–10.4.

Remarque : si votre réseau contient un mélange de versions 10.3 et de versions 10.4 de Mac OS Server, sachez qu'une version ne peut pas être la réplique d'un maître de l'autre version. Un maître Open Directory en version 10.4 ne peut pas se répliquer vers Mac OS Server 10.3. De même, un maître Open Directory sous Mac OS Server 10.3 ne peut pas se répliquer vers Mac OS Server 10.4.

Important : lorsque vous configurez une réplique Open Directory pour la première fois, toutes les données de répertoires et d'authentification doivent être copiées sur celle-ci à partir du maître Open Directory. La duplication peut durer plusieurs secondes ou plusieurs minutes selon la taille du domaine de répertoire. Si la duplication est effectuée via une liaison réseau lente, elle peut durer très longtemps. Pendant la duplication, le maître ne peut pas fournir les services de répertoires et d'authentification. Les comptes d'utilisateur du répertoire LDAP maître ne peuvent être utilisés pour se connecter aux services ou s'authentifier avant la fin de la duplication. Pour minimiser l'interruption des services de répertoires, configurez une réplique avant que le répertoire LDAP du maître ne soit complètement rempli ou à un moment de la journée où le service de répertoire n'est pas utilisé. Le fait de disposer d'une autre réplique déjà configurée permettra aux clients du service de répertoire de ne pas être affectés en cas d'indisponibilité du maître.

Important : si vous modifiez un ordinateur Mac OS Server qui était connecté à un autre système de répertoire pour qu'il devienne une réplique Open Directory, le serveur reste connecté à l'autre système de répertoire. Le serveur recherchera les fiches d'utilisateur et d'autres informations dans son domaine de répertoire LDAP partagé avant de rechercher dans d'autres systèmes de répertoire auxquels il est connecté.

Pour configurer un serveur afin qu'il héberge une réplique d'un maître Open Directory :

1. Assurez-vous que le maître, la future réplique et tous les coupe-feu entre eux sont configurés pour autoriser les communications SSH (port 22).

   Vous pouvez activer SSH pour Mac OS Server dans Admin Serveur. Sélectionnez le serveur dans la liste Ordinateurs et services, cliquez sur Réglages, puis sur Général, puis sélectionnez l'option SSH. Pour plus d'informations sur SSH, consultez le guide Premiers contacts.

   Pour obtenir des instructions sur l'autorisation de communications SSH à travers le coupe-feu de Mac OS Server, consultez le guide d'administration de services réseau.

2. Ouvrez Admin Serveur et sélectionnez Open Directory pour un des serveurs de la liste Ordinateurs et services.

3. Cliquez sur Réglages (vers le bas de la fenêtre), puis cliquez sur Général (vers le haut).

4 Sélectionnez Réplique Open Directory dans le menu local Rôle et saisissez les informations demandées.

"Adresse IP du maître Open Directory :" saisissez l'adresse IP du serveur qui est le maître Open Directory.

"Mot de passe root sur le maître Open Directory :" saisissez le mot de passe de l'utilisateur root du système maître Open Directory (nom d'utilisateur de l'administrateur système).

"Nom abrégé de l'administrateur de domaine sur le maître :" saisissez le nom d'un compte d'administrateur du domaine de répertoire LDAP.

"Mot de passe de l'administrateur de domaine sur le maître :" saisissez le mot de passe du compte d'administrateur dont vous avez saisi le nom.

5 Cliquez sur OK, puis sur Enregistrer.

6 Assurez-vous que la date, l'heure et le fuseau horaire sont exacts sur la réplique et sur le maître.

La réplique et le maître doivent utiliser le même service horaire de réseau pour que leurs horloges restent synchronisées.

Après que vous ayez configuré une réplique Open Directory, les autres ordinateurs s'y connecteront automatiquement selon leurs besoins. Les ordinateurs sous les versions 10.3–10.4 de Mac OS X ou de Mac OS Server conservent une liste des répliques Open Directory. Si l'un de ces ordinateurs ne parvient pas à contacter le maître Open Directory pour des services de répertoires et d'authentification, il se connecte automatiquement à la réplique du maître la plus proche.

Vous pouvez configurer les ordinateurs Mac OS X pour qu'ils se connectent à une réplique Open Directory plutôt qu'au maître Open Directory pour les services de répertoires et d'authentification. Sur chaque ordinateur Mac OS X, vous pouvez utiliser Format de répertoire pour créer une configuration LDAPv3 afin d'accéder au répertoire LDAP de la réplique. Vous pouvez également configurer un service DHCP pour qu'il fournisse le répertoire LDAP de la réplique aux ordinateurs Mac OS X qui obtiennent l'adresse d'un serveur LDAP par le service DHCP. Consultez les sections "Accès à des répertoires LDAP" à la page 130 et "Définition de politiques de recherche automatiques" à la page 127.

Le maître Open Directory met automatiquement la réplique à jour. Vous pouvez configurer le maître pour qu'il effectue ces mises à jour soit à intervalles de temps programmés, soit dès que le répertoire maître est modifié. Pour obtenir des instructions, consultez la section "Planification de la réplication d'un maître Open Directory" à la page 183.

Création de plusieurs répliques d'un maître Open Directory

Si vous souhaitez créer plus d'une réplique d'un maître Open Directory, créez une réplique à la fois. Si vous essayez de créer deux répliques simultanément, une tentative va réussir, l'autre va échouer. Une nouvelle tentative de créer la seconde réplique devrait réussir.

Configuration du basculement Open Directory

Si un maître Open Directory ou l'une de ses répliques devient indisponible, ses ordinateurs clients sous Mac OS X ou Mac OS Server trouveront automatiquement une réplique disponible et s'y connecteront.

Les répliques permettent seulement aux clients de lire les informations de répertoires. Ces informations enregistrées sur la réplique ne peuvent être modifiées avec les outils d'administration tels que Gestionnaire de groupe de travail.

Les utilisateurs dont le type de mot de passe est Open Directory peuvent modifier leurs mots de passe sur les ordinateurs connectés aux répliques Open Directory. Les répliques synchronisent automatiquement les modifications de mots de passe avec le maître. Si le maître est indisponible pendant un certain temps, les répliques synchronisent les modifications de mots de passe avec le maître une fois que ce dernier est de nouveau disponible.

Si le maître Open Directory est en panne de façon permanente et que vous disposez d'une archive à jour de ses données, vous pouvez restaurer les données sur un nouveau maître. Ou sinon, vous pouvez promouvoir une réplique en maître. Pour plus de détails, voir "Restauration d'un maître Open Directory" à la page 187 et "Promotion d'une réplique Open Directory" à la page 183.

Remarque : si un maître ou une réplique Open Directory avait des ordinateurs clients sous Mac OS X ou Mac OS Server 10.2 ou antérieur, les ordinateurs et les serveurs de version 10.2 ne basculeront pas automatiquement vers une autre réplique. Si vous remplacez un maître en panne en promouvant une réplique en maître, vous reconfigurez manuellement chaque ordinateur et serveur de version 10.2 pour qu'ils se connectent à ce nouveau maître ou à une de ses répliques. Cela se fait en utilisant Format de répertoire sur chaque ordinateur et serveur de version 10.2 pour créer une configuration LDAPv3 qui spécifie la façon dont l'ordinateur accède au nouveau maître ou à une de ses répliques. Pour obtenir des instructions, consultez la section "Accès à des répertoires LDAP" à la page 130.

Configuration d'une connexion à un système de répertoire

A l'aide d'Admin Serveur, vous pouvez configurer Mac OS Server pour obtenir des enregistrements d'utilisateur et d'autres informations de répertoires à partir du domaine de répertoire partagé d'un autre serveur. Cet autre serveur fournit également l'authentification pour ses informations de répertoires. Mac OS Server continuera à recevoir des informations de répertoire de son propre domaine de répertoire local et fournira de l'authentification pour ces informations de répertoire local.

Important : modifier Mac OS Server afin qu'il soit connecté à un autre système de répertoire et qu'il ne soit plus un maître Open Directory entraîne la désactivation de son domaine de répertoire LDAP partagé, avec les conséquences suivantes :

- Les enregistrements d'utilisateur et les autres informations qui figurent dans le domaine de répertoire partagé seront supprimés.
- Si d'autres serveurs étaient connectés au domaine de répertoire du maître, leurs services risquent d'être interrompus si les comptes d'utilisateur et d'autres informations du domaine de répertoire désactivé deviennent inaccessibles.
- Les utilisateurs dont les comptes se trouvaient dans le domaine de répertoire désactivé ne pourront plus accéder à des fichiers et dossiers du maître Open Directory et des autres serveurs qui étaient connectés au domaine de répertoire maître.

Pour configurer un serveur afin qu'il obtienne des services de répertoires à partir d'un système existant :

1. Ouvrez Admin Serveur et sélectionnez Open Directory pour un des serveurs de la liste Ordinateurs et services.
2. Cliquez sur Réglages (vers le bas de la fenêtre), puis cliquez sur Général (vers le haut).
3. Sélectionnez "Connecté à un système de répertoire" dans le menu local Rôle.
4. Si le serveur était un maître Open Directory et que vous êtes sûr que les utilisateurs et les services n'ont plus besoin d'accéder aux données de répertoires enregistrées dans le domaine de répertoire partagé que le serveur a hébergé, cliquez sur Enregistrer.
5. Cliquez sur le bouton Accès Open Directory pour configurer l'accès à l'un (ou à plusieurs) des systèmes de répertoire.

   Pour des instructions sur la configuration de l'accès à un type particulier de service de répertoire, consultez le chapitre 7, "Gestion de Format de répertoire"

   Remarque : si vous connectez Mac OS Server 10.4 ou ultérieur à un domaine de répertoire de Mac OS Server 10.3 ou antérieur, sachez que les utilisateurs définis dans le domaine de répertoire le plus ancien ne peuvent être authentifiés par la méthode NTLMv2. Cette méthode peut s'avérer nécessaire pour authentifier de façon sûre certains utilisateurs Windows pour les services Windows de Mac OS Server 10.4 et ultérieur. Le serveur de mots de passe Open Directory dans Mac OS Server 10.4 et ultérieur prend en charge l'authentification NTLMv2, mais le serveur de mots de passe dans Mac OS Server 10.3 et antérieur ne prend pas en charge NTLMv2.

   De la même façon, si vous configurez Mac OS Server 10.4 ou ultérieur pour qu'il accède à un domaine de répertoire de Mac OS Server 10.2 ou antérieur, les utilisateurs définis dans le domaine de répertoire le plus ancien ne peuvent être authentifiés par la méthode MS-CHAPv2. Cette méthode peut s'avérer nécessaire pour authentifier de façon sûre des utilisateurs pour le service VPN de Mac OS Server 4 et ultérieur. Open Directory de Mac OS Server 10.4 prend en charge l'authentification MS-CHAPv2, mais le serveur de mots de passe de Mac OS Server 10.2 ne prend pas en charge MS-CHAPv2.
6. Si le serveur que vous configurez a accès à un système de répertoire qui héberge aussi un royaume Kerberos, vous pouvez connecter le serveur au royaume Kerberos.

Pour le connecter au royaume Kerberos, vous devez connaître le nom et le mot de passe d'un administrateur Kerberos ou d'un utilisateur à qui l'on a délégué l'autorité de connecter des serveurs au royaume. Pour obtenir des instructions, consultez la section "Connecter un serveur à un royaume Kerberos" à la page 95.

Configuration de l'authentification Kerberos par signature unique

La configuration de l'authentification Kerberos à signature unique implique les tâches suivantes :

- DNS doit être disponible sur le réseau et doit être configuré correctement pour résoudre le nom DNS complet du serveur maître Open Directory (ou d'un autre serveur Kerberos) et à le convertir en son adresse IP. DNS doit aussi être configuré pour résoudre l'adresse IP et la convertir dans le nom DNS complet du serveur.
- Un administrateur configure un système de répertoire pour qu'il héberge un royaume Kerberos. Pour obtenir des instructions sur la configuration de Mac OS Server pour qu'il héberge un royaume Kerberos, consultez la section "Configuration d'un royaume Kerberos Open Directory" (ci-après).
- Un administrateur Kerberos d'un maître Open Directory peut déléguer l'autorité de connecter des serveurs au royaume Kerberos du maître Open Directory. (L'administrateur n'a pas besoin d'autorité déléguée. Un administrateur Kerberos a implicitement l'autorité de connecter tout serveur au royaume Kerberos). Consultez la section "Délégation d'autorité pour connecter des serveurs à un royaume Kerberos Open Directory" à la page 92.
- Un administrateur ou des utilisateurs Kerberos possédant l'autorité déléguée nécessaire connectent les serveurs au royaume Kerberos qui fournit alors l'authentification Kerberos par signature unique pour les services fournis par les serveurs qui ont été connectés. Consultez la section "Connecter un serveur à un royaume Kerberos" à la page 95.
- Tous les ordinateurs utilisant Kerberos doivent être réglés sur la date, l'heure et le fuseau horaire exacts. Ils doivent tous être configurés pour utiliser le même serveur horloge de réseau. Le bon fonctionnement de Kerberos repose sur la synchronisation des horloges de tous les ordinateurs participants.

Les différents services de Mac OS Server ne nécessitent aucune configuration pour la signature unique ou pour Kerberos. Les services suivants sont prêts pour l'authentification Kerberos par signature unique sur tous les serveurs sous Mac OS Server 10.4 ou ultérieur qui sont connectés ou qui sont un maître ou une réplique Open Directory : fenêtre de connexion, service de courrier, AFP, FTP, SMB/CIFS (en tant que membre d'un royaume Kerberos Active Directory), VPN, service Web Apache et service de répertoires LDAPv3 (sur un maître ou une réplique Open Directory).

Configuration d'un royaume Kerberos Open Directory

Vous pouvez fournir l'authentification Kerberos par signature unique sur votre réseau en configurant un maître Open Directory. Vous pouvez configurer un maître Open Directory lors de la configuration initiale qui suit l'installation de Mac OS Server. Mais si vous avez configuré Mac OS Server pour un autre rôle Open Directory, vous pouvez transformer ce rôle en maître Open Directory à l'aide d'Admin Serveur. Pour obtenir des instructions, consultez les sections "Configuration d'un maître Open Directory" à la page 83 et "Démarrage de Kerberos après la configuration d'un maître Open Directory" à la page 91.

Un serveur jouant le rôle de maître Open Directory ne nécessite aucune configuration supplémentaire pour gérer l'authentification Kerberos par signature unique pour tous les services kerbérisés qu'il fournit lui-même. Ce serveur peut également gérer l'authentification Kerberos par signature unique pour les services kerbérisés d'autres serveurs du réseau. Les autres serveurs doivent être configurés pour se connecter au royaume Kerberos Open Directory. Pour obtenir des instructions, consultez les sections "Délégation d'autorité pour connecter des serveurs à un royaume Kerberos Open Directory" à la page 92 et "Connecter un serveur à un royaume Kerberos" à la page 95.

Important : un maître Open Directory requiert un DNS configuré correctement pour fournir une authentification Kerberos par signature unique.

- Le service DNS doit être configuré pour résoudre les noms DNS complets de tous les serveurs, y compris le maître Open Directory lui-même, en les convertissant en adresses IP et pour fournir les recherches inverses correspondantes. Pour obtenir des instructions sur la configuration du service DNS, consultez le guide d'administration de services réseau.
- Les préférences Réseau du serveur maître Open Directory doivent être configurées pour utiliser le serveur DNS qui convertit le nom du serveur. (Si le serveur maître Open Directory fournit son propre service DNS, ses préférences Réseau doivent être configurées pour s'utiliser lui-même comme serveur DNS).

Démarrage de Kerberos après la configuration d'un maître Open Directory

Si Kerberos ne démarre pas automatiquement lorsque vous configurez un maître Open Directory, vous pouvez utiliser Admin Serveur pour le démarrer manuellement. Vous devez d'abord résoudre le problème qui empêche Kerberos de démarrer. D'habitude, le problème vient du service DNS qui n'est pas configuré correctement ou ne tourne pas du tout.

Remarque : une fois que vous avez démarré Kerberos manuellement, il se peut que les utilisateurs dont les comptes sont dotés de mots de passe Open Directory et qui ont été créés dans le répertoire LDAP du maître Open Directory alors que Kerberos était arrêté doivent réinitialiser leurs mots de passe la prochaine fois qu'ils se connectent. Un compte d'utilisateur n'est donc affecté que si toutes les méthodes d'authentification récupérables pour les mots de passe Open Directory ont été désactivées pendant que Kerberos était à l'arrêt.

Pour démarrer Kerberos manuellement sur un maître Open Directory :

1. Ouvrez Admin Serveur, connectez-vous au maître Open Directory et sélectionnez Open Directory pour le maître Open Directory dans la liste Ordinateurs et services.
2. Cliquez sur Rafraîchir (ou choisissez Présentation > Rafraîchir) et vérifiez l'état de Kerberos qui est affiché dans la sous-fenêtre Vue d'ensemble.

   Si Kerberos tourne, il n'y a rien d'autre à faire.
3. Utilisez Utilitaire de réseau (dans /Applications/Utilitaires/) pour effectuer une recherche DNS du nom DNS du maître Open Directory et une recherche inverse de l'adresse IP.

   Si le nom DNS ou l'adresse IP du serveur ne se résolvent pas correctement :
   - Dans la sous-fenêtre Réseau des Préférences Système, regardez les réglages TCP/IP de l'interface réseau principale du serveur (généralement, Ethernet intégré). Assurez-vous que le premier serveur DNS listé est celui qui résout le nom du serveur Open Directory.
   - Vérifiez la configuration du service DNS et assurez-vous qu'il tourne.
4. Dans Admin Serveur, sélectionnez Open Directory pour le serveur maître, cliquez sur Réglages, puis sur Général.
5. Cliquez sur Kerbériser, puis saisissez les informations requises.

   Nom d'administrateur et *Mot de passe :* vous devez vous authentifier en tant qu'administrateur du répertoire LDAP du maître Open Directory.

   Nom de royaume : ce champ est préréglé pour être identique au nom DNS du serveur converti en lettres majuscules. Il s'agit d'une convention pour nommer les royaumes Kerberos. Vous pouvez saisir un autre nom, si nécessaire.

Délégation d'autorité pour connecter des serveurs à un royaume Kerberos Open Directory

À l'aide d'Admin Serveur, vous pouvez déléguer l'autorité de connecter un serveur à un serveur maître Open Directory pour l'authentification Kerberos par signature unique. Vous pouvez déléguer cette autorité à un ou plusieurs comptes d'utilisateur. Les comptes d'utilisateur auxquels vous déléguez cette autorité doivent être dotés d'un mot de passe de type Open Directory et résider dans le répertoire LDAP du serveur maître Open Directory. Le serveur dépendant pour lequel vous déléguez l'autorité doit tourner sous Mac OS X Server 10.3 ou ultérieur.

Remarque : si un compte possédant l'autorité Kerberos déléguée est supprimé et recréé sur le serveur maître Open Directory, le nouveau compte ne possédera pas l'autorité de connecter le serveur dépendant au royaume Kerberos du maître Open Directory.

Un administrateur Kerberos, c'est-à-dire un administrateur LDAP Open Directory, n'a pas besoin d'autorité déléguée pour connecter des serveurs dépendants au royaume Kerberos Open Directory. Un administrateur Kerberos a implicitement l'autorité de connecter tout serveur au royaume Kerberos.

Pour déléguer l'autorité de se connecter à un royaume Kerberos Open Directory :

1. Dans Gestionnaire de groupe de travail, créez une liste d'ordinateurs dans le domaine de répertoire LDAP du serveur maître Open Directory ou sélectionnez une liste d'ordinateurs existante dans ce répertoire.

   - Pour sélectionner une liste d'ordinateurs existante dans Gestionnaire de groupe de travail, cliquez sur Comptes ou choisissez Présentation > Comptes, cliquez sur le bouton Ordinateurs (au-dessus de la liste des comptes), puis sélectionnez la liste d'ordinateurs souhaitée.
   - Si le serveur LDAP n'a pas encore de liste d'ordinateurs à laquelle vous souhaitez ajouter le serveur dépendant, vous pouvez en créer une.
     Cliquez sur Comptes, puis cliquez sur le bouton Ordinateurs.

     Cliquez sur l'icône représentant un globe au-dessus de la liste des comptes, puis déroulez le menu local pour ouvrir le répertoire LDAP du maître Open Directory.

     Cliquez sur le cadenas et authentifiez-vous comme administrateur du répertoire LDAP.

     Cliquez sur Liste (à droite), puis sur Nouvelle liste d'ordinateurs ou choisissez Serveur > Nouvelle liste d'ordinateurs.

     Tapez le nom de la liste comme, par exemple, Serveurs kerbérisés.

2. Cliquez ensuite sur le bouton Ajouter [+], puis saisissez l'adresse Ethernet principale du serveur dépendant dans le champ Adresse et le nom DNS complet du serveur dans le champ Nom.

   - *Adresse :* saisissez l'adresse Ethernet du port Ethernet principal du serveur dépendant. Le port Ethernet principal est le premier qui apparaît dans la liste de la sous-fenêtre État du réseau de l'adresse des préférences Réseau du serveur dépendant. L'adresse de ce port est affichée dans le champ Identifiant Ethernet de la sous-fenêtre Ethernet des préférences Réseau. Si vous ne saisissez pas l'adresse Ethernet correcte, le serveur dépendant sera incapable de se connecter au maître Open Directory pour l'authentification Kerberos.
   - *Nom :* Saisissez le nom DNS complet du serveur dépendant, pas seulement son nom d'hôte. Par exemple, le nom pourrait être serveur2.exemple.com, mais pas juste serveur2. Ce nom est utilisé pour créer des principaux Kerberos dans le centre de distribution de clés. Si ce nom est incorrect, les utilisateurs ne pourront pas s'authentifier à l'aide de Kerberos.
     Votre système DNS doit posséder une entrée pour le nom du serveur dépendant et une entrée de recherche inverse pour l'adresse IP du serveur dépendant.
   - *"Utiliser ce nom pour identifier l'ordinateur :"* n'affecte pas les opérations Kerberos.
   - *Commentaires :* est facultatif et purement informatif.

3. Cliquez sur Enregistrer pour enregistrer vos modifications apportées à la liste d'ordinateurs.

4. Cliquez sur Préférences et assurez-vous que la liste d'ordinateurs ne possède aucun réglage de préférence gérée.

Si une petite flèche apparaît en regard de l'icône d'un des éléments des catégories de préférences, l'élément possède des réglages de préférences gérées. Pour supprimer les préférences gérées d'un élément, cliquez sur l'élément, sélectionnez Non géré, puis cliquez sur Appliquer. Si l'élément dispose de plusieurs sous-fenêtres, sélectionnez Non géré dans chacune des sous-fenêtres, puis cliquez sur Appliquer.

5 Si vous souhaitez déléguer l'autorité Kerberos à un ou plusieurs nouveaux comptes d'utilisateur, créez-les dès à présent.

- Assurez-vous que vous travaillez bien dans le répertoire LDAP du serveur maître Open Directory. Si nécessaire, cliquez sur le petit globe et utilisez le menu local pour ouvrir ce répertoire. Cliquez ensuite sur le cadenas et authentifiez-vous comme administrateur de ce répertoire.
- Cliquez sur le bouton Utilisateurs (à gauche), puis sur Nouvel utilisateur ou choisissez Serveur > Nouvel utilisateur.
  Saisissez un nom, un nom abrégé et un mot de passe. Il n'est pas nécessaire de cocher les cases "L'utilisateur peut se connecter" et "L'utilisateur peut administrer ce serveur". Vous pouvez changer des réglages dans d'autres sous-fenêtres, mais ne changez pas le type de mot de passe d'utilisateur dans la sous-fenêtre Avancé. Tout utilisateur avec autorité Kerberos déléguée doit posséder un mot de passe Open Directory.

6 Cliquez sur Enregistrer pour enregistrer le nouveau compte d'utilisateur.

7 Ouvrez Admin Serveur, connectez-vous au serveur maître Open Directory et sélectionnez Open Directory pour ce serveur dans la liste Ordinateurs et services.

8 Cliquez sur Réglages (vers le bas de la fenêtre), puis cliquez sur Général (vers le haut).

9 Confirmez le rôle de maître Open Directory, cliquez sur Ajouter un enregistrement Kerberos, puis saisissez les informations requises.

- *Nom d'administrateur :* saisissez le nom d'un administrateur de répertoire LDAP sur le serveur maître Open Directory.
- *Mot de passe d'administrateur :* saisissez le mot de passe du compte d'administrateur que vous avez saisi.
- *Nom de fiche de configuration :* saisissez le nom DNS complet exactement comme vous l'avez saisi quand vous avez ajouté le serveur dépendant à la liste d'ordinateurs à l'étape 2.
- *Administrateurs délégués :* saisissez un nom abrégé ou un nom long pour chaque compte d'utilisateur auquel vous souhaitez déléguer l'autorité Kerberos pour le serveur spécifié. Au cas où le compte d'utilisateur serait supprimé un jour, saisissez au moins deux noms.

10 Cliquez sur Enregistrer pour déléguer l'autorité Kerberos.

Si vous souhaitez déléguer l'autorité pour plusieurs serveurs dépendants, répétez cette procédure pour chacun d'entre eux.

Pour obtenir des instructions sur la connexion d'un serveur à un royaume Kerberos Open Directory, consultez la section "Connecter un serveur à un royaume Kerberos" (ci-après).

Connecter un serveur à un royaume Kerberos

Avec Admin Serveur, un administrateur Kerberos ou un utilisateur dont le compte possède l'autorité déléguée correctement peut connecter Mac OS Server à un royaume Kerberos. Le serveur ne peut se connecter qu'à un seul royaume Kerberos. Il peut s'agir d'un royaume Kerberos Open Directory, d'un royaume Kerberos Active Directory ou d'un royaume Kerberos MIT existant.

Pour se connecter à un royaume Kerberos Open Directory, vous devez disposer d'un compte d'administrateur Kerberos ou d'un compte d'utilisateur possédant l'autorité Kerberos déléguée. Pour obtenir des instructions, consultez la section "Délégation d'autorité pour connecter des serveurs à un royaume Kerberos Open Directory" à la page 92.

Pour connecter un serveur à un royaume Kerberos :

1. Assurez-vous que le serveur que vous souhaitez connecter au royaume Kerberos est configuré pour accéder au domaine de répertoire partagé du serveur Kerberos.

   Pour confirmer, ouvrez Format de répertoire sur le serveur que vous souhaitez connecter au royaume Kerberos ou connectez-vous au serveur à l'aide de Format de répertoire sur un autre ordinateur. Cliquez sur Authentification et assurez-vous que le domaine de répertoire du serveur Kerberos apparaît bien dans la liste. Si ce n'est pas le cas, consultez le chapitre 7, "Gestion de Format de répertoire" pour obtenir des instructions sur la configuration de l'accès au répertoire.

2. Ouvrez Admin Serveur, connectez-vous au serveur que vous souhaitez connecter au royaume Kerberos et sélectionnez Open Directory pour ce serveur dans la liste Ordinateurs et services.
3. Cliquez sur Réglages (vers le bas de la fenêtre), puis cliquez sur Général (vers le haut).
4. Confirmez que le Rôle est bien Connecté à un système de répertoire, puis cliquez sur Se connecter à Kerberos et saisissez les informations requises.
   - Pour un royaume Kerberos Open Directory ou un royaume Kerberos Active Directory, choisissez le royaume dans le menu local et saisissez le nom et le mot de passe d'un administrateur Kerberos ou d'un utilisateur possédant l'autorité Kerberos déléguée pour le serveur.
   - Pour un royaume Kerberos MIT, saisissez le nom et le mot de passe d'un administrateur Kerberos, le nom du royaume Kerberos et le nom DNS du serveur de centre de distribution de clés Kerberos.

Définition d'options pour un maître ou une réplique Open Directory

Vous pouvez définir des politiques de liaison, de sécurité et de mot de passe pour un maître Open Directory et ses répliques. Vous pouvez aussi définir plusieurs options LDAP pour un maître ou une réplique Open Directory. Pour obtenir des instructions, consultez les sections suivantes :

- "Configuration d'une politique de liaison pour un maître Open Directory" (ci-après).
- "Configuration d'une politique de sécurité pour un maître et des répliques Open Directory" à la page 97.
- "Changement de politique de mot de passe globale" à la page 110.
- "Modification de l'emplacement d'une base de données LDAP" à la page 97.
- "Limitation des résultats de la recherche pour le service LDAP" à la page 98.
- "Modification du délai de recherche autorisé pour le service LDAP" à la page 98.
- "Configuration de SSL pour le service LDAP" à la page 99.

Configuration d'une politique de liaison pour un maître Open Directory

À l'aide d'Admin Serveur, vous pouvez configurer un maître Open Directory pour qu'il autorise ou exige une liaison sécurisée entre le répertoire LDAP et les ordinateurs qui y accèdent. Les répliques du maître Open Directory héritent automatiquement de sa politique de liaison.

Une liaison LDAP sécurisée est authentifiée mutuellement. L'ordinateur prouve son identité en utilisant le nom et le mot de passe d'un administrateur du répertoire LDAP pour s'authentifier auprès du répertoire LDAP. Le répertoire LDAP prouve son authenticité au moyen d'un enregistrement d'ordinateur authentifié qui est créé dans le répertoire lorsque vous configurez la liaison sécurisée.

Les clients ne peuvent pas être configurés pour utiliser à la fois la liaison LDAP sécurisée et un serveur LDAP fourni par le DHCP (connu aussi sous le nom d'option DHCP 95). La liaison LDAP sécurisée est en réalité une liaison statique, alors que le LDAP fourni le DHCP est une liaison dynamique. Pour plus de détails, consultez la section "Activation ou désactivation d'un répertoire LDAP fourni via DHCP" à la page 131.

Remarque : les clients ont besoin de la version 10.4 ou ultérieure de Mac OS X ou de Mac OS Server pour pouvoir utiliser la liaison LDAP sécurisée. Les clients sous 10.3 ou antérieur ne sont pas capables de configurer la liaison sécurisée.

Pour configurer la politique de liaison pour un maître Open Directory :

1. Ouvrez Admin Serveur, connectez-vous au serveur maître Open Directory et sélectionnez ce serveur dans la liste Ordinateurs et services.
2. Cliquez sur Réglages (au bas de la fenêtre), puis sur Politique (en haut).
3. Cliquez sur Liaison, puis définissez les options de liaison de répertoire souhaitées.
   - Pour autoriser la liaison sécurisée, cochez la case "Activer la liaison de répertoire".
   - Pour exiger la liaison sécurisée, cochez aussi la case "Requiert les clients pour se lier au répertoire".
4. Cliquez sur Enregistrer.

Configuration d'une politique de sécurité pour un maître et des répliques Open Directory

À l'aide d'Admin Serveur, vous pouvez configurer une politique de sécurité pour accéder au répertoire LDAP d'un maître Open Directory.

Les répliques du maître Open Directory héritent automatiquement de sa politique de sécurité.

Pour configurer la politique de sécurité pour un maître Open Directory :

1. Ouvrez Admin Serveur, connectez-vous au serveur maître Open Directory et sélectionnez ce serveur dans la liste Ordinateurs et services.
2. Cliquez sur Réglages (dans le bas de la fenêtre), puis sur Politique (dans la haut).
3. Cliquez sur Liaison, puis définissez les options de sécurité souhaitées.
   - *"Désactiver les mots de passe en clair"* détermine si les clients peuvent envoyer les mots de passe en clair si les mots de passe ne peuvent pas être validés à l'aide d'une méthode d'authentification qui envoie les mots de passe cryptés. Pour plus d'informations, consultez les sections "Sélection de méthodes d'authentification pour des utilisateurs de mots de passe shadow" à la page 113 et "Sélection de méthodes d'authentification pour des utilisateurs de mots de passe Open Directory" à la page 114.
   - *"Signer tous les paquets numériquement (requiert Kerberos)"* permet de s'assurer que les données de répertoire provenant du serveur LDAP ne seront pas interceptées et modifiées par un autre ordinateur pendant qu'elles transitent vers les ordinateurs clients.
   - *"Crypter tous les paquets (requiert SSL ou Kerberos)"* oblige le serveur LDAP à crypter les données de répertoire à l'aide de SSL ou de Kerberos avant de les envoyer aux ordinateurs clients.
   - *" Bloquer les attaques Man-in-the-Middle (requiert Kerberos)"* empêche un éventuel serveur malveillant de se faire passer pour la serveur LDAP. Plus efficace avec l'option "Signer tous les paquets numériquement".
4. Cliquez sur Enregistrer.

En fonction du réglage ici, les options de sécurité peuvent aussi être configurées individuellement sur les différents clients d'un maître ou d'une réplique Open Directory. Si vous sélectionnez une option ici, elle ne pourra pas être désélectionnée pour un client. Pour obtenir des instructions sur la configuration de ces options sur un client, consultez la section "Modification de la politique de sécurité pour une connexion LDAP" à la page 142.

Modification de l'emplacement d'une base de données LDAP

En utilisant Admin Serveur, vous pouvez spécifier l'emplacement du disque de la base de données qui stocke les enregistrements d'utilisateur et d'autres informations dans un domaine de répertoire LDAP d'un maître ou d'une réplique Open Directory. La base de données LDAP est généralement située sur le volume de démarrage, mais peut se trouver sur un volume local différent.

Remarque : pour des raisons de sécurité, les bases de données qui contiennent les informations d'authentification pour Open Directory et Kerberos sont toujours placées sur le volume de démarrage, quel que soit l'emplacement de la base de données LDAP.

Pour modifier l'emplacement d'une base de données LDAP partagée :

1. Ouvrez Admin Serveur, puis, dans la liste des Ordinateurs et services, sélectionnez Open Directory pour un serveur qui est un maître ou une réplique Open Directory.
2. Cliquez sur Réglages (vers le bas de la fenêtre), puis cliquez sur Protocoles (vers le haut).
3. Choisissez Réglages LDAP dans le menu local Configurer, puis spécifiez le chemin d'accès au dossier dans lequel vous voulez placer la base de données LDAP.

   Vous pouvez saisir le chemin à un dossier dans le champ Base de données ou sélectionner l'emplacement d'un dossier en cliquant sur le bouton Parcourir (...).
4. Cliquer sur Enregistrer.

Limitation des résultats de la recherche pour le service LDAP

Admin Serveur vous permet d'empêcher un type d'attaque par saturation sur le Mac OS Server en limitant le nombre de résultats de recherche renvoyés par le domaine de répertoire LDAP partagé du serveur. Cela empêche un utilisateur malveillant de bloquer le serveur en lui envoyant des requêtes de recherches LDAP multiples et complexes.

Pour définir un nombre maximal de résultats de recherche LDAP :

1. Ouvrez Admin Serveur, puis, dans la liste des Ordinateurs et services, sélectionnez Open Directory pour un serveur qui est un maître ou une réplique Open Directory.
2. Cliquez sur Réglages (vers le bas de la fenêtre), puis cliquez sur Protocoles (vers le haut).
3. Choisissez Réglages LDAP dans le menu local Configurer, puis tapez le nombre maximal de résultats de recherche.
4. Cliquer sur Enregistrer.

Modification du délai de recherche autorisé pour le service LDAP

A l'aide d'Admin Serveur, vous pouvez empêcher un type d'attaque par saturation sur le Mac OS Server en limitant le temps alloué au serveur pour effectuer une recherche sur son domaine de répertoire LDAP partagé. Cela empêche un utilisateur malveillant de bloquer le serveur en lui envoyant une requête de recherche LDAP exceptionnellement complexe.

Pour définir un délai pour les recherches LDAP :

1. Ouvrez Admin Serveur, puis, dans la liste des Ordinateurs et services, sélectionnez Open Directory pour un serveur qui est un maître ou une réplique Open Directory.
2. Cliquez sur Réglages (vers le bas de la fenêtre), puis cliquez sur Protocoles (vers le haut).
3. Choisissez Réglages LDAP dans le menu local Configurer, puis spécifiez un délai de recherche.
4. Cliquer sur Enregistrer.

Configuration de SSL pour le service LDAP

À l'aide d'Admin Serveur, vous pouvez activer Secure Sockets Layer (SSL) pour les communications cryptées entre un domaine de répertoire LDAP d'un serveur Open Directory et les ordinateurs qui y accèdent. SSL utilise des certificats numériques pour fournir une identité certifiée pour le serveur. Vous pouvez utiliser un certificat auto-signé ou un certificat provenant d'une autorité de certification. Consultez le guide d'administration de services de messagerie pour obtenir des informations détaillées sur la définition, l'obtention et l'installation de certificats sur votre serveur.

Les communications SSL pour LDAP utilisent le port 636. Si SSL est désactivé pour le service LDAP, les communications sont envoyées en clair sur le port 389.

Pour configurer des communications SSL pour le service LDAP :

1. Ouvrez Admin Serveur, puis, dans la liste des Ordinateurs et services, sélectionnez Open Directory pour un serveur qui est un maître ou une réplique Open Directory.
2. Cliquez sur Réglages (vers le bas de la fenêtre), puis cliquez sur Protocoles (vers le haut).
3. Choisissez Réglages LDAP dans le menu local Configurer, puis cochez la case Activer SSL (Secure Sockets Layer).
4. Utilisez le menu local Certificat pour choisir le certificat SSL que vous souhaitez voir utiliser par le service LDAP.

   Le menu dresse la liste tous les certificats SSL qui sont installés sur le serveur. Pour utiliser un certificat qui ne figure pas dans la liste, choisissez Configuration personnalisée dans le menu local.
5. Cliquer sur Enregistrer.

Migration d'un domaine de répertoire de NetInfo vers LDAP

Vous pouvez utiliser Admin Serveur pour faire migrer un domaine de répertoire NetInfo partagé vers LDAP une fois que vous avez procédé à une installation de mise à niveau vers Mac OS Server 10.4 ou ultérieur. Une fois que vous avez fait migrer le domaine de répertoire, les ordinateurs clients peuvent continuer à utiliser NetInfo pour accéder au domaine de répertoire ou bien ils peuvent être configurés pour utiliser LDAP afin d'y accéder.

Vous pouvez faire basculer automatiquement des ordinateurs clients sous Mac OS X 10.3–10.4 ou Mac OS Server 10.3–10.4 vers l'utilisation de LDAP pour accéder au domaine de répertoire ayant migré. Le processus de migration peut enregistrer des informations d'aiguillage automatique dans le domaine de répertoire. Lorsque Mac OS X et Mac OS Server 10.3–10.4 utilisent NetInfo pour accéder à un domaine de répertoire ayant migré vers LDAP, ils collectent les informations d'aiguillage automatique présentes dans le domaine de répertoire et se reconfigurent pour accéder au domaine de répertoire en utilisant dorénavant LDAP. Pour en savoir plus, consultez la section "Bascule de l'accès au répertoire de NetInfo vers LDAP" (la prochaine rubrique).

Si aucun des ordinateurs clients de votre réseau n'a besoin de l'accès NetInfo à un domaine de répertoire ayant migré vers LDAP, vous pouvez désactiver l'accès NetInfo à ce domaine en cliquant sur un bouton. Après la désactivation de NetInfo, les ordinateurs clients ne peuvent plus basculer automatiquement vers LDAP. (L'accès au domaine de répertoire NetInfo local n'est pas affecté). Pour obtenir des instructions, consultez la section "Désactivation de NetInfo après la migration vers LDAP" à la page 102.

Le processus de migration déplace tous les types d'enregistrements et de données standard de la base de données NetInfo vers une base de données LDAP. Si le domaine de répertoire NetInfo avait été modifié pour accueillir des types d'enregistrements ou de données personnalisés, ces derniers ne sont pas transférés vers la base de données LDAP.

La migration vers LDAP ne modifie pas la méthode de validation des mots de passe d'utilisateurs, sauf pour les mots de passe validés par le Gestionnaire d'authentification. Les mots de passe qui étaient validés par un serveur de mots de passe continuent à l'être par le même serveur. Si certains comptes d'utilisateur du domaine NetInfo utilisaient le Gestionnaire d'authentification pour la validation des mots de passe, le processus de migration convertit ces comptes pour qu'ils disposent d'un type de mot de passe Open Directory. Bien entendu, un administrateur peut modifier le type de mot de passe de tout compte d'utilisateur ayant migré vers Open Directory pour que ce compte d'utilisateur puisse bénéficier de l'authentification Kerberos par signature unique.

Avertissement : veillez à ne pas cliquer par inadvertance sur le bouton Désactiver NetInfo. Cette action a pour effet de désactiver immédiatement l'accès NetInfo au domaine de répertoire. Cette action est irréversible. Après la désactivation de NetInfo, tous les ordinateurs ayant besoin de se connecter au domaine de répertoire doivent être configurés pour se connecter via LDAP.

Pour faire migrer un domaine de répertoire partagé d'un serveur de NetInfo vers LDAP :

1. Ouvrez Admin Serveur et sélectionnez Open Directory pour un serveur maître Open Directory dans la liste des Ordinateurs et services.
2. Cliquez sur Réglages (vers le bas de la fenêtre), puis cliquez sur Protocoles (vers le haut).
3. Choisissez Migration NetInfo dans le menu local Configurer.
4. Cliquez sur Migrer et définissez des options de migration.

   "Nom abrégé d'administrateur :" le nom abrégé d'un compte d'administrateur du domaine de répertoire local du serveur que vous voulez copier vers le répertoire LDAP ayant migré. Ce compte sera un administrateur du domaine de répertoire LDAP.

   " Mot de passe d'administrateur :" le mot de passe du compte administrateur dont vous avez saisi le nom abrégé.

"Nom de royaume Kerberos :" par convention, le nom de royaume Kerberos est identique au nom DNS du serveur, mais il s'écrit en lettres capitales. Ainsi, un serveur dont le nom DNS est exemple.com aurait le nom de royaume Kerberos EXEMPLE.COM.

"Base de recherche (facultatif):" le suffixe de base de recherche du répertoire LDAP ayant migré. Le suffixe de la base de recherche provient généralement du nom DNS du serveur. Ainsi, le suffixe de la base de recherche pourrait être "dc=exemple, dc=com" pour un serveur dont le nom DNS est serveur.exemple.com.

"Faire basculer les clients NetInfo existants sur LDAP :" permet aux ordinateurs clients sous Mac OS X ou Mac OS Server 10.3–10.4 de se reconfigurer automatiquement pour accéder au domaine de répertoire ayant migré en utilisant LDAP au lieu de NetInfo.

5 Cliquez sur OK pour lancer la migration.

Le processus de migration peut durer un certain temps.

Lorsque la migration est terminée, vous pouvez configurer le service DHCP pour qu'il fournisse l'adresse du serveur LDAP aux ordinateurs clients disposant de politiques de recherche automatique. Les ordinateurs sous Mac OS X ou Mac OS Server 10.2–10.4 peuvent posséder des politiques de recherche automatique. Ces ordinateurs n'ont pas besoin d'être configurés individuellement pour accéder au serveur LDAP. Lorsque ces ordinateurs démarrent, ils tentent d'obtenir une adresse d'un serveur LDAP à partir du service DHCP. Pour obtenir des instructions sur la configuration du service DHCP afin qu'il fournisse une adresse de serveur LDAP, consultez le guide d'administration de services réseau.

Bascule de l'accès au répertoire de NetInfo vers LDAP

Après la migration d'un domaine de répertoire partagé de Mac OS Server de NetInfo vers LDAP, certains clients basculeront automatiquement vers LDAP, mais il se peut que vous ayez à configurer d'autres clients pour qu'ils utilisent LDAP et à reconfigurer le service DHCP.

- Les ordinateurs sous Mac OS X ou Mac OS Server 10.3–10.4 qui utilisaient NetInfo pour accéder au domaine de répertoire ayant migré peuvent basculer automatiquement vers LDAP. Les basculement automatique doit être activé au moment de la migration du domaine de répertoire de NetInfo vers LDAP. Mac OS X ne peut plus basculer automatiquement vers LDAP après la désactivation de NetInfo sur le serveur du domaine de répertoire migré. Consultez la section "Migration d'un domaine de répertoire de NetInfo vers LDAP" à la page 99.
- Vous pouvez configurer les différents ordinateurs pour accéder au répertoire LDAP plutôt qu'au domaine de répertoire NetInfo. Pour obtenir des instructions, consultez la section au chapitre 7, "Gestion de Format de répertoire".

- Les ordinateurs disposant d'une politique de recherche automatique peuvent obtenir l'adresse de leur serveur de répertoires via le service DHCP. Si votre serveur Open Directory a de tels clients, vous pouvez changer le service DHCP pour qu'il fournisse l'adresse du serveur du répertoire LDAP ayant migré.
- Lorsqu'aucun des ordinateurs clients de votre réseau n'a besoin de l'accès NetInfo à un domaine de répertoire ayant migré vers LDAP, vous pouvez désactiver NetInfo à l'aide d'Admin Serveur. consultez la section "Désactivation de NetInfo après la migration vers LDAP" (ci-après).

Désactivation de NetInfo après la migration vers LDAP

Si aucun des ordinateurs clients de votre réseau n'a besoin de l'accès NetInfo à un domaine de répertoire ayant migré vers LDAP, vous pouvez utiliser Admin Serveur pour désactiver l'accès NetInfo à ce domaine. (L'accès au domaine de répertoire NetInfo local n'est pas affecté).

Important : ne désactivez pas NetInfo prématurément. Après la désactivation de NetInfo, tous les ordinateurs ayant besoin de se connecter au domaine de répertoire doivent être configurés pour se connecter via LDAP.

Pour désactiver l'accès NetInfo à un domaine de répertoire ayant fait l'objet d'une migration vers LDAP :

1. Avant de désactiver NetInfo sur le serveur, assurez-vous que le DHCP ne fournit pas l'adresse du serveur pour la liaison NetInfo.
2. Ouvrez Admin Serveur et sélectionnez Open Directory pour un serveur maître Open Directory dans la liste des Ordinateurs et services.
3. Cliquez sur Réglages (vers le bas de la fenêtre), puis cliquez sur Protocoles (vers le haut).
4. Choisissez Migration NetInfo dans le menu local Configurer.
5. Cliquez sur Désactiver NetInfo.

   Cette action a pour effet de désactiver immédiatement l'accès NetInfo au domaine de répertoire. Cette action est irréversible.

Gestion de l'authentification d'utilisateur

6

Apprenez comment réinitialiser des mots de passe d'utilisateur, changer de type de mot de passe, définir des politiques de mot de passe, sélectionner des méthodes d'authentification, etc.

Vous pouvez gérer les informations d'authentification des utilisateurs stockées dans les domaines de répertoire. Pour trouver les descriptions des tâches et des instructions, reportez-vous à :

Composition d'un mot de passe

Le mot de passe associé à un compte d'utilisateur doit être saisi par l'utilisateur lorsqu'il s'authentifie pour ouvrir une session ou pour d'autres services. Le mot de passe est sensible à la casse (hormis les mots de passe LAN Manager-SMB). Il est masqué à l'écran pendant sa saisie.

Quel que soit le type de mot de passe choisi pour un utilisateur, voici quelques directives à suivre pour la composition d'un mot de passe d'utilisateur de Mac OS X Server :

- Les mots de passe doivent contenir des lettres, des chiffres et des symboles et former des combinaisons difficiles à deviner par les utilisateurs non autorisés. Ils ne doivent pas être constitués de mots réels. Les bons mots de passe associent des chiffres et des symboles (comme # ou $). Ils peuvent également être composés en juxtaposant la première lettre de tous les mots d'une phrase particulière. Utilisez une combinaison de lettres minuscules et majuscules.
- Évitez les espaces ainsi que les caractères obtenus à l'aide de la touche Option.
- Évitez les caractères impossibles à saisir sur les ordinateurs dont se servira l'utilisateur ou qui réclament, sur d'autres claviers et plates-formes, l'emploi d'une combinaison de touches spéciale.
- Certains protocoles réseau n'acceptent pas les mots de passe contenant des espaces initiaux, des espaces incorporés ou des espaces finaux.
- Un mot de passe vide n'est pas recommandé ; Open Directory et certains systèmes (comme la liaison LDAP) ne l'acceptent pas.

Pour une compatibilité optimale avec les ordinateurs et services auxquels vos utilisateurs sont susceptibles d'accéder, utilisez uniquement des caractères ASCII dans les mots de passe.

Modification du mot de passe d'un utilisateur

Vous pouvez utiliser Gestionnaire de groupe de travail pour changer le mot de passe d'un compte d'utilisateur défini dans un autre domaine de répertoire sur lequel vous possédez un accès en lecture/écriture. Par exemple, vous pouvez changer le mot de passe d'un compte d'utilisateur du répertoire LDAP d'un maître LDAP.

Important : si vous changez le mot de passe d'un compte d'utilisateur qui est utilisé pour authentifier la connexion de répertoire LDAP d'un ordinateur, vous devez soit apporter le même changement aux réglages de connexion LDAP de l'ordinateur concerné, soit configurer le répertoire LDAP et toutes les connexions pour qu'ils utilisent la liaison sécurisée. Pour obtenir des instructions, consultez les sections "Modification du mot de passe utilisé pour authentifier une connexion LDAP" à la page 151 ou "Configuration d'une politique de liaison pour un maître Open Directory" à la page 96 et "Configuration d'une liaison sécurisée vers un répertoire LDAP" à la page 146.

Pour changer le mot de passe d'un utilisateur :

1. Dans Gestionnaire de groupe de travail, cliquez sur le bouton Comptes, puis sur le bouton Utilisateur.
2. Ouvrez le domaine de répertoire contenant le compte d'utilisateur dont vous voulez changer le mot de passe et authentifiez-vous en tant qu'administrateur du domaine.

   Pour ouvrir un domaine de répertoire, cliquez sur l'icône de globe au-dessus de la liste des utilisateurs, puis choisissez un domaine dans le menu local.

   Si le type du mot de passe de l'utilisateur est Open Directory, vous devez vous authentifier en tant qu'administrateur dont le type de mot de passe est Open Directory.
3. Sélectionnez le compte du mot de passe à changer.
4. Tapez un mot de passe dans la sous-fenêtre Élémentaire, puis cliquez sur Enregistrer.
5. Indiquez à l'utilisateur le nouveau mot de passe à employer pour ouvrir une session.

   Une fois que l'utilisateur a ouvert une session sous Mac OS X à l'aide du nouveau mot de passe, il peut le modifier en cliquant sur Comptes dans Préférences Système.

Si vous changez le mot de passe d'un compte dont le type de mot de passe est Open Directory et que ce compte réside dans le répertoire LDAP d'une réplique ou d'un maître Open Directory, le changement sera synchronisé avec le maître et toutes ses répliques. Mac OS X Server synchronise automatiquement les modifications de mots de passe Open Directory entre un maître et ses répliques.

Réinitialisation des mots de passe de plusieurs utilisateurs

À l'aide de Gestionnaire de groupe de travail, vous pouvez sélectionner en même temps plusieurs comptes utilisateurs et les modifier pour qu'ils prennent tous le même type de mot de passe et le même mot de passe temporaire.

Pour changer le type de mot de passe et le mot de passe de plusieurs comptes d'utilisateur :

1. Dans Gestionnaire de groupe de travail, cliquez sur le bouton Comptes, puis sur le bouton Utilisateur.
2. Ouvrez le domaine de répertoire contenant le compte d'utilisateur dont vous voulez réinitialiser les types de mot de passe et les mots de passe, puis authentifiez-vous en tant qu'administrateur du domaine.

   Pour ouvrir un domaine de répertoire, cliquez sur l'icône de globe au-dessus de la liste des utilisateurs, puis choisissez un domaine dans le menu local.

   Si vous voulez régler le type de mot de passe sur Open Directory, vous devez vous authentifier en tant qu'administrateur dont le type de mot de passe est Open Directory.
3. Cliquez sur les comptes d'utilisateur en maintenant les touches Commande ou Maj pour sélectionner ceux dont le type de mot de passe doit être changé.

4 Tapez un mot de passe dans la sous-fenêtre Élémentaire, puis définissez le type de mot de passe dans la sous-fenêtre Avancé.

5 Cliquer sur Enregistrer.

6 Indiquez aux utilisateurs le mot de passe temporaire, de sorte qu'ils puissent ouvrir une session.

Après avoir ouvert une session à l'aide du mot de passe temporaire, un utilisateur peut changer le mot de passe en cliquant sur Comptes dans Préférences Système.

Si vous changez le mot de passe de comptes dont le type de mot de passe est Open Directory et que ces comptes résident dans le répertoire LDAP d'une réplique ou d'un maître Open Directory, le changement sera synchronisé avec le maître et toutes ses répliques. Mac OS X Server synchronise automatiquement les modifications de mots de passe Open Directory entre un maître et ses répliques.

Modification du type de mot de passe d'un utilisateur

Vous pouvez définir le type de mot de passe dans la sous-fenêtre Avancé de Gestionnaire de groupe de travail. Les types de mot de passe disponibles sont les suivants :

- Open Directory active plusieurs méthodes d'authentification héritées, ainsi que l'authentification Kerberos par signature unique si le compte de l'utilisateur se trouve dans le répertoire LDAP d'un maître ou d'une réplique Open Directory. Les mots de passe Open Directory sont stockés séparément de la base de données du serveur de mots de passe Open Directory et du centre de distribution de clés Kerberos. Consultez la section "Choix du type de mot de passe Open Directory" à la page 107.
- Le mot de passe shadow active plusieurs méthodes d'authentification héritées pour les comptes d'utilisateur dans le domaine de répertoire local. Les mots de passe shadow sont stockés hors du domaine de répertoire, dans des fichiers qui ne sont lisibles que par l'utilisateur root. Consultez la section "Choix du type de mot de passe shadow" à la page 109.
- Le mot de passe crypté fournit une authentification élémentaire pour un compte d'utilisateur dans un domaine de répertoire partagé. Un mot de passe crypté est stocké dans l'enregistrement de compte d'utilisateur, dans le domaine de répertoire. Un mot de passe crypté est nécessaire pour se connecter à Mac OS X 10.1 et antérieur. Consultez la section "Changement du type de mot en Mot de passe crypté" à la page 108.

Choix du type de mot de passe Open Directory

Avec Gestionnaire de groupe de travail, vous pouvez indiquer qu'un compte d'utilisateur dispose d'un mot de passe Open Directory stocké dans des bases de données sécurisées hors du domaine de répertoire. Les comptes d'utilisateur dans les domaines de répertoire suivants peuvent disposer de mots de passe Open Directory :

- domaine de répertoire LDAP sous Mac OS X Server 10.3–10.4
- domaine de répertoire local de Mac OS X Server 10.3 ou serveur mis à niveau à partir de la version 10.3
- domaine de répertoire sur Mac OS X Server 10.2 configuré pour utiliser un serveur de mots de passe

Le type de mot de passe Open Directory prend en charge la signature unique à l'aide de l'authentification Kerberos. Il prend aussi en charge le serveur de mots de passe Open Directory, qui offre des protocoles d'authentification Simple Authentication and Security Layer (SASL), notamment APOP, CRAM-MD5, DHX, Digest-MD5, MS-CHAPv2, NTLMv2, NTLM (aussi appelé Windows NT ou SMB-NT), LAN Manager (LM) et WebDAV-Digest.

Remarque : pour régler le type de mot de passe d'un compte d'utilisateur sur Open Directory, vous devez posséder des droits d'administrateur pour l'authentification Open Directory dans le domaine de répertoire contenant le compte d'utilisateur. Cela veut dire que vous devez vous authentifier en tant qu'administrateur de domaine de répertoire dont le type de mot de passe est Open Directory. Pour plus d'informations, consultez la section "Attribution de droits d'administrateur pour l'authentification Open Directory" à la page 115.

Pour indiquer qu'un compte d'utilisateur doit avoir un mot de passe Open Directory :

1. Assurez-vous que le compte réside dans un domaine de répertoire qui gère l'authentification Open Directory.

   Les domaines de répertoire qui prennent en charge l'authentification Open Directory sont cités plus haut dans cette rubrique.

2. Dans Gestionnaire de groupe de travail, ouvrez le compte à utiliser (si ce n'est déjà fait).

   Pour ouvrir un compte, cliquez sur le bouton Comptes, puis sur le bouton Utilisateurs. Cliquez sur l'icône de globe située au-dessus de la liste des utilisateurs, puis utilisez le menu local pour ouvrir le domaine de répertoire où réside le compte de l'utilisateur. Cliquez sur le cadenas, puis authentifiez-vous en tant qu'administrateur de domaine de répertoire dont le type de mot de passe est Open Directory. Sélectionnez ensuite l'utilisateur dans la liste.

3. Cliquez sur Avancé, puis choisissez Open Directory dans le menu local Type du mot de passe.

4. Lorsque vous y êtes invité, tapez et confirmez un nouveau mot de passe.

Le mot de passe ne doit pas contenir plus de 512 octets (jusqu'à 512 caractères d'après la langue), bien que le protocole d'authentification réseau puisse imposer d'autres limites, comme, par exemple, 128 caractères pour NTLMv2 et NTLM, et 14 pour LAN Manager. "Composition d'un mot de passe" à la page 104 vous donne des indications pour le choix de mots de passe.

5 Dans la sous-fenêtre Avancé, cliquez sur Options pour configurer la politique de mot de passe de l'utilisateur, puis sur OK lorsque vous avez terminé de choisir vos options.

Si vous sélectionnez l'option "Désactiver connexion à partir de", tapez une date au format JJ/MM/AAAA ; par exemple, 22/02/2004.

Si vous sélectionnez une option qui nécessite une réinitialisation (un changement) du mot de passe, souvenez-vous que tous les protocoles n'acceptent pas le changement de mots de passe. Par exemple, les utilisateurs ne peuvent changer leur mot de passe lors d'une authentification au service de courrier IMAP.

L'identifiant de mot de passe est un nombre unique à 128 bits attribué lors de la création du mot de passe dans la base de données du serveur de mots de passe Open Directory. Il peut se révéler utile en cas de dépannage, puisqu'il apparaît dans l'historique de serveur de mots de passe lorsqu'un problème se produit. Pour obtenir des instructions, consultez la section "Affichage des états et des historiques Open Directory" à la page 178. Pour afficher cet historique Open Directory, ouvrez Admin Serveur.

6 Cliquer sur Enregistrer.

Changement du type de mot en Mot de passe crypté

Si nécessaire, vous pouvez utiliser Gestionnaire de groupe de travail pour indiquer qu'un mot de passe crypté doit être stocké dans le compte d'utilisateur. Le compte d'utilisateur peut faire partie d'un domaine de répertoire LDAP ou d'un domaine NetInfo partagé hérité.

Les comptes d'utilisateur inutilisés sur les ordinateurs qui requièrent un mot de passe crypté doivent avoir un mot de passe Open Directory ou un mot de passe shadow. Il faut un mot de passe crypté pour se connecter sur un ordinateur client sous Mac OS X 10.1 et antérieur et sur les ordinateurs clients sous certaines variantes d'UNIX.

Le mot de passe crypté est stocké sous forme de valeur cryptée (ou empreinte) dans le compte d'utilisateur. Le mot de passe crypté étant facilement accessible à partir du domaine de répertoire, il est sujet à des attaques hors connexion et par conséquent il est moins sûr que les autres types de mot de passe.

Pour indiquer qu'un compte d'utilisateur doit être doté d'un mot de passe crypté :

1 Dans Gestionnaire de groupe de travail, ouvrez le compte à utiliser (si ce n'est déjà fait).

Pour ouvrir un compte, cliquez sur le bouton Comptes, puis sur le bouton Utilisateurs. Cliquez sur l'icône de globe située au-dessus de la liste des utilisateurs, puis utilisez le menu local pour ouvrir le domaine de répertoire où réside le compte de l'utilisateur. Cliquez sur le cadenas et authentifiez-vous en tant qu'administrateur de domaine de répertoire. Sélectionnez ensuite l'utilisateur dans la liste.

2 Cliquez sur Avancé, puis choisissez Mot de passe crypté dans le menu local Type du mot de passe.

3 Lorsque vous y êtes invité, tapez et confirmez un nouveau mot de passe.

La longueur maximale d'un mot de passe crypté est de huit octets (huit caractères ASCII). Si vous tapez un mot de passe plus long, seuls les huit premiers octets seront utilisés.

4 Cliquer sur Enregistrer.

Choix du type de mot de passe shadow

Gestionnaire de groupe de travail vous permet d'indiquer qu'un utilisateur dispose d'un mot de passe shadow stocké dans un fichier sécurisé en dehors du domaine de répertoire. Seuls les utilisateurs dont les comptes résident dans le domaine de répertoire local peuvent disposer d'un mot de passe shadow.

Pour indiquer qu'un compte d'utilisateur doit être doté d'un mot de passe shadow :

1 Dans Gestionnaire de groupe de travail, ouvrez le compte à utiliser (si ce n'est déjà fait).

Pour ouvrir un compte, cliquez sur le bouton Comptes, puis sur le bouton Utilisateurs. Cliquez sur l'icône de globe au-dessus de la liste des utilisateurs, puis choisissez dans le menu local le domaine de répertoire local où se trouve le compte de l'utilisateur. Cliquez sur le cadenas et authentifiez-vous en tant qu'administrateur de domaine de répertoire. Sélectionnez ensuite l'utilisateur dans la liste.

2 Cliquez sur Avancé, puis choisissez Mot de passe Shadow dans le menu local Type du mot de passe.

3 Lorsque vous y êtes invité, tapez et confirmez un nouveau mot de passe.

Il se peut qu'un mot de passe long soit tronqué pour certaines méthodes d'authentification. Les 128 premiers caractères du mot de passe sont utilisés pour NTLMv2 et NTLM, mais seuls les 14 premiers caractères sont utilisés pour LAN Manager. "Composition d'un mot de passe" à la page 104 vous donne des indications pour le choix de mots de passe.

4 Dans la sous-fenêtre Avancé, cliquez sur Options pour configurer la politique de mot de passe de l'utilisateur, puis sur OK lorsque vous avez terminé de choisir vos options.

Si vous sélectionnez l'option "Désactiver connexion à partir de", tapez une date au format JJ/MM/AAAA, comme, par exemple, 22/02/2005.

Si vous utilisez une politique qui nécessite un changement de mot de passe d'utilisateur, rappelons que tous les protocoles n'acceptent pas la modification de mots de passe. Par exemple, les utilisateurs ne peuvent changer leur mot de passe lors d'une authentification au service de courrier IMAP.

5 Dans la sous-fenêtre Avancé, cliquez sur Sécurité pour activer ou désactiver des méthodes d'authentification pour l'utilisateur, puis sur OK lorsque vous avez terminé.

Pour plus d'informations, consultez la section "Configuration des politiques de mot de passe d'utilisateurs individuels" à la page 111.

6 Cliquez sur Enregistrer.

Activation de l'authentification Kerberos par signature unique pour un utilisateur

L'activation de l'authentification Kerberos par signature unique pour un compte d'utilisateur dans un répertoire LDAP de Mac OS X Server se fait en réglant le type de mot de passe du compte sur Open Directory dans la sous-fenêtre Avancé de Gestionnaire de groupe de travail.

Les comptes d'utilisateur à partir de Mac OS X Server 10.2 qui disposent déjà d'un mot de passe de type Open Directory doivent être réinitialisés pour activer Kerberos et l'authentification par signature unique. Réglez d'abord le type de mot de passe sur Mot de passe crypté, puis réglez-le sur Open Directory. Pour obtenir des instructions détaillées, consultez les sections "Changement du type de mot en Mot de passe crypté" à la page 108 et "Choix du type de mot de passe Open Directory" à la page 107.

Changement de politique de mot de passe globale

Admin Serveur vous permet de définir une politique de mot de passe globale pour les comptes d'utilisateur d'un domaine de répertoire Mac OS X Server. La politique de mot de passe globale affecte les comptes d'utilisateur du domaine de répertoire local du serveur. Si le serveur est un maître ou une réplique Open Directory, la politique de mot de passe globale affecte aussi les comptes d'utilisateur qui ont un mot de passe de type Open Directory dans le domaine de répertoire LDAP du serveur. Si vous changez la politique de mot de passe globale sur une réplique Open Directory, les réglages de la politique seront synchronisés avec le maître et toutes ses autres répliques.

Les administrateurs de comptes ne sont pas affectés par les politiques de mot de passe. Chaque utilisateur peut avoir une politique de mot de passe individuelle qui redéfinit certains réglages de la politique de mot de passe globale. Pour plus d'informations, consultez la section "Configuration des politiques de mot de passe d'utilisateurs individuels" à la page 111.

Kerberos et le serveur de mots de passe Open Directory maintiennent des politiques de mot de passe séparées. Mac OS X Server synchronise les règles de la politique de mot de passe de Kerberos avec les règles de la politique de mot de passe du serveur de mots de passe Open Directory.

Pour changer la politique de mot de passe globale de tous les comptes d'utilisateur du même domaine :

1. Ouvrez Admin Serveur, connectez-vous à un maître ou à une réplique Open Directory et sélectionnez Open Directory pour ce serveur dans la liste Ordinateurs et services.
2. Cliquez sur Réglages (au bas de la fenêtre), puis sur Politique (en haut).
3. Cliquez sur Mots de passe, puis définissez les options de politique de mot de passe souhaitées pour les utilisateurs qui ne disposent pas de leur propre politique de mot de passe individuelle.

   Si vous sélectionnez une option qui nécessite une réinitialisation du mot de passe, souvenez-vous que certains protocoles de services n'autorisent pas le changement de mots de passe. Par exemple, les utilisateurs ne peuvent changer leur mot de passe lors d'une authentification au service de courrier IMAP.
4. Cliquez sur Enregistrer.

Les répliques du maître Open Directory héritent automatiquement de sa politique de mot de passe globale.

À partir de la ligne de commande

Vous pouvez aussi définir des politiques de mot de passe à l'aide de la commande `pwpolicy` dans Terminal. Pour en savoir plus, consultez le chapitre consacré à Open Directory du guide d'administration à l'aide de la ligne de commande.

Configuration des politiques de mot de passe d'utilisateurs individuels

À l'aide de Gestionnaire de groupe de travail, vous pouvez définir des politiques de mot de passe pour des comptes d'utilisateur individuels dont le type de mot de passe est Open Directory ou Mot de passe shadow. La politique de mot de passe d'un utilisateur prime sur la politique de mot de passe globale définie dans la sous-fenêtre Réglages d'authentification du service Open Directory dans Admin Serveur.

La politique de mot de passe pour un compte d'utilisateur mobile s'applique lorsque le compte est utilisé alors que l'ordinateur portable est déconnecté du réseau. La politique de mot de passe provenant du compte d'utilisateur réseau correspondant s'applique lorsque l'ordinateur portable est connecté au réseau. Les administrateurs de comptes ne sont pas affectés par les politiques de mot de passe.

Pour définir une politique de mot de passe pour un compte d'utilisateur qui dispose d'un mot de passe Open Directory, vous devez posséder des droits d'administrateur pour l'authentification Open Directory dans le domaine de répertoire contenant le compte d'utilisateur. Cela veut dire que vous devez vous authentifier en tant qu'administrateur de domaine de répertoire dont le type de mot de passe est Open Directory. Pour plus d'informations, consultez la section "Attribution de droits d'administrateur pour l'authentification Open Directory" à la page 115.

Kerberos et le serveur de mots de passe Open Directory conservent séparément les politiques de mot de passe. Mac OS X Server synchronise les règles de la politique de mot de passe de Kerberos avec les règles de la politique de mot de passe du serveur de mots de passe Open Directory.

N'utilisez pas le bouton Options de la sous-fenêtre Avancé pour configurer des politiques de mot de passe pour des administrateurs de domaine de répertoire. Les politiques de mot de passe n'affectent pas les comptes d'administrateur. Les administrateurs de domaines de répertoire doivent pouvoir changer les politiques de mot de passe des comptes d'utilisateur individuels.

Pour changer la politique de mot de passe d'un compte d'utilisateur :

1 Dans Gestionnaire de groupe de travail, ouvrez le compte à utiliser (si ce n'est déjà fait).

Pour ouvrir un compte, cliquez sur le bouton Comptes, puis sur le bouton Utilisateurs. Cliquez sur l'icône de globe située au-dessus de la liste des utilisateurs, puis utilisez le menu local pour ouvrir le domaine de répertoire où réside le compte de l'utilisateur. Cliquez sur le cadenas, puis authentifiez-vous en tant qu'administrateur de domaine de répertoire dont le type de mot de passe est Open Directory. Sélectionnez ensuite l'utilisateur dans la liste.

2 Cliquez sur Avancé, puis sur Options.

Vous ne pouvez cliquer sur Options que si le type de mot de passe est Open Directory ou Mot de passe Shadow.

3 Modifiez les options de politique de mot de passe, puis cliquez sur OK.

Si vous sélectionnez une option qui nécessite une réinitialisation (un changement) du mot de passe, souvenez-vous que certains protocoles de services n'autorisent pas le changement de mots de passe. Par exemple, les utilisateurs ne peuvent changer leur mot de passe lors d'une authentification au service de courrier IMAP.

4 Cliquez sur Enregistrer.

À partir de la ligne de commande

Vous pouvez aussi définir des politiques de mot de passe à l'aide de la commande `pwpolicy` dans Terminal. Pour en savoir plus, consultez le chapitre consacré à Open Directory du guide d'administration à l'aide de la ligne de commande.

Sélection de méthodes d'authentification pour des utilisateurs de mots de passe shadow

À l'aide de Gestionnaire de groupe de travail, vous pouvez sélectionner les méthodes d'authentification qui seront disponibles pour un compte d'utilisateur dont le type de mot de passe est Mot de passe Shadow. Le mot de passe shadow prend en charge les méthodes d'authentification disponibles pour la compatibilité avec certains logiciels clients. Si vous savez que l'utilisateur n'utilisera jamais un logiciel client qui requiert une méthode d'authentification particulière, vous pouvez désactiver cette méthode. Pour plus d'informations, consultez la section "Désactivation des méthodes d'authentification de mots de passe shadow" à la page 57.

Important : si vous désactivez une méthode d'authentification, son condensé numérique sera supprimé du fichier de mots de passe shadow à la prochaine authentification de l'utilisateur. Si vous activez une méthode d'authentification qui était désactivée, le condensé numérique de la méthode nouvellement activée sera ajouté au fichier de mots de passe shadow de l'utilisateur à la prochaine authentification de l'utilisateur pour un service qui peut utiliser un mot de passe en clair comme, par exemple, la fenêtre de connexion ou AFP. D'un autre côté, le mot de passe de l'utilisateur peut être réinitialisé pour ajouter le condensé numérique de la méthode nouvellement activée. Les utilisateurs peuvent réinitialiser leurs propres mots de passe ou un administrateur de répertoire peut le faire pour eux.

Si vous souhaitez activer ou désactiver des méthodes d'authentification pour des comptes d'utilisateur dont le type de mot de passe est Open Directory, consultez la rubrique suivante.

Pour activer ou désactiver des méthodes d'authentification pour un utilisateur de mot de passe shadow :

1. Dans Gestionnaire de groupe de travail, ouvrez le compte à utiliser (si ce n'est déjà fait).

   Pour ouvrir un compte, cliquez sur le bouton Comptes, puis sur le bouton Utilisateurs. Cliquez sur l'icône de globe au-dessus de la liste des utilisateurs, puis choisissez dans le menu local le domaine de répertoire local où se trouve le compte de l'utilisateur. Cliquez sur le cadenas et authentifiez-vous en tant qu'administrateur de domaine de répertoire. Sélectionnez ensuite l'utilisateur dans la liste.

2. Cliquez sur Avancé, puis sur Sécurité.

   Vous ne pouvez cliquer sur Sécurité que si le type de mot de passe est Open Directory ou Mot de passe Shadow.

3. Sélectionnez les méthodes d'authentification que vous souhaitez activer et désélectionnez celles que vous souhaitez désactiver, puis cliquez sur OK.

4. Cliquer sur Enregistrer.

À partir de la ligne de commande

Vous pouvez aussi activer ou désactiver des méthodes d'authentification pour un utilisateur possédant un mot de passe shadow à l'aide de la commande `pwpolicy` dans Terminal. Pour en savoir plus, consultez le chapitre consacré à Open Directory du guide d'administration à l'aide de la ligne de commande.

Sélection de méthodes d'authentification pour des utilisateurs de mots de passe Open Directory

À l'aide d'Admin Serveur, vous pouvez sélectionner les méthodes d'authentification qui seront disponibles pour tous les comptes d'utilisateur dont le type de mot de passe est Open Directory. Le mot de passe Open Directory prend en charge les méthodes d'authentification disponibles pour la compatibilité avec certains logiciels clients. Si vous savez que les utilisateurs n'utiliseront jamais un logiciel client qui requiert une méthode d'authentification particulière, vous pouvez désactiver cette méthode. Pour plus d'informations, consultez la section "Désactivation des méthodes d'authentification Open Directory" à la page 56.

Important : si vous désactivez une méthode d'authentification, son condensé numérique sera supprimé de la base de données de mots de passe à la prochaine authentification de l'utilisateur. Si vous activez une méthode d'authentification qui était désactivée, chaque mot de passe Open Directory doit être réinitialisé pour ajouter le condensé numérique de la méthode nouvellement activée à la base de données de mots de passe. Les utilisateurs peuvent réinitialiser leurs propres mots de passe ou un administrateur de répertoire peut le faire pour eux.

Si vous souhaitez activer ou désactiver des méthodes d'authentification pour des comptes d'utilisateur dont le type de mot de passe est Mot de passe Shadow, consultez la rubrique suivante.

Pour activer ou désactiver des méthodes d'authentification pour des mots de passe Open Directory :

1. Ouvrez Admin Serveur, connectez-vous à un maître Open Directory et sélectionnez Open Directory pour ce serveur dans la liste Ordinateurs et services.
2. Cliquez sur Réglages (au bas de la fenêtre), puis sur Politique (en haut).
3. Cliquez sur Sécurité, puis sélectionnez les méthodes d'authentification que vous souhaitez activer et désélectionnez celles que vous souhaitez désactiver.
4. Cliquer sur Enregistrer.

Les répliques du maître Open Directory héritent automatiquement des réglages de méthode d'authentification pour les mots de passe Open Directory dans le répertoire LDAP.

À partir de la ligne de commande

Vous pouvez aussi activer ou désactiver des méthodes d'authentification du serveur de mots de passe pour tous les mots de passe Open Directory à l'aide de la commande `NeST` avec les arguments `-getprotocols` et `-setprotocols` dans Terminal. Pour en savoir plus, consultez le chapitre consacré à Open Directory du guide d'administration à l'aide de la ligne de commande.

Attribution de droits d'administrateur pour l'authentification Open Directory

À l'aide de Gestionnaire de groupe de travail et d'un compte d'administrateur possédant les droits nécessaires pour définir des réglages de mot de passe Open Directory, vous pouvez attribuer ces droits à d'autres comptes d'utilisateur du même domaine de répertoire. Pour assigner ces droits, votre compte d'utilisateur doit avoir un mot de passe Open Directory et les autorisations nécessaires pour administrer des comptes d'utilisateur. Cette restriction renforce la protection des mots de passe stockés dans le centre de distribution de clés Kerberos et dans la base de données du serveur de mots de passe Open Directory.

Pour attribuer des droits d'administrateur pour l'authentification Open Directory à un compte d'utilisateur :

1. Dans Gestionnaire de groupe de travail, ouvrez le compte souhaité, cliquez sur Avancé et assurez-vous que le type de mot de passe est bien réglé sur Open Directory.

   Pour plus d'informations, consultez la section "Choix du type de mot de passe Open Directory" à la page 107.

2. Dans la sous-fenêtre Élémentaire, assurez-vous que la case "L'utilisateur peut administrer ce domaine de répertoire" est bien cochée.
3. Cliquez sur Autorisations et assurez-vous que la case "Modifier les comptes d'utilisateur" est bien cochée.

   Pour en savoir plus sur la configuration d'autorisations d'administrateur, consultez le guide de gestion des utilisateurs.

Synchronisation des mots de passe d'administrateur principaux

Sur un serveur Open Directory mis à niveau à partir de Mac OS X Server 10.3, le compte d'administrateur principal existe, en principe, tant dans le répertoire local du serveur que dans son répertoire LDAP. Ce compte a été copié du répertoire local vers le répertoire LDAP lors de la création du maître Open Directory avec Mac OS X Server 10.3. À l'origine, les deux copies de ce compte avaient toutes deux l'identifiant d'utilisateur 501, le même nom et le même mot de passe. Chaque compte est un administrateur de son domaine de répertoire et les deux sont des administrateurs de serveur. Lorsque vous vous connectez au serveur dans Gestionnaire de groupe de travail à l'aide du nom et du mot de passe du compte, vous êtes automatiquement authentifié pour le domaine de répertoire local et le domaine de répertoire LDAP.

Si vous changez un des deux mots de passe, vous ne serez plus authentifié automatiquement pour les deux domaines de répertoire. Par exemple, si vous utilisez le mot de passe de l'administrateur du répertoire local lorsque vous vous connectez au serveur dans Gestionnaire de groupe de travail, vous ne pourrez apporter des modifications qu'au répertoire local. Pour apporter des modifications au répertoire LDAP, vous devrez alors cliquer sur le cadenas et vous authentifier à l'aide du mot de passe de l'administrateur LDAP.

Avoir des mots de passe différents pour le compte d'administrateur local principal et pour le compte d'administrateur LDAP (identifiant d'utilisateur 501) peut prêter à confusion. C'est pourquoi il est recommandé de garder les mêmes mots de passe.

Remarque : un serveur Open Directory créé avec Mac OS X Server 10.4 possède des comptes d'administrateur différents pour son répertoire local et son répertoire LDAP. Ils sont dotés de noms et d'identifiants d'utilisateur différents, ce qui permet d'utiliser des mots de passe différents sans prêter à confusion.

Activation de l'authentification par liaison LDAP pour un utilisateur

Vous pouvez activer l'utilisation de l'authentification par liaison LDAP pour un compte d'utilisateur stocké dans un domaine de répertoire LDAP. Cette technique de validation de mot de passe se fie au serveur LDAP contenant le compte d'utilisateur pour authentifier le mot de passe de l'utilisateur.

Pour activer l'authentification des utilisateurs par liaison LDAP :

1 Assurez-vous que l'ordinateur Mac OS X qui doit authentifier le compte d'utilisateur dispose d'une connexion au répertoire LDAP dans lequel le compte d'utilisateur réside et que la politique de recherche de l'ordinateur contient la connexion du répertoire LDAP.

Consultez "Accès à des répertoires LDAP" à la page 130 pour obtenir plus d'informations sur la configuration de connexions au serveur LDAP et sur les politiques de recherche.

2 Si vous configurez une connexion LDAP qui ne mappe pas les attributs de Mot de passe et d'autorité d'authentification, l'authentification de liaison sera automatique.

Pour obtenir des instructions, consultez la section "Configuration des recherches et mappages LDAP" à la page 143.

3 Si la connexion est configurée pour autoriser les mots de passe en clair, elle doit aussi être configurée pour utiliser SSL de façon à protéger le mot de passe en clair pendant le transit.

Pour obtenir des instructions, consultez les sections "Modification de la politique de sécurité pour une connexion LDAP" à la page 142 et "Modification des réglages de connexion d'un répertoire LDAP" à la page 141.

Configuration de mots de passe d'utilisateurs exportés ou importés

Lorsque vous exportez des comptes d'utilisateur dont le type de mot de passe est Open Directory ou Mot de passe shadow, les mots de passe ne sont pas exportés. Cela protège la base de données du serveur de mots de passe Open Directory et les fichiers de mots de passe shadow. Avant l'importation, vous pouvez ouvrir le fichier des utilisateurs exportés dans un tableur et prédéfinir leurs mots de passe, qu'ils pourront modifier lors de leur prochaine ouverture de session. Le guide de gestion des utilisateurs contient des instructions sur l'utilisation de fichiers d'utilisateurs exportés.

Après l'importation, vous disposez de deux possibilités pour définir les mots de passe des comptes des utilisateurs importés :

- Vous pouvez affecter à tous les comptes d'utilisateur importés un mot de passe temporaire que chacun pourra changer lors de sa prochaine fois ouverture de session. Pour obtenir des instructions, consultez la section "Réinitialisation des mots de passe de plusieurs utilisateurs" à la page 105.
- Vous pouvez définir individuellement le mot de passe de chaque compte d'utilisateur importé dans la sous-fenêtre Élémentaire de Gestionnaire de groupe de travail. Pour obtenir des instructions, consultez la section "Modification du type de mot de passe d'un utilisateur" à la page 106.

Migration de mots de passe à partir de Mac OS X Server 10.1 ou antérieur

Il est possible de faire migrer les comptes d'utilisateur de versions antérieures de Mac OS X Server en important les enregistrements des comptes ou en mettant à jour le serveur où ils résident. Les comptes d'utilisateur créés avec Mac OS X Server 10.1 ou antérieur n'ont pas d'attribut d'autorité d'authentification mais possèdent des mots de passe cryptés. Pour conserver la compatibilité avec ces comptes d'utilisateur, Mac OS X Server considère qu'un compte d'utilisateur sans attribut d'autorité d'authentification possède un mot de passe crypté.

Si vous importez des comptes d'utilisateur de Mac OS X Server versions 10.1 ou antérieures, ces comptes ne possèdent pas d'attribut d'autorité d'authentification. Par conséquent, ils sont configurés initialement pour disposer de mots de passe cryptés. Si vous importez ces comptes d'utilisateur dans le domaine de répertoire local du serveur, qui est un domaine NetInfo, ils sont convertis automatiquement d'un mot de passe crypté en un mot de passe shadow lorsque l'utilisateur ou l'administrateur change le mot de passe, ou lorsque l'utilisateur s'authentifie pour un service qui peut utiliser une méthode d'authentification récupérable. Pour obtenir des informations sur l'importation de comptes d'utilisateur, consultez le guide de gestion des utilisateurs.

De même, si vous opérez une mise à jour à partir de Mac OS X Server version 10.1 ou antérieure, les comptes d'utilisateur créés avant la mise à jour ne possèdent pas d'attribut d'autorité d'authentification. Après leur mise à niveau, ces comptes sont supposés disposer de mots de passe cryptés.

Il est possible de continuer à utiliser tous les mots de passe cryptés existants après leur importation ou mise à niveau. Vous pouvez également modifier les comptes d'utilisateur pour qu'ils utilisent des mots de passe Open Directory ou des mots de passe shadow. Vous pouvez modifier des comptes d'utilisateur individuels ou plusieurs comptes d'utilisateur à l'aide de Gestionnaire de groupe de travail. La modification du type de mot de passe d'un compte d'utilisateur réinitialise son mot de passe. Pour plus de détails, voir "Choix du type de mot de passe Open Directory" à la page 107 et "Choix du type de mot de passe shadow" à la page 109.

Certains comptes d'utilisateur créés avec Mac OS X Server version 10.1 ou antérieure peuvent utiliser Gestionnaire d'authentification. Il s'agit d'une technologie héritée pour l'authentification des utilisateurs de service de fichiers Windows et Apple dont les ordinateurs Mac OS 8 n'ont pas été mis à niveau avec le logiciel client AFP version 3.8.3 ou ultérieure.

Lors de la migration d'utilisateurs Gestionnaire d'authentification, vous disposez des possibilités suivantes :

- Si vous mettez d'abord à niveau le serveur Mac OS X Server de la version 10.1 vers l a version 10.2, puis vers la version 10.4, les utilisateurs existants peuvent continuer à utiliser leurs mots de passe.
  - Vous pouvez changer tout ou partie des comptes d'utilisateur mis à niveau pour qu'ils utilisent des mots de passe Open Directory ou des mots de passe shadow, plus sûrs que les mots de passe cryptés. Pour plus d'informations, consultez la section "Exportation et importation d'utilisateurs Gestionnaire d'authentification" (ci-après).
  - Si le serveur mis à niveau dispose d'un domaine NetInfo partagé et si vous le migrez vers un répertoire LDAP, tous les comptes d'utilisateur sont automatiquement convertis en des mots de passe Open Directory. Pour plus de détails, consultez la rubrique "Migration d'un domaine de répertoire de NetInfo vers LDAP" à la page 99
  - Chaque compte d'utilisateur existant dans le domaine de répertoire local du serveur, qui est un domaine NetInfo, est converti automatiquement d'un mot de passe crypté en un mot de passe shadow lorsque l'utilisateur ou l'administrateur change le mot de passe ou lorsque l'utilisateur s'authentifie pour un service qui peut utiliser une méthode d'authentification récupérable.
- Si vous importez des comptes d'utilisateur qui utilisent le Gestionnaire d'authentification dans le répertoire LDAP, ils seront convertis pour l'utilisation de mots de passe Open Directory pendant l'importation.

Exportation et importation d'utilisateurs Gestionnaire d'authentification

Lorsque vous exportez des comptes d'utilisateur possédant des mots de passe cryptés à partir d'un domaine NetInfo pour lequel Gestionnaire d'authentification est activé, les mots de passe ne sont pas exportés. Après importation vers un domaine de répertoire de Mac OS X Server 10.4, vous avez deux possibilités pour définir les mots de passe des comptes d'utilisateur importés :

- Vous pouvez affecter à tous les comptes d'utilisateur importés un mot de passe temporaire que chacun pourra changer lors de sa prochaine fois ouverture de session. Pour obtenir des instructions, consultez la section "Réinitialisation des mots de passe de plusieurs utilisateurs" à la page 105.
- Vous pouvez définir individuellement le mot de passe de chaque compte d'utilisateur importé dans la sous-fenêtre Élémentaire de Gestionnaire de groupe de travail. Pour obtenir des instructions, consultez la section "Modification du type de mot de passe d'un utilisateur" à la page 106.

Le Gestionnaire d'authentification est une technologie héritée pour la validation sécurisée de mots de passe d'utilisateurs du service de fichiers Windows et d'utilisateurs du service de fichiers Apple dont les ordinateurs Mac OS 8 n'ont pas été mis à niveau avec le logiciel client AFP version 3.8.3 ou ultérieure. Le Gestionnaire d'authentification ne fonctionne qu'avec les comptes d'utilisateur qui ont été créés dans un domaine NetInfo de Mac OS X Server 10.0–10.2. Gestionnaire d'authentification doit avoir été activé pour le domaine NetInfo. Pour plus d'informations, consultez la section "Gestionnaire d'authentification" à la page 60.

Gestion de Format de répertoire 7

Vous pouvez utiliser Format de répertoire pour configurer et gérer la manière dont un ordinateur sous Mac OS X ou un serveur sous Mac OS X Server accède aux services de répertoire et détecte les services de réseau.

Pour les descriptions et les instructions sur les tâches de configuration et de gestion, reportez-vous à :

- "Configuration de Format de répertoire sur un serveur distant" (ci-après).
- "Configuration de l'accès à des services" à la page 122.
- "Configuration de politiques de recherche" à la page 126.
- "Accès à des répertoires LDAP" à la page 130.
- "Accès à un domaine Active Directory" à la page 154.
- "Accès à un domaine NIS" à la page 169.
- "Utilisation de fichiers de configuration BSD" à la page 169.
- "Accès aux domaines NetInfo hérités" à la page 171.

Configuration de Format de répertoire sur un serveur distant

Vous pouvez utiliser l'application Format de répertoire sur votre ordinateur pour configurer et gérer la manière dont Mac OS X Server sur un serveur distant accède aux services de répertoire et détecte les services de réseau.

Pour configurer l'accès à un répertoire sur un serveur distant :

1. Dans Format de répertoire, à partir de votre ordinateur, choisissez l'option Se connecter au menu Serveur.
2. Tapez les informations de connexion et d'authentification pour le serveur à configurer, puis cliquez sur Se connecter.

   Adresse : tapez le nom DNS ou l'adresse IP du serveur à configurer.

   Nom d'utilisateur : tapez le nom d'utilisateur d'un administrateur du serveur.

   Mot de passe : tapez le mot de passe correspondant au nom d'utilisateur que vous avez saisi.

3 Cliquez sur les onglets Services, Authentification et Contacts, puis apportez les modifications nécessaires aux réglages.

Toutes les modifications effectuées affectent le serveur distant auquel vous vous êtes connecté au cours des étapes précédentes.

4 Une fois la configuration du serveur distant terminée, choisissez Déconnecter dans le menu Serveur, sur votre ordinateur.

Configuration de l'accès à des services

Format de répertoire énumère les différentes catégories de services auxquelles Mac OS X peut accéder. La liste inclut les services de répertoires qui donnent à Mac OS X accès aux informations d'utilisateur et autres données administratives stockées dans les domaines de répertoire. La liste comporte également les types de services de réseau que Mac OS X est capable de détecter sur le réseau.

Vous pouvez activer ou désactiver l'accès à chaque type de service. Si vous désactivez un type de service dans Format de répertoire, Mac OS X ne peut plus accéder aux services de ce type. Cependant, la désactivation d'un type de service dans Format de répertoire n'affecte pas la capacité de Mac OS X à employer ou à fournir des services de ce type. Par exemple, si vous désactivez SMB/CIFS, Mac OS X ne l'utilise pas pour détecter les services de fichiers, mais vous pouvez toujours activer le partage Windows dans la sous-fenêtre Partage des Préférences Système et vous connecter à un serveur de fichiers Windows, si vous connaissez son adresse "smb://" .

Pour trouver les descriptions des tâches et des instructions, reportez-vous à :

- "Activation ou désactivation du service Active Directory" à la page 122.
- "Activation ou désactivation de la détection de services AppleTalk" à la page 123.
- "Activation ou désactivation de BSD fichier plat et des services de répertoires NIS" à la page 123.
- "Activation ou désactivation des services de répertoires LDAP" à la page 124.
- "Activation ou désactivation des services de répertoires NetInfo" à la page 124.
- "Activation de la détection de services Bonjour" à la page 125.
- "Activation ou désactivation de la détection de services SLP" à la page 125.
- "Activation ou désactivation de la détection de services SMB/CIFS" à la page 125.
- "Configuration de la détection de services SMB/CIFS" à la page 125.

Activation ou désactivation du service Active Directory

Format de répertoire permet d'activer ou de désactiver l'utilisation des services Active Directory fournis par un serveur Windows. Active Directory est le service de répertoire des serveurs Windows 2000 et 2003.

Si vous désactivez les services Active Directory et si tous les domaines Active Directory sont intégrés à une politique de recherche personnalisée, ils sont affichés en rouge dans la sous-fenêtre Authentification ou Contacts de Format de répertoire.

Pour activer ou désactiver l'accès à Active Directory :

1. Dans Format de répertoire, cliquez sur Services.
2. Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.
3. Cochez la case située en regard de Active Directory, puis cliquez sur Appliquer.

Pour obtenir des instructions sur la configuration, consultez la section "Accès à un domaine Active Directory" à la page 154.

Activation ou désactivation de la détection de services AppleTalk

Vous pouvez utiliser Format de répertoire pour activer ou désactiver la détection des services de réseau AppleTalk. AppleTalk est un protocole Mac OS hérité destiné aux services de réseau de fichiers et d'impression. Certains ordinateurs utilisent AppleTalk pour partager des fichiers et certains serveurs l'utilisent pour les services de fichiers. De plus, certaines imprimantes partagées exploitent également AppleTalk.

Pour activer ou désactiver la détection de services AppleTalk :

1. Dans Format de répertoire, cliquez sur Services.
2. Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.
3. Cochez la case située en regard de AppleTalk, puis cliquez sur Appliquer.

AppleTalk ne requiert aucune configuration.

Activation ou désactivation de BSD fichier plat et des services de répertoires NIS

Format de répertoire permet d'activer ou de désactiver l'utilisation de fichiers de configuration BSD et l'accès aux services de répertoires NIS (Network Information Service). Les fichiers de configuration BSD constituent la méthode d'origine pour accéder aux données administratives situées sur des ordinateurs UNIX. Certaines entreprises les utilisent encore. Certains serveurs UNIX utilisent NIS pour fournir des services de répertoires.

Si vous désactivez les services de répertoire BSD et NIS et si tous les domaines BSD et NIS sont intégrés à une politique de recherche personnalisée, ils sont affichés en rouge dans la sous-fenêtre Authentification ou Contacts de Format de répertoire.

Pour activer ou désactiver BSD fichier plat et les services de répertoires NIS :

1. Dans Format de répertoire, cliquez sur Services.
2. Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.
3. Cochez la case située en regard de "BSD fichier plat et NIS", puis cliquez sur Appliquer.

Pour obtenir des instructions sur la configuration, consultez la section "Accès à un domaine NIS" à la page 169 et "Utilisation de fichiers de configuration BSD" à la page 169.

Activation ou désactivation des services de répertoires LDAP

Vous pouvez utiliser Format de répertoire pour activer ou désactiver l'accès aux services de répertoires qui utilisent les versions 2 et 3 du protocole LDAP (Lightweight Directory Access Protocol). Un unique module externe Format de répertoire nommé LDAPv3 fournit l'accès aux deux versions de LDAP, la 2 et la 3.

Les services de répertoire fournis par Mac OS X Server utilisent LDAPv3, comme de nombreux autres serveurs. LDAPv3 est une norme ouverte commune dans les réseaux mixtes de systèmes Macintosh, UNIX et Windows. Certains serveurs utilisent la version antérieure, LDAPv2, pour fournir des services de répertoire.

Si vous désactivez les services de répertoire LDAP et si tous les répertoires LDAP sont intégrés à une politique de recherche personnalisée, ils sont affichés en rouge dans la sous-fenêtre Authentification ou Contacts de Format de répertoire.

Pour activer ou désactiver les services de répertoires LDAP :

1. Dans Format de répertoire, cliquez sur Services.
2. Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.
3. Cochez la case située en regard de LDAPv3, puis cliquez sur Appliquer.

Pour obtenir des instructions sur la configuration, consultez la section "Accès à des répertoires LDAP" à la page 130.

Activation ou désactivation des services de répertoires NetInfo

Vous pouvez utiliser Format de répertoire pour activer ou désactiver l'accès aux domaines de répertoire NetInfo partagés. NetInfo est un service de répertoire hérité encore utilisé pour le domaine de répertoire local sur tous les ordinateurs Mac OS X, y compris Mac OS X Server. NetInfo peut également être utilisé pour un domaine de répertoire partagé de Mac OS X Server versions 10.2 et antérieures.

La désactivation de NetInfo dans Format de répertoire ne désactive pas l'accès au domaine NetInfo local de l'ordinateur. Seul l'accès aux domaines NetInfo partagés peut être désactivé.

Si vous désactivez les services de répertoire NetInfo et si tous les domaines de répertoire NetInfo sont intégrés à une politique de recherche personnalisée, ils sont affichés en rouge dans la sous-fenêtre Authentification ou Contacts de Format de répertoire.

Pour activer ou désactiver les services de répertoire NetInfo :

1. Dans Format de répertoire, cliquez sur Services.
2. Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.
3. Cochez la case située en regard de NetInfo, puis cliquez sur Appliquer.

Pour obtenir des instructions sur la configuration, consultez la section “Accès aux domaines NetInfo hérités” à la page 171.

Activation de la détection de services Bonjour

La détection de services Bonjour est toujours activée. Vous ne pouvez pas désactiver l’utilisation de Bonjour pour la détection de services de réseau.

Activation ou désactivation de la détection de services SLP

Vous pouvez utiliser Format de répertoire pour activer ou désactiver la détection de services qui exploitent le protocole SLP (Service Location Protocol) pour se faire connaître sur le réseau. SLP est un standard ouvert pour la détection des services de fichiers et d’impression sur les réseaux IP (Internet Protocol).

Pour activer ou désactiver la détection de services SLP :

1. Dans Format de répertoire, cliquez sur Services.
2. Si l’icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d’un administrateur.
3. Cochez la case située en regard de SLP, puis cliquez sur Appliquer.

SLP ne nécessite aucune configuration.

Activation ou désactivation de la détection de services SMB/CIFS

Vous pouvez utiliser Format de répertoire pour activer ou désactiver la détection de services qui utilisent Server Message Block/Common Internet File System (SMB/CIFS) pour se faire connaître sur le réseau. SMB est un protocole utilisé par Microsoft Windows pour les services de fichiers et d’impression.

Pour activer ou désactiver la détection de services SMB/CIFS :

1. Dans Format de répertoire, cliquez sur Services.
2. Si l’icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d’un administrateur.
3. Cochez la case située en regard de SMB, puis cliquez sur Appliquer.

Pour obtenir des instructions sur la configuration, reportez-vous à “Configuration de la détection de services SMB/CIFS” (ci-après).

Configuration de la détection de services SMB/CIFS

Vous pouvez configurer la manière dont Mac OS X utilise le protocole Server Message Block (SMB/CIFS) pour détecter les serveurs de fichiers Windows sur le réseau. Vous pouvez utiliser l’application Format de répertoire pour spécifier les informations suivantes :

- Le groupe de travail Windows dont l’ordinateur est membre
- Un serveur Windows Internet Naming Service (WINS) sur le réseau

Pour configurer la détection de serveurs de fichiers Windows SMB/CIFS :

1. Dans Format de répertoire, cliquez sur Services.
2. Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.
3. Sélectionnez SMB dans la liste de services, puis cliquez sur Configurer.
4. Dans le champ Groupe de travail, tapez un nom de groupe de travail ou sélectionnez-en un dans la liste déroulante.

   La liste déroulante contient les noms des groupes de travail Windows dont font partie les autres ordinateurs du réseau.
5. Tapez le nom DNS ou l'adresse IP d'un serveur WINS qui fournit la résolution de noms NetBIOS pour le réseau, puis cliquez sur OK.

   Sur un réseau comportant des routeurs et plusieurs sous-réseaux, un serveur WINS permet de convertir les noms d'ordinateurs Windows en adresses IP.

   Si le réseau ne dispose pas d'un serveur WINS, laissez vide le champ Serveur WINS.

Configuration de politiques de recherche

Format de répertoire définit une politique de recherche pour l'authentification et une politique de recherche pour les informations de contact.

- *Authentification :* Mac OS X utilise la politique de recherche d'authentification pour localiser et récupérer, à partir des domaines de répertoire, les informations d'authentification d'utilisateur et d'autres données administratives.
- *Contacts :* Mac OS X utilise la politique de recherche de contacts pour localiser et récupérer, à partir des domaines de répertoire, les noms, adresses et autres informations de contact. Le Carnet d'adresses de Mac OS X utilise ces informations de contact. D'autres applications peuvent être programmées pour les exploiter.

Chaque politique de recherche se compose d'une liste de domaines de répertoire (également connus sous le nom de nœuds de répertoire). L'ordre des domaines de répertoire dans la liste définit la politique de recherche. En commençant en haut de la liste, Mac OS X examine tour à tour chaque domaine de répertoire listé, jusqu'à ce qu'il trouve les informations nécessaires ou qu'il atteigne la fin de la liste sans trouver ces informations.

Chaque politique de recherche (d'authentification et de contacts) peut être réglée sur Automatique, Répertoire local ou Chemin personnalisé.

- *Automatique* commence par le domaine de répertoire local et peut inclure un répertoire LDAP fourni automatiquement par DHCP et les domaines NetInfo auxquels l'ordinateur est lié. La politique de recherche automatique est la valeur par défaut pour Mac OS X versions 10.2 et ultérieures et offre la plus grande souplesse pour les ordinateurs nomades.

- *Répertoire local* n'inclut que le domaine de répertoire local.
- *Chemin personnalisé* commence par le domaine de répertoire local et inclut votre sélection de répertoires LDAP, un domaine Active Directory, les domaines NetInfo, les fichiers de configuration BSD et un domaine NIS.

Pour trouver les descriptions des tâches et des instructions, reportez-vous à :
- "Définition de politiques de recherche automatiques" (ci-après).
- "Définition de politiques de recherche personnalisées" à la page 128.
- "Définition de politiques de recherche de répertoire local" à la page 129.
- "Attente de l'entrée en vigueur d'une modification de la politique de recherche" à la page 129.

Définition de politiques de recherche automatiques

À l'aide de Format de répertoire, vous pouvez faire en sorte que les politiques de recherche d'authentification et de contacts d'un ordinateur Mac OS X soient créées automatiquement. Une politique de recherche définie automatiquement inclut le domaine de répertoire local. Elle peut aussi inclure un serveur de répertoires LDAP spécifié par service DHCP et des domaines NetInfo partagés auxquels l'ordinateur est lié. C'est la configuration par défaut tant pour la politique de recherche d'authentification que de contacts.

Remarque : certaines applications, comme Mail et Carnet d'adresses de Mac OS X, sont capables d'accéder directement aux répertoires LDAP, sans utiliser Open Directory. Pour configurer une de ces applications pour qu'elle accède directement aux répertoires LDAP, ouvrez l'application et réglez la préférence appropriée.

Important : si vous configurez Mac OS X pour qu'il utilise une politique de recherche automatique d'authentification et un serveur LDAP fourni par DHCP ou un domaine NetInfo fourni par DHCP, vous augmenterez le risque de voir un utilisateur malveillant prendre le contrôle de votre ordinateur. Le risque est encore plus élevé si votre ordinateur est configuré pour se connecter à réseau un sans fil. Pour plus de détails, consultez la section "Protection d'ordinateurs contre un serveur DHCP malveillant" à la page 130.

Pour obtenir qu'une politique de recherche soit automatiquement définie :

1. Dans Format de répertoire, cliquez sur Authentification ou sur Contacts.
   - *Authentification* montre la politique de recherche utilisée pour l'authentification et la plupart des autres données administratives.
   - *Contacts* montre la politique de recherche utilisée pour les informations de contact dans les applications comme Carnet d'adresses.
2. Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.
3. Dans le menu local Rechercher, choisissez Automatique, puis cliquez sur Appliquer.

4 Dans Préférences Système, assurez-vous que les préférences de réseau de l'ordinateur sont configurées pour utiliser DHCP ou DHCP via une adresse IP manuelle.

5 Pour intégrer un serveur LDAP dans la politique de recherche automatique, assurez-vous que l'utilisation d'un répertoire LDAP fourni par DHCP est activée dans Format de répertoire et que le service DHCP est configuré pour fournir l'adresse du serveur LDAP.

Pour obtenir des instructions, consultez la section "Activation ou désactivation d'un répertoire LDAP fourni via DHCP" à la page 131.

Pour obtenir des instructions sur la configuration du service DHCP de Mac OS X Server, reportez-vous au guide d'administration de services réseau.

6 Pour intégrer un domaine NetInfo partagé existant dans la politique de recherche automatique, assurez-vous que l'ordinateur est configuré pour se lier au domaine NetInfo.

Pour obtenir des instructions, consultez la section "Configuration d'une liaison NetInfo" à la page 172.

Définition de politiques de recherche personnalisées

À l'aide de Format de répertoire, vous pouvez obtenir que les politiques de recherche d'authentification et de contacts d'un ordinateur Mac OS X utilisent une liste personnalisée de domaines de répertoire. Une liste personnalisée commence par le domaine de répertoire local de l'ordinateur et vous pouvez aussi inclure des domaines de répertoire Open Directory et autres LDAP, un domaine Active Directory, des domaines NetInfo partagés, des fichiers de configuration BSD et un domaine NIS.

Si un domaine de répertoire spécifié dans la politique de recherche personnalisée d'un ordinateur n'est pas disponible, il y aura un délai lors du démarrage de l'ordinateur.

Pour spécifier une liste personnalisée de domaines de répertoire pour une politique de recherche :

1 Dans Format de répertoire, cliquez sur Authentification ou sur Contacts.

Authentification montre la politique de recherche utilisée pour l'authentification et la plupart des autres données administratives.

Contacts montre la politique de recherche utilisée pour les informations de contact dans les applications comme Carnet d'adresses.

2 Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.

3 Choisissez l'option Chemin personnalisé dans le menu local Rechercher.

4 Ajoutez si nécessaire des domaines de répertoire.

Ajoutez des domaines de répertoire en cliquant sur Ajouter, puis en sélectionnant un ou plusieurs répertoires et en cliquant de nouveau sur Ajouter.

5 Modifiez l'ordre des domaines de répertoire répertoriés comme requis, puis supprimez ceux que vous ne souhaitez pas inclure dans la politique de recherche.

Pour déplacer un domaine de répertoire, faites-le glisser vers le haut ou le bas de la liste.

Pour supprimer un domaine de répertoire répertorié, sélectionnez-le, puis cliquez sur Supprimer.

6 Cliquez sur Appliquer.

Si vous souhaitez ajouter un répertoire qui ne figure pas parmi les répertoires disponibles, assurez-vous que l'ordinateur a été configuré pour accéder au répertoire. Pour obtenir des instructions, consultez les sections suivantes :

- "Accès à des répertoires LDAP" à la page 130.
- "Accès à un domaine Active Directory" à la page 154.
- "Accès à un domaine NIS" à la page 169.
- "Utilisation de fichiers de configuration BSD" à la page 169.
- "Accès aux domaines NetInfo hérités" à la page 171.

Définition de politiques de recherche de répertoire local

À l'aide de Format de répertoire, vous pouvez obtenir que les politiques de recherche d'authentification et de contacts d'un ordinateur Mac OS X utilisent uniquement le domaine de répertoire local de l'ordinateur. Une politique de recherche qui n'utilise que le répertoire local limite l'accès d'un ordinateur aux informations d'authentification et autres données administratives. Si vous restreignez la politique de recherche d'authentification d'un ordinateur à l'emploi du répertoire local, seuls les utilisateurs possédant un compte local pourront ouvrir une session.

Pour qu'une politique de recherche n'utilise que le domaine de répertoire local :

1 Dans Format de répertoire, cliquez sur Authentification ou sur Contacts.

- *Authentification* montre la politique de recherche utilisée pour l'authentification et la plupart des autres données administratives.
- *Contacts* montre la politique de recherche utilisée pour les informations de contact dans les applications comme Carnet d'adresses.

2 Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.

3 Choisissez "Répertoire local" dans le menu local Rechercher, puis cliquez sur Appliquer.

Attente de l'entrée en vigueur d'une modification de la politique de recherche

Une fois que vous avez changé de politique de recherche dans la sous-fenêtre Authentification ou Contacts de Format de répertoire, vous devez attendre 10 ou 15 secondes avant que les modifications n'entrent en vigueur. Les tentatives de connexion à l'aide d'un compte provenant d'un domaine de répertoire dans la politique de recherche d'authentification échoueront jusqu'à ce que les modifications qui y ont été apportées entrent en vigueur.

Protection d'ordinateurs contre un serveur DHCP malveillant

Apple recommande de ne pas utiliser de politique de recherche d'authentification automatique avec un serveur LDAP fourni par DHCP et/ou un domaine NetInfo fourni par DHCP dans un environnement dans lequel la sécurité est un souci majeur. Un bidouilleur malveillant qui a accès à votre réseau peut utiliser un serveur DHCP leurre et un répertoire LDAP ou un domaine NetInfo leurre pour contrôler votre ordinateur en tant qu'utilisateur root.

D'abord, le serveur DHCP leurre du bidouilleur doit faire partie de votre réseau local, ou "sous-réseau". Donc, si vos ordinateurs sont les seuls sur votre réseau local et s'ils ont accès à Internet par le service NAT de Mac OS X Server ou par un routeur NAT, ce type de brèche dans la sécurité n'est pas possible. Toutefois, un réseau local sans fil augmente le risque en matière de sécurité car un bidouilleur peut accéder plus facilement à un réseau local sans fil qu'à un réseau local câblé.

Vous pouvez protéger votre Mac contre les attaques malveillantes à partir d'un serveur DHCP leurre en désactivant l'utilisation d'un répertoire LDAP fourni par DHCP et en désactivant la liaison Broadcast et DHCP pour NetInfo (ou en désactivant entièrement NetInfo). Pour obtenir des instructions, consultez les sections "Activation ou désactivation d'un répertoire LDAP fourni via DHCP" à la page 131, et "Configuration d'une liaison NetInfo" à la page 172.

Si vous disposez d'un ordinateur nomade qui se connecte à un serveur LDAP ou NetInfo lorsque l'ordinateur est connecté à un réseau et si vous changez la politique de recherche de l'ordinateur d'automatique à personnalisée (dans la sous-fenêtre Authentification de Format de répertoire), un délai se produira au démarrage lorsque l'ordinateur n'est pas connecté au réseau. Le délai se produit si l'ordinateur ne peut pas se connecter à un domaine de répertoire spécifique qui figure dans la politique de recherche personnalisée de l'ordinateur. Vous ne remarquerez aucun délai lorsque vous réveillerez un ordinateur qui a été déconnecté du réseau pendant la suspension d'activité.

Accès à des répertoires LDAP

Vous pouvez configurer un serveur équipé de Mac OS X Server ou un ordinateur doté de Mac OS X pour accéder à des répertoires LDAP particuliers, y compris le répertoire LDAP d'un maître Open Directory de Mac OS X Server. Pour trouver les descriptions des tâches et des instructions, reportez-vous à :

- "Accès à des répertoires LDAP dans Mail et Carnet d'adresses" à la page 131.
- "Activation ou désactivation d'un répertoire LDAP fourni via DHCP" à la page 131.
- "Affichage ou masquage de configurations pour serveurs LDAP" à la page 132.
- "Configuration de l'accès à un répertoire LDAP" à la page 133.
- "Configuration manuelle de l'accès à un répertoire LDAP" à la page 135.
- "Modification d'une configuration pour l'accès à un répertoire LDAP" à la page 137.

Accès à des répertoires LDAP dans Mail et Carnet d'adresses

Mac OS X Mail, Carnet d'adresses et d'autres applications similaires peuvent accéder à des répertoires LDAP directement, sans utiliser Open Directory. Vous pouvez configurer ces applications pour qu'elles effectuent des recherches dans des répertoires LDAP particuliers. Pour plus d'instructions, ouvrez Mail et choisissez Aide > Aide Mail ou ouvrez Carnet d'adresses et choisissez Aide > Aide de Carnet d'adresses ; puis cherchez de l'aide sur LDAP.

Activation ou désactivation d'un répertoire LDAP fourni via DHCP

Format de répertoire vous permet de configurer un ordinateur Mac OS X afin qu'il obtienne automatiquement l'adresse d'un serveur de répertoire LDAP au démarrage. Mac OS X requiert l'adresse d'un serveur de répertoire LDAP auprès du service DHCP qui fournit également l'adresse IP de l'ordinateur, l'adresse du routeur et les adresses de serveur DNS. Mac OS X ajoute l'adresse du serveur LDAP fournie via DHCP à la politique de recherche automatique de l'ordinateur. Le serveur LDAP fourni par DHCP apparaît aussi (estompé) dans la liste des configurations LDAP. Pour plus d'informations, consultez les sections "Définition de politiques de recherche automatiques" à la page 127 et "Modification d'une configuration pour l'accès à un répertoire LDAP" à la page 137.

L'ordinateur ne peut pas être configuré pour l'utilisation à la fois d'un répertoire LDAP fourni par DHCP et d'une liaison LDAP sécurisée. La liaison LDAP sécurisée est en réalité une liaison statique, alors que le LDAP fourni par DHCP est une liaison dynamique. Pour plus d'informations, consultez les sections "Configuration d'une liaison sécurisée vers un répertoire LDAP" à la page 146 et "Configuration d'une politique de liaison pour un maître Open Directory" à la page 96.

Important : si vous configurez Mac OS X pour qu'il utilise une politique de recherche automatique d'authentification et un serveur LDAP fourni par DHCP ou un domaine NetInfo fourni par DHCP, vous augmentez le risque de voir un utilisateur malveillant prendre le contrôle de votre ordinateur. Le risque est encore plus élevé si votre ordinateur est configuré pour se connecter à réseau un sans fil. Pour plus de détails, consultez la section "Protection d'ordinateurs contre un serveur DHCP malveillant" à la page 130.

Pour activer ou désactiver l'accès automatique à un serveur LDAP :

1. Dans Format de répertoire, cliquez sur Services.
2. Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.
3. Sélectionnez LDAPv3 dans la liste des services, puis cliquez sur Configurer.
4. Choisissez un emplacement sur le réseau dans le menu local Emplacement.

   L'option LDAP fournie par DHCP peut être activée ou désactivée indépendamment pour chaque emplacement de réseau qui est défini dans la sous-fenêtre Réseau de Préférences Système.
5. Cliquez sur "Ajouter les serveurs LDAP fournis par DHCP aux règles de recherche automatique".

   Si vous désactivez cette option, l'ordinateur n'utilise pas de serveur de répertoire LDAP fourni par DHCP. Il peut cependant accéder automatiquement à des domaines NetInfo partagés. Pour plus de détails, consultez la section "Accès aux domaines NetInfo hérités" à la page 171.

   Si vous activez ce réglage, le serveur qui fournit le service DHCP à cet ordinateur doit être configuré pour fournir l'adresse d'un serveur de répertoire LDAP. Pour obtenir des instructions, consultez le chapitre consacré à DHCP du guide d'administration de services réseau.

Affichage ou masquage de configurations pour serveurs LDAP

Vous pouvez afficher ou masquer la liste des configurations disponibles pour accéder aux répertoires LDAP. Chaque configuration spécifie la manière dont Open Directory accède à un répertoire LDAP particulier. Lorsque vous affichez la liste, vous pouvez voir et modifier certains réglages pour chaque configuration LDAP qui n'est pas estompée dans la liste. Les configurations LDAP estompées sont fournies par DHCP, comme décrit dans la section "Activation ou désactivation d'un répertoire LDAP fourni via DHCP" à la page 131.

Pour afficher ou masquer les configurations de répertoire LDAP disponibles :

1. Dans Format de répertoire, cliquez sur Services.
2. Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.
3. Sélectionnez LDAPv3 dans la liste des services, puis cliquez sur Configurer.
4. En fonction du contexte, cliquez sur Afficher les options ou sur Masquer les options.

Configuration de l'accès à un répertoire LDAP

Format de répertoire peut vous aider à créer une configuration qui spécifie comment Mac OS X accède à un répertoire LDAPv3 particulier. Vous devez connaître le nom DNS ou l'adresse IP du serveur de répertoire LDAP. De plus, si le répertoire n'est pas hébergé par un serveur qui fournit ses propres mappages, comme, par exemple, Mac OS X Server, vous devez connaître la base de recherche et le modèle pour le mappage de données Mac OS X aux données du répertoire. Les modèles de mappage pris en charge sont les suivants :

- Serveur Open Directory — pour un répertoire qui utilise le schéma de Mac OS X Server
- Active Directory — pour un répertoire hébergé par un serveur Windows 2000 ou 2003
- RFC 2307 — pour la plupart des répertoires hébergés par les serveurs UNIX

Le module externe LDAPv3 prend entièrement en charge la réplication et le basculement Open Directory. Si le maître Open Directory devient indisponible, le module externe bascule automatiquement sur une réplique proche.

Si vous devez spécifier des mappages personnalisés pour les données du répertoire, suivez les instructions de la section "Configuration manuelle de l'accès à un répertoire LDAP" (ci-après) plutôt que les instructions ci-dessous.

Pour que Format de répertoire vous aide à configurer l'accès à un répertoire LDAP :

1. Dans Format de répertoire, cliquez sur Services.
2. Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.
3. Sélectionnez LDAPv3 dans la liste des services, puis cliquez sur Configurer.

   Vous pouvez sélectionner LDAPv3 dans la liste des services sans cocher la case Activer pour LDAPv3.
4. Cliquez sur Nouveau, puis tapez le nom DNS ou l'adresse IP du serveur LDAP.
5. Sélectionnez les options pour l'accès au répertoire, puis cliquez sur Continuer pour que Format de répertoire obtienne les informations du serveur LDAP.
   - Cochez la case "Crypter via SSL" si vous souhaitez qu'Open Directory utilise Secure Sockets Layer (SSL) pour les connexions avec le répertoire LDAP.

- Cochez la case “Utiliser pour l’authentification” si ce répertoire contient des comptes d’utilisateur que quelqu’un va utiliser pour la connexion ou pour l’authentification à des services.
- Cochez la case “Utiliser pour les contacts” si ce répertoire contient des adresses électroniques et d’autres informations que vous souhaitez utiliser dans Carnet d’adresses.

Si Format de répertoire ne peut pas contacter le serveur LDAP, il affiche un message et vous devez alors configurer l’accès manuellement ou annuler le processus de configuration. Pour obtenir des instructions sur la configuration manuelle, consultez la section “Configuration manuelle de l’accès à un répertoire LDAP” (ci-après).

6 Si la zone de dialogue se développe pour afficher des options de mappage, choisissez le modèle de mappage dans le menu local, tapez le suffixe de la base de recherche, puis cliquez sur Continuer.

Le suffixe de la base de recherche provient généralement du nom DNS du serveur. Par exemple, le suffixe de la base de recherche pourrait être “dc=ods, dc=exemple, dc=com” pour un serveur dont le nom DNS est ods.exemple.com.

Si aucun des modèles de mappage disponibles ne s’applique à la connexion que vous êtes en train de configurer, cliquez sur Manuel et consultez la section “Configuration manuelle de l’accès à un répertoire LDAP” (ci-après) pour des instructions supplémentaires.

7 Si la zone de dialogue se développe pour afficher des options relatives à la liaison sécurisée, tapez le nom de l’ordinateur ainsi que le nom d’utilisateur et le mot de passe d’un administrateur de répertoire (il se peut que la liaison soit facultative).

- La zone de dialogue vous indique si le répertoire LDAP requiert la liaison sécurisée ou la rend facultative. La liaison sécurisée est mutuelle : chaque fois que l’ordinateur se connecte au répertoire LDAP, ils s’authentifient l’un et l’autre.
- Si la liaison sécurisée est déjà configurée ou si le répertoire LDAP ne prend pas en charge la liaison sécurisée, le bouton Relier n’est pas affiché.
- Si vous voyez apparaître un avertissement disant qu’il existe une fiche d’ordinateur, vous pouvez cliquer sur Écraser pour remplacer la fiche d’ordinateur.
  Avant de remplacer une fiche d’ordinateur existante, assurez-vous que vous avez bien fourni le bon nom d’ordinateur. Cliquez sur Annuler pour revenir sur vos pas et changer le nom de l’ordinateur.

  La fiche d’ordinateur existante peut être abandonnée ou appartenir à un autre ordinateur. Si vous décidez de remplacer une fiche d’ordinateur, prévenez l’administrateur du répertoire LDAP, au cas où le remplacement de la fiche désactiverait un autre ordinateur. Dans ce cas, l’administrateur du répertoire LDAP doit ajouter à nouveau l’ordinateur désactivé dans la liste des ordinateurs à laquelle il appartenait en utilisant un autre nom pour cet ordinateur. Pour obtenir des instructions sur l’ajout d’un ordinateur à une liste d’ordinateurs, consultez le chapitre consacré aux listes d’ordinateurs du guide de gestion des utilisateurs.

8 Si la zone de dialogue se développe pour afficher des options relatives à la connexion, sélectionnez l'option "Utiliser l'authentification lors de la sélection" puis tapez le nom distinctif et le mot de passe d'un compte d'utilisateur du répertoire.

Les options pour une connexion authentifiée apparaissent si le serveur LDAP prend en charge une connexion authentifiée, mais pas la liaison sécurisée. La connexion authentifiée n'est pas mutuelle : le serveur LDAP authentifie le client, mais le client n'authentifie pas le serveur.

L'option "Utiliser l'authentification lors de la sélection" est présélectionnée, mais estompée si le serveur LDAP requiert que vous fournissiez le nom distinctif et le mot de passe d'un compte d'utilisateur pour une connexion authentifiée.

Le nom distinctif peut spécifier tout compte d'utilisateur qui a l'autorisation de voir les données dans le répertoire. Par exemple, un compte d'utilisateur dont le nom abrégé est "dirauth" sur un serveur LDAP dont l'adresse est ods.exemple.com porterait le nom distinctif uid=dirauth,cn=utilisateurs,dc=ods,dc=exemple,dc=com.

Important : si le nom distinctif ou le mot de passe est incorrecte personne ne pourra se connecter à l'ordinateur à l'aide de comptes d'utilisateur provenant du répertoire LDAP.

9 Cliquez sur OK pour clôturer la création de la nouvelle connexion LDAP, puis sur OK pour clôturer la configuration des options LDAPv3.

Si vous avez sélectionné l'option "Utiliser pour l'authentification" ou l'option "Utiliser pour les contacts" à l'étape 5, la configuration de répertoire LDAP que vous venez de créer est ajoutée automatiquement à une politique de recherche personnalisée dans la sous-fenêtre Authentification ou Contacts de Format de répertoire.

Vous devez vous assurer que LDAPv3 est activé dans la sous-fenêtre Services afin que l'ordinateur utilise la configuration LDAP que vous venez de créer. Pour obtenir des instructions, consultez la section "Activation ou désactivation des services de répertoires LDAP" à la page 124.

Configuration manuelle de l'accès à un répertoire LDAP

Vous pouvez créer manuellement une configuration qui spécifie comment Mac OS X accède à un répertoire LDAPv3 ou LDAPv2 particulier. Vous devez connaître le nom DNS ou l'adresse IP du serveur de répertoire LDAP. De plus, si le répertoire n'est pas hébergé par un serveur sous Mac OS X Server, vous devez connaître la base de recherche et le modèle pour le mappage de données Mac OS X vers les données du répertoire. Les modèles de mappage pris en charge sont :

- À partir du serveur — pour un répertoire qui fournit ses propres mappages et sa propre base de recherche, comme par exemple Mac OS X Server
- Serveur Open Directory — pour un répertoire qui utilise la schéma de Mac OS X Server
- Active Directory — pour un répertoire hébergé par un serveur Windows 2000 ou 2003
- RFC 2307 — pour la plupart des répertoires hébergés par des serveurs UNIX
- Personnalisé — pour les répertoires qui n'utilisent aucun des mappages cités plus haut

Le module externe LDAPv3 prend entièrement en charge la réplication et le basculement Open Directory. Si le maître Open Directory devient indisponible, le module externe bascule automatiquement sur une réplique proche.

Pour configurer manuellement l'accès à un répertoire LDAP :

1. Dans Format de répertoire, cliquez sur Services.
2. Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.
3. Sélectionnez LDAPv3 dans la liste des services, puis cliquez sur Configurer.

   Vous pouvez sélectionner LDAPv3 dans la liste des services sans cocher la case Activer pour LDAPv3.
4. Cliquez sur Nouveau, puis sur Manuel.
5. Tapez un nom pour la configuration.
6. Appuyez sur la touche Tabulation, puis tapez le nom DNS ou l'adresse IP du serveur qui héberge le répertoire LDAP auquel vous voulez accéder.
7. Cliquez sur le menu local en regard du nom DNS ou de l'adresse IP et choisissez un modèle ou une méthode de mappage :
   - *Si vous choisissez Serveur*, il n'est pas nécessaire de saisir un suffixe de la base de recherche. Dans ce cas, Open Directory assume que le suffixe de la base de recherche est le premier niveau du répertoire LDAP.
   - *Si vous choisissez un modèle*, saisissez le suffixe de la base de recherche pour le répertoire LDAP, puis cliquez sur OK. Vous devez saisir un suffixe de base de recherche, sinon l'ordinateur ne pourra pas trouver d'informations dans le répertoire LDAP. Le suffixe de la base de recherche provient généralement du nom DNS du serveur. Par exemple, le suffixe de la base de recherche pourrait être "dc=ods, dc=exemple, dc=com" pour un serveur dont le nom DNS est ods.exemple.com.
   - *Si vous choisissez Personnalisé*, vous devez configurer des mappages entre les types de fiches et les attributs Mac OS X et entre les classes et les attributs du répertoire LDAP auquel vous vous connectez. Pour obtenir des instructions, consultez la section "Configuration des recherches et mappages LDAP" à la page 143.
8. Pour qu'Open Directory utilise SSL (Secure Sockets Layer) pour les connexions avec le répertoire LDAP, cochez la case SSL.
9. Si vous souhaitez modifier les réglages de la liaison sécurisée, des options de connexion ou la politique de sécurité de cette configuration LDAP, cliquez sur Modifier pour afficher les options de la configuration LDAP sélectionnée, puis sur OK une fois que vous avez fini de modifier les options de la configuration LDAP.
   - Cliquez sur Relier pour configurer la liaison sécurisée (si le répertoire LDAP la prend en charge). Pour obtenir des instructions détaillées, consultez la section "Configuration d'une liaison sécurisée vers un répertoire LDAP" à la page 146.

- Cliquez sur Connexion pour définir des options de délai, spécifier un port personnalisé, ignorer des références de serveur ou forcer l'utilisation du protocole LDAPv2 (lecture seule). Pour obtenir des instructions détaillées, consultez la section "Modification des réglages de connexion d'un répertoire LDAP" à la page 141.
- Cliquez sur Sécurité pour configurer des options de connexion authentifiée (plutôt que de liaison sécurisée) et d'autres options de politique de sécurité. Pour obtenir des instructions détaillées, consultez la section "Modification de la politique de sécurité pour une connexion LDAP" à la page 142.

10 Cliquez sur OK pour clôturer manuellement la création de la configuration d'accès au répertoire LDAP.

11 Pour que l'ordinateur accède au répertoire LDAP pour lequel vous venez de créer une configuration, vous devez ajouter le répertoire à une politique de recherche personnalisée dans la sous-fenêtre Authentification ou Contacts de Format de répertoire. Vous devez également vous assurer que LDAPv3 est activé dans la sous-fenêtre Services.

Pour plus de détails, consultez les sections "Activation ou désactivation des services de répertoires LDAP" à la page 124 et "Définition de politiques de recherche personnalisées" à la page 128.

Remarque : pour pouvoir utiliser Gestionnaire de groupe de travail pour créer des utilisateurs sur un serveur LDAP non-Apple qui utilise des mappages RFC 2307 (UNIX), vous devez modifiez le mappage du type de fiche Utilisateurs. Pour obtenir des instructions, consultez la section "Modification du mappage RFC 2307 pour activer la création d'utilisateurs" à la page 152.

Modification d'une configuration pour l'accès à un répertoire LDAP

Vous pouvez utiliser Format de répertoire pour modifier les réglages d'une configuration de répertoire LDAP. Les paramètres de configuration spécifient la manière dont Open Directory accède à un répertoire LDAPv3 ou LDAPv2 particulier. Vous ne pouvez pas modifier une configuration LDAP fournie par DHCP. D'ailleurs, une telle configuration apparaît estompée dans la liste des configurations LDAP.

Pour modifier une configuration d'accès à un répertoire LDAP :

1 Dans Format de répertoire, cliquez sur Services.

2 Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.

3 Sélectionnez LDAPv3 dans la liste des services, puis cliquez sur Configurer.

4 Si la liste des configurations de serveur est masquée, cliquez sur Afficher les options.

5 Modifiez l'un des réglages figurant dans la liste des configurations de serveur.

- *Activer :* cochez une case pour activer ou désactiver l'accès à un serveur de répertoire LDAP.

- *Nom de la configuration :* double-cliquez sur un nom de configuration pour le modifier.
- *Nom du serveur ou adresse IP :* double-cliquez sur un nom de serveur ou une adresse IP pour le modifier.
- *Mappage LDAP :* choisissez un modèle dans le menu local, puis saisissez le suffixe de la base de recherche pour le répertoire LDAP et cliquez sur OK.
  Si vous avez choisi un modèle, vous devez saisir un suffixe de base de recherche, sinon l'ordinateur ne pourra pas trouver d'informations dans le répertoire LDAP.
  Le suffixe de la base de recherche provient généralement du nom DNS du serveur. Par exemple, le suffixe de la base de recherche pourrait être "dc=ods, dc=exemple, dc=com" pour un serveur dont le nom DNS est ods.exemple.com.

  Si vous avez sélectionné À partir du serveur au lieu d'un modèle, vous n'avez pas besoin de saisir de suffixe de base de recherche. Dans ce cas, Open Directory assume que le suffixe de base de recherche est le premier niveau du répertoire LDAP.

  Si vous choisissez Personnalisé, vous devez maintenant configurer des mappages entre les types de fiches et les attributs Mac OS X et les classes et les attributs du répertoire LDAP auquel vous vous connectez. Pour obtenir des instructions, consultez la section "Configuration des recherches et mappages LDAP" à la page 143.
- *SSL :* cochez une case pour activer ou désactiver les communications cryptées à l'aide du protocole Secure Sockets Layer (SSL).

6 Si vous souhaitez modifier les réglages par défaut de la liaison sécurisée, des options de connexion ou la politique de sécurité de cette configuration LDAP, cliquez sur Modifier pour afficher les options de la configuration LDAP sélectionnée, puis sur OK une fois que vous avez fini de modifier les options de la configuration LDAP.

- Cliquez sur le bouton Relier pour configurer la liaison sécurisée ou sur le bouton Rompre la liaison pour arrêter la liaison sécurisée. (Il se peut que vous ne voyiez pas ces boutons si le répertoire LDAP n'autorise pas la liaison sécurisée). Pour obtenir des instructions détaillées, consultez la section "Configuration d'une liaison sécurisée vers un répertoire LDAP" à la page 146.
- Cliquez sur Connexion pour définir des options de délai, spécifier un port personnalisé, ignorer des références de serveur ou forcer l'utilisation du protocole LDAPv2 (lecture seule). Pour obtenir des instructions détaillées, consultez la section "Modification des réglages de connexion d'un répertoire LDAP" à la page 141.
- Cliquez sur Sécurité pour configurer une connexion authentifiée (plutôt qu'une liaison sécurisée) et d'autres options de politique de sécurité. Pour obtenir des instructions détaillées, consultez la section "Modification de la politique de sécurité pour une connexion LDAP" à la page 142.

7 Cliquez sur OK pour clôturer la modification de la configuration d'accès à un répertoire LDAP.

Duplication d'une configuration pour l'accès à un répertoire LDAP

Vous pouvez utiliser Format de répertoire pour dupliquer une configuration qui spécifie comment Mac OS X accède à un répertoire LDAPv3 ou LDAPv2 particulier. Après avoir dupliqué une configuration de répertoire LDAP, vous pouvez en modifier les réglages pour la différencier de la configuration d'origine.

Pour dupliquer une configuration d'accès à un répertoire LDAP :

1. Dans Format de répertoire, cliquez sur Services.
2. Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.
3. Sélectionnez LDAPv3 dans la liste des services, puis cliquez sur Configurer.
4. Si la liste des configurations de serveur est masquée, cliquez sur Afficher les options.
5. Sélectionnez une configuration de serveur dans la liste, puis cliquez sur Dupliquer.
6. Modifiez l'un des réglages de configuration du double de la configuration.
   - *Activer :* cochez une case pour activer ou désactiver l'accès à un serveur de répertoire LDAP.
   - *Nom de la configuration :* double-cliquez sur un nom de configuration pour le modifier.
   - *Nom du serveur ou adresse IP :* double-cliquez sur un nom de serveur ou une adresse IP pour le modifier.
   - *Mappage LDAP :* choisissez un modèle dans le menu local, puis saisissez le suffixe de la base de recherche pour le répertoire LDAP et cliquez sur OK.
     Si vous avez choisi un modèle, vous devez saisir un suffixe de base de recherche, sinon l'ordinateur ne pourra pas trouver d'informations dans le répertoire LDAP.
     Le suffixe de la base de recherche provient généralement du nom DNS du serveur. Par exemple, le suffixe de la base de recherche pourrait être "dc=ods, dc=exemple, dc=com" pour un serveur dont le nom DNS est ods.exemple.com.

     Si vous avez sélectionné À partir du serveur au lieu d'un modèle, vous n'avez pas besoin de saisir de suffixe de base de recherche. Dans ce cas, Open Directory assume que le suffixe de base de recherche est le premier niveau du répertoire LDAP.

     Si vous choisissez Personnalisé, vous devez maintenant configurer des mappages entre les types de fiches et les attributs Mac OS X et les classes et les attributs du répertoire LDAP auquel vous vous connectez. Pour obtenir des instructions, consultez la section "Configuration des recherches et mappages LDAP" à la page 143.
   - *SSL :* cochez une case pour activer ou désactiver les connexions SSL (Secure Sockets Layer).
7. Si vous souhaitez modifier les réglages par défaut de la liaison sécurisée, des options de connexion ou la politique de sécurité de la configuration LDAP dupliquée, cliquez sur Modifier pour afficher les options, puis sur OK une fois que vous avez fini de les modifier.

- Cliquez sur le bouton Relier pour configurer la liaison sécurisée ou sur le bouton Rompre la liaison pour arrêter la liaison sécurisée. (Il se peut que vous ne voyiez pas ces boutons si le répertoire LDAP n'autorise pas la liaison sécurisée). Pour obtenir des instructions détaillées, consultez la section "Configuration d'une liaison sécurisée vers un répertoire LDAP" à la page 146.
- Cliquez sur Connexion pour configurer la liaison sécurisée (si le répertoire LDAP la prend en charge), définir des options de délai, spécifier un port personnalisé, ignorer des références de serveur ou forcer l'utilisation du protocole LDAPv2 (lecture seule). Pour obtenir des instructions détaillées, consultez la section "Modification des réglages de connexion d'un répertoire LDAP" à la page 141.
- Cliquez sur Sécurité pour configurer une connexion authentifiée (plutôt qu'une liaison sécurisée) et d'autres options de politique de sécurité. Pour obtenir des instructions détaillées, consultez la section "Modification de la politique de sécurité pour une connexion LDAP" à la page 142.

8 Cliquez sur OK pour clôturer la modification de la configuration dupliquée.

9 Pour que l'ordinateur accède au répertoire LDAP spécifié par la copie de configuration que vous venez de créer, vous devez ajouter le répertoire à une politique de recherche personnalisée dans la sous-fenêtre Authentification ou Contacts de Format de répertoire. Vous devez également vous assurer que LDAPv3 est activé dans la sous-fenêtre Services.

Pour obtenir des instructions, consultez les sections "Activation ou désactivation des services de répertoires LDAP" à la page 124 et "Définition de politiques de recherche personnalisées" à la page 128.

Suppression d'une configuration pour l'accès à un répertoire LDAP

Vous pouvez utiliser Format de répertoire pour supprimer une configuration qui spécifie la manière dont l'ordinateur accède à un répertoire LDAPv3 ou LDAPv2 particulier. Vous ne pouvez pas supprimer une configuration LDAP fournie par DHCP. D'ailleurs, une telle configuration apparaît estompée dans la liste des configurations LDAP.

Pour supprimer une configuration d'accès à un répertoire LDAP :

1 Dans Format de répertoire, cliquez sur Services.

2 Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.

3 Sélectionnez LDAPv3 dans la liste des services, puis cliquez sur Configurer.

4 Si la liste des configurations de serveur est masquée, cliquez sur Afficher les options.

5 Sélectionnez une configuration de serveur dans la liste, puis cliquez sur Supprimer.

6 Si vous voyez apparaître un avertissement disant que l'ordinateur est lié au répertoire LDAP et si vous souhaitez arrêter la liaison sécurisée : cliquez sur OK, puis saisissez les références demandées.

- Saisissez le nom et le mot de passe d'un administrateur de répertoire LDAP (pas un administrateur de l'ordinateur local).

- Si vous voyez apparaître un avertissement disant que l'ordinateur ne peut pas contacter le serveur LDAP, vous pouvez cliquer sur OK pour forcer l'arrêt de la liaison sécurisée.
  Si vous forcez l'arrêt de la liaison sécurisée, cet ordinateur disposera toujours d'une fiche d'ordinateur dans le répertoire LDAP. Prévenez l'administrateur du répertoire LDAP pour qu'il supprime l'ordinateur de sa liste d'ordinateurs. Pour obtenir des instructions sur la suppression d'un ordinateur de sa liste d'ordinateurs, consultez le chapitre consacré aux listes d'ordinateurs du guide de gestion des utilisateurs.

La configuration supprimée est effacée automatiquement des politiques de recherche personnalisées pour l'authentification et les contacts.

Modification des réglages de connexion d'un répertoire LDAP

Vous pouvez utiliser Format de répertoire pour modifier les réglages de connexion d'une configuration qui spécifie la manière dont l'ordinateur accède à un répertoire LDAPv3 ou LDAPv2 particulier.

Pour modifier les réglages de connexion pour l'accès à un répertoire LDAP :

1. Dans Format de répertoire, cliquez sur Services.
2. Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.
3. Sélectionnez LDAPv3 dans la liste des services, puis cliquez sur Configurer.
4. Si la liste des configurations de serveur est masquée, cliquez sur Afficher les options.
5. Sélectionnez une configuration de serveur dans la liste, puis cliquez sur Modifier.
6. Cliquez sur Connexion, puis modifiez les réglages souhaités.
   - *Nom de la configuration* identifie cette configuration dans la liste des configurations de répertoire LDAP. (Vous pouvez également modifier le nom directement dans la liste des configurations de répertoire LDAP.)
   - *Nom du serveur ou adresse IP* spécifie le nom DNS ou l'adresse IP du serveur. (Vous pouvez également modifier directement ces éléments dans la liste des configurations de répertoire LDAP.)
   - *"L'ouverture/fermeture expire après"* spécifie le nombre de secondes avant l'annulation d'une tentative de connexion au serveur LDAP.
   - *"La requête expire après"* spécifie le nombre de secondes avant l'annulation d'une requête envoyée au répertoire LDAP.
   - *"Nouvelle tentative de liaison après"* spécifie le nombre de secondes avant une nouvelle tentative de connexion au cas où le serveur LDAP ne répondrait pas. Vous pouvez augmenter cette valeur pour éviter des tentatives de reconnexion continues.
   - *"La connexion expirera après"* spécifie le nombre de secondes nécessaires pour permettre à une connexion inactive ou sans réponse de demeurer ouverte.
   - *"Crypter via SSL"* détermine si SSL (Secure Sockets Layer) doit être utilisé pour crypter les communications avec le répertoire LDAP. (Vous pouvez également modifier ce paramètre directement dans la liste des configurations de répertoire LDAP.)

- *"Utiliser le port personnalisé"* spécifie un numéro de port autre que celui du port par défaut pour les connexions LDAP (389 sans SSL ou 636 avec SSL).
- *"Ignorer les références du serveur"* détermine s'il faut ignorer ou suivre les références d'un serveur LDAP pour rechercher des informations sur d'autres serveurs LDAP ou répliques. Les références de serveur peuvent aider un ordinateur à trouver des informations, mais peuvent aussi retarder la connexion ou provoquer d'autres délais si l'ordinateur finit par rechercher des références sur de nombreux serveurs LDAP.
- *"Utiliser LDAPv2 (lecture seule)"* détermine s'il faut utiliser l'ancien protocole LDAPv2 pour l'accès en lecture seule à un répertoire LDAP.

Modification de la politique de sécurité pour une connexion LDAP

Format de répertoire vous permet de configurer une politique de sécurité pour ne connexion LDAPv3 plus stricte que la politique de sécurité du répertoire LDAP. Par exemple, si la politique de sécurité du répertoire LDAP autorise les mots de passe en clair, vous pouvez configurer une connexion LDAPv3 pour qu'elle n'autorise pas les mots de passe en clair.

Définir une politique de sécurité plus stricte protège votre ordinateur contre les tentatives des bidouilleurs d'utiliser un serveur LDAP piraté pour prendre le contrôle de votre ordinateur.

L'ordinateur doit communiquer avec le serveur LDAP pour montrer de façon précise l'état des options de sécurité. C'est pourquoi, lorsque vous modifiez des options de sécurité pour une connexion LDAPv3, la politique de recherche d'authentification de l'ordinateur doit inclure la connexion LDAPv3.

Les réglages autorisés pour les options de sécurité d'une connexion LDAPv3 dépendent des possibilités et des besoins en matière de sécurité du serveur LDAP. Par exemple, si le serveur LDAP ne prend pas en charge l'authentification Kerberos, plusieurs options de sécurité de la connexion LDAPv3 sont désactivées.

Pour modifier des options de sécurité d'une connexion LDAPv3 :

1. Dans Format de répertoire, cliquez sur Authentification et assurez-vous que le répertoire LDAPv3 souhaité figure bien dans la politique de recherche.

   Pour obtenir des instructions sur l'ajout d'un répertoire LDAPv3 à une politique de recherche d'authentification, consultez la section "Définition de politiques de recherche personnalisées" à la page 128.
2. Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.
3. Cliquez sur Services, sélectionnez LDAPv3 dans la liste des services, puis cliquez sur Configurer.
4. Si la liste des configurations de serveur est masquée, cliquez sur Afficher les options.
5. Sélectionnez la configuration de répertoire souhaitée, puis cliquez sur Modifier.

6 Cliquez sur Sécurité, puis modifiez les réglages souhaités.

Si une des quatre dernières options est sélectionnée mais désactivée, le répertoire LDAP la requiert. Si une de ces options est désélectionnée et désactivée, le serveur LDAP ne la prend pas en charge. Pour obtenir des instructions sur la définition de ces options pour un répertoire LDAP Mac OS X Server, consultez la section "Configuration d'une politique de sécurité pour un maître et des répliques Open Directory" à la page 97.

- *"Utiliser l'authentification lors de la connexion"* détermine si la connexion LDAPv3 s'authentifie auprès du répertoire LDAP en fournissant le nom distinctif et le mot de passe. Cette option n'apparaît pas si la connexion LDAPv3 utilise la liaison sécurisée avec le répertoire LDAP.
- *"Relié au répertoire en tant que"* spécifie les références que la connexion LDAPv3 utilise pour la liaison sécurisée avec le répertoire LDAP. Vous ne pouvez pas changer cette option ni les références ici. Par contre, vous pouvez rompre le lien, puis l'établir à nouveau avec d'autres références. Pour obtenir des instructions, consultez les sections "Arrêt d'une liaison sécurisée avec un répertoire LDAP" à la page 147 et "Configuration d'une liaison sécurisée vers un répertoire LDAP" à la page 146. Cette option n'est affichée que si la connexion LDAPv3 utilise la liaison sécurisée.
- *"Désactiver les mots de passe en clair"* détermine si le mot de passe doit être envoyé sous la forme de texte en clair si le mot de passe ne peut être validé à l'aide d'aucune méthode d'authentification qui envoie les mots de passe cryptés. Pour plus d'informations, consultez les sections "Sélection de méthodes d'authentification pour des utilisateurs de mots de passe shadow" à la page 113 et "Sélection de méthodes d'authentification pour des utilisateurs de mots de passe Open Directory" à la page 114.
- *"Signer tous les paquets numériquement (requiert Kerberos)"* permet de s'assurer que les données de répertoire provenant du serveur LDAP ne sont pas interceptées et modifiées par un autre ordinateur pendant qu'elles transitent vers votre ordinateur.
- *"Crypter tous les paquets (requiert SSL ou Kerberos)"* force le serveur LDAP à crypter les données de répertoire à l'aide de SSL ou de Kerberos avant de les envoyer à votre ordinateur.
- *"Bloquer les attaques "Man-in-the-Middle" (requiert Kerberos)"* empêche un éventuel serveur malveillant de se faire passer pour la serveur LDAP. Le plus efficace avec l'option "Signer tous les paquets numériquement".

Configuration des recherches et mappages LDAP

Format de répertoire vous permet de modifier les mappages, les bases de recherche et les étendues de recherche qui spécifient comment Mac OS X trouve des données particulières dans un répertoire LDAP. Vous pouvez modifier ces réglages séparément pour chaque configuration de répertoire LDAP listée dans Format de répertoire. Chaque configuration de répertoire LDAP spécifie la manière dont Mac OS X accède aux données dans un répertoire LDAPv3 ou LDAPv2.

- Vous pouvez modifier le mappage de chaque type de fiche Mac OS X vers une ou plusieurs classes d'objets LDAP.

- Pour chaque type de fiche, vous pouvez aussi modifier le mappage des types de données (ou attributs) Mac OS X à des attributs LDAP.
- Vous pouvez modifier la base de recherche et l'étendue de recherche LDAP qui déterminent l'emplacement où Mac OS X doit rechercher un type de fiche Mac OS X particulier dans un répertoire LDAP.

Important : lors du mappage d'attributs d'utilisateur Mac OS X vers un domaine de répertoire LDAP en lecture/écriture (un domaine LDAP qui n'est pas en lecture seule), l'attribut LDAP mappé vers RealName ne doit pas être le même que le premier attribut d'une liste d'attributs LDAP mappés vers RecordName. Par exemple, l'attribut cn ne doit pas être le premier attribut mappé vers RecordName si cn est également mappé vers RealName. Si l'attribut LDAP mappé vers RealName est le même que le premier attribut mappé vers RecordName, des problèmes se produiront lorsque vous essaierez de modifier le nom complet (long) ou le premier nom abrégé dans Gestionnaire de groupe de travail.

Pour obtenir des spécifications détaillées de types de fiches et d'attributs Mac OS X, consultez l'annexe "Données de répertoire Mac OS X".

Pour modifier les bases de recherche et les mappages d'un serveur LDAP :

1. Dans Format de répertoire, cliquez sur Services.
2. Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.
3. Sélectionnez LDAPv3 dans la liste des services, puis cliquez sur Configurer.
4. Si la liste des configurations de serveur est masquée, cliquez sur Afficher les options.
5. Sélectionnez une configuration de serveur dans la liste, puis cliquez sur Modifier.
6. Cliquez sur Recherche et mappages.
7. Sélectionnez les mappages à utiliser en tant que point de départ, le cas échéant.

   Cliquez sur le menu local "Accéder à ce serveur LDAPv3 via" et choisissez soit un modèle de mappage comme point de départ, soit "Personnalisé" pour commencer sans mappage prédéfini.
8. Ajoutez des types de fiches et modifiez leurs bases de recherche selon vos besoins.
   - Pour ajouter des types de fiches, cliquez sur Ajouter situé sous la liste Types d'enregistrement et attributs. Dans la fenêtre à l'écran, sélectionnez Types d'enregistrement, choisissez un ou plusieurs types de fiches dans la liste, puis cliquez sur OK.
   - Pour modifier la base de recherche et l'étendue de recherche d'un type de fiche, sélectionnez-le dans la liste Types d'enregistrement et attributs. Modifiez ensuite le contenu du champ "Base de recherche". Sélectionnez "tous les sous-arbres" pour configurer l'étendue de recherche pour qu'elle contienne l'ensemble de la hiérarchie du répertoire LDAP à partir de la base de recherche. Sélectionnez "le premier niveau" pour configurer l'étendue de recherche pour qu'elle ne contienne que la base de recherche et un niveau sous cette dernière dans la hiérarchie du répertoire LDAP.

- Pour supprimer un type d'enregistrement, sélectionnez-le dans la liste Types d'enregistrement et attributs, puis cliquez sur Supprimer.
- Pour ajouter un mappage pour un type de fiche, sélectionnez ce type dans la liste Types d'enregistrement et attributs. Cliquez ensuite sur le bouton Ajouter situé sous "Mapper sur __ éléments listés" et tapez le nom d'une classe d'objet du répertoire LDAP. Pour ajouter une autre classe d'objet LDAP, vous pouvez appuyer sur la touche Retour et saisir le nom de la classe d'objet souhaitée. Spécifiez si vous souhaitez utiliser toutes les classes d'objets LDAP ou l'une d'entre elles via la menu local situé au-dessus de la liste.
- Pour changer un mappage pour un type de fiche, sélectionnez ce type dans la liste Types d'enregistrement et attributs. Double-cliquez ensuite sur la classe d'objet LDAP à modifier, dans "Mapper sur __ éléments listés", puis modifiez-la. Spécifiez si vous souhaitez utiliser toutes les classes d'objets LDAP ou l'une d'entre elles via la menu local situé au-dessus de la liste.
- Pour supprimer un mappage pour un type de fiche, sélectionnez ce type dans la liste Types d'enregistrement et attributs. Dans "Mapper sur __ éléments listés", cliquez sur la classe d'objet LDAP à supprimer, puis cliquez sur le bouton Supprimer.

9 Ajoutez des attributs, puis modifiez leur mappage comme requis.

- Pour ajouter des attributs à un type de fiche, sélectionnez ce type dans la liste Types d'enregistrement et attributs. Cliquez sur le bouton Ajouter situé sous la liste Types d'enregistrement et attributs. Dans la fenêtre à l'écran, sélectionnez Types d'attributs, choisissez un ou plusieurs types d'attributs dans la liste, puis cliquez sur OK.
- Pour ajouter un mappage pour un attribut, sélectionnez l'attribut dans la liste Types d'enregistrement et attributs. Cliquez ensuite sur le bouton Ajouter, sous "Mapper sur __ éléments listés", puis tapez le nom d'un attribut du répertoire LDAP. Pour ajouter un autre attribut LDAP, vous pouvez appuyer sur la touche Retour et saisir le nom de l'attribut.
- Pour changer un mappage pour un attribut, sélectionnez l'attribut dans la liste Types d'enregistrement et attributs. Dans Mapper sur __ éléments listés, double-cliquez sur l'élément à modifier, puis changez le nom de l'élément.
- Pour supprimer un mappage pour un attribut, sélectionnez l'attribut dans la liste Types d'enregistrement et attributs. Dans Mapper sur __ éléments listés, cliquez sur l'élément LDAPv3 à supprimer, puis sur le bouton Supprimer situé sous Mapper sur __ éléments listés.
- Pour modifier l'ordre des attributs dans la liste située à droite, glissez les attributs vers le haut ou le bas dans la liste.

10 Cliquez sur Enregistrer le modèle si vous souhaitez enregistrer vos mappages sous la forme d'un modèle.

Les modèles enregistrés dans l'emplacement par défaut apparaissent dans les menus locaux des modèles de mappages LDAP la prochaine fois que l'utilisateur ouvre Format de répertoire. L'emplacement par défaut pour les modèles est le dossier de départ de l'utilisateur courant dans le chemin suivant :

~/Library/Application Support/Directory Access/LDAPv3/Templates

11 Cliquez sur "Écrire sur le serveur" pour stocker les mappages dans le répertoire LDAP pour lui permettre de les fournir automatiquement à ses clients.

Vous devez saisir une base de recherche dans laquelle stocker les mappages, un nom distinctif d'administrateur ou de tout autre utilisateur possédant des permissions d'écriture sur la base de recherche (par exemple, uid=diradmin,cn=utilisateurs,dc=ods,dc=exemple,dc=com) et un mot de passe. Si vous écrivez des mappages sur un serveur LDAP Open Directory, la base de recherche correcte est "cn=config, *suffixe*" (où *suffixe* est le suffixe de la base de recherche du serveur, comme par exemple "dc=exemple, dc=com").

Le répertoire LDAP fournit ses mappages aux clients Mac OS X dont la politique de recherche personnalisée contient une connexion qui est configurée pour obtenir les mappages du serveur LDAP. Le répertoire LDAP fournit aussi ses mappages à tous les clients Mac OS X qui disposent d'une politique de recherche automatique. Pour plus de détails, consultez les sections "Configuration de l'accès à un répertoire LDAP" à la page 133 et "Configuration de politiques de recherche" à la page 126.

Configuration d'une liaison sécurisée vers un répertoire LDAP

Vous pouvez utiliser Format de répertoire pour configurer la liaison sécurisée entre l'ordinateur et un répertoire LDAP qui prend en charge la liaison sécurisée. La liaison est authentifiée de façon mutuelle au moyen d'une fiche d'ordinateur authentifié, créée dans le répertoire lorsque vous configurez la liaison sécurisée.

L'ordinateur ne peut pas être configuré pour utiliser à la fois la liaison sécurisée LDAP et un répertoire LDAP fourni par DHCP. La liaison LDAP sécurisée est en réalité une liaison statique, alors que le LDAP fourni par DHCP est une liaison dynamique. Pour plus d'informations, consultez les sections "Activation ou désactivation d'un répertoire LDAP fourni via DHCP" à la page 131 et "Configuration d'une politique de liaison pour un maître Open Directory" à la page 96..

Pour configurer la liaison sécurisée vers un répertoire LDAP :

1 Dans Format de répertoire, cliquez sur Services.

2 Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.

3 Sélectionnez LDAPv3 dans la liste des services, puis cliquez sur Configurer.

4 Si la liste des configurations de serveur est masquée, cliquez sur Afficher les options.

5 Sélectionnez la configuration de serveur souhaitée, puis cliquez sur Modifier.

6 Cliquez sur Relier, saisissez les références demandées, puis cliquez sur OK.

Saisissez le nom de l'ordinateur, et le nom et le mot de passe d'un administrateur de domaine de répertoire LDAP. Le nom de l'ordinateur ne peut pas déjà être utilisé par un autre ordinateur pour la liaison sécurisée ou d'autres services de réseau.

Si le bouton Relier n'apparaît pas, le répertoire LDAP ne prend pas en charge la liaison sécurisée.

7 Si vous voyez apparaître un avertissement disant qu'il existe une fiche d'ordinateur, vous pouvez cliquer sur Écraser pour remplacer la fiche d'ordinateur existante.

Avant de remplacer une fiche d'ordinateur, assurez-vous que vous avez bien fourni le bon nom d'ordinateur à l'étape précédente. Cliquez sur Annuler pour revenir sur vos pas et changer le nom de l'ordinateur.

La fiche d'ordinateur existante peut être abandonnée ou appartenir à un autre ordinateur. Si vous décidez de remplacer une fiche d'ordinateur, prévenez l'administrateur du répertoire LDAP, au cas où le remplacement de la fiche désactiverait un autre ordinateur. Dans ce cas, l'administrateur du répertoire LDAP doit ajouter à nouveau l'ordinateur désactivé dans la liste des ordinateurs à laquelle il appartenait en utilisant un autre nom pour cet ordinateur. Pour obtenir des instructions sur l'ajout d'un ordinateur à une liste d'ordinateurs, consultez le chapitre consacré aux listes d'ordinateurs du guide de gestion des utilisateurs.

8 Cliquez sur OK pour clôturer la configuration de la liaison sécurisée.

Arrêt d'une liaison sécurisée avec un répertoire LDAP

Vous pouvez utiliser Format de répertoire pour arrêter une liaison sécurisée entre un ordinateur et un répertoire LDAP qui autorise, mais ne requiert pas la liaison sécurisée.

Pour arrêter une liaison sécurisée vers un répertoire LDAP :

1 Dans Format de répertoire, cliquez sur Services.

2 Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.

3 Sélectionnez LDAPv3 dans la liste des services, puis cliquez sur Configurer.

4 Si la liste des configurations de serveur est masquée, cliquez sur Afficher les options.

5 Sélectionnez la configuration de serveur souhaitée, puis cliquez sur Modifier.

6 Cliquez sur Rompre la liaison, puis saisissez les références requises et cliquez sur OK.

Saisissez le nom et le mot de passe d'un administrateur de répertoire LDAP (pas un administrateur de l'ordinateur local).

- Si la liaison sécurisée n'a pas été configurée sur cet ordinateur, le bouton Rompre l a liaison n'apparaît pas.
- Si vous voyez apparaître un avertissement disant que l'ordinateur ne peut pas contacter le serveur LDAP, vous pouvez cliquer sur OK pour forcer l'arrêt de la liaison sécurisée.

Si vous forcez l'arrêt de la liaison sécurisée, cet ordinateur disposera toujours d'une fiche d'ordinateur dans le répertoire LDAP. Prévenez l'administrateur du répertoire LDAP pour qu'il supprime l'ordinateur de sa liste d'ordinateurs. Pour obtenir des instructions sur la suppression d'un ordinateur de sa liste d'ordinateurs, consultez le chapitre consacré aux listes d'ordinateurs du guide de gestion des utilisateurs.

7 Cliquez sur OK pour clôturer l'arrêt de la liaison sécurisée.

Modification du délai d'ouverture/de fermeture pour une connexion LDAP

Format de répertoire permet de spécifier combien de temps Open Directory doit attendre avant d'annuler une tentative de connexion au serveur LDAP.

Pour définir le délai d'ouverture/de fermeture pour une connexion LDAP :

1 Dans Format de répertoire, cliquez sur Services.

2 Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.

3 Sélectionnez LDAPv3 dans la liste des services, puis cliquez sur Configurer.

4 Si la liste des configurations de serveur est masquée, cliquez sur Afficher les options.

5 Sélectionnez une configuration de serveur dans la liste, puis cliquez sur Modifier.

6 Cliquez sur Connexion et saisissez une valeur dans le champ "L'ouverture/fermeture expire après __ secondes".

La valeur par défaut est 15 secondes.

Modification du délai de requête pour une connexion LDAP

Format de répertoire permet de spécifier combien de temps Open Directory doit attendre avant d'annuler une requête envoyée au serveur LDAP.

Pour définir le délai de requête pour une connexion LDAP :

1 Dans Format de répertoire, cliquez sur Services.

2 Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.

3 Sélectionnez LDAPv3 dans la liste des services, puis cliquez sur Configurer.

4 Si la liste des configurations de serveur est masquée, cliquez sur Afficher les options.

5 Sélectionnez une configuration de serveur dans la liste, puis cliquez sur Modifier.

6 Cliquez sur Connexion et saisissez une valeur dans le champ "La requête expire après __ secondes".

La valeur par défaut est 120 secondes.

Modification du délai de tentative de reconnexion pour une connexion LDAP

Format de répertoire permet de spécifier combien de temps attendre avant de tenter de se reconnecter si le serveur LDAP ne répond pas. Vous pouvez augmenter cette valeur pour éviter des tentatives de reconnexion continues.

Pour définir le délai de tentative de reconnexion pour les clients LDAP inactifs :

1. Dans Format de répertoire, cliquez sur Services.
2. Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.
3. Sélectionnez LDAPv3 dans la liste des services, puis cliquez sur Configurer.
4. Si la liste des configurations de serveur est masquée, cliquez sur Afficher les options.
5. Sélectionnez une configuration de serveur dans la liste, puis cliquez sur Modifier.
6. Cliquez sur Connexion et saisissez une valeur dans le champ "Tentative de reconnexion après __ secondes".

   La valeur par défaut est 120 secondes.

Modification du délai d'inactivité pour une connexion LDAP

Format de répertoire permet de spécifier combien de temps une connexion LDAP reste inactive avant qu'Open Directory ne ferme la connexion. Vous pouvez ajuster ce réglage pour réduire le nombre de connexions ouvertes sur le serveur LDAP.

Pour définir le délai d'inactivité pour une connexion LDAP :

1. Dans Format de répertoire, cliquez sur Services.
2. Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.
3. Sélectionnez LDAPv3 dans la liste des services, puis cliquez sur Configurer.
4. Si la liste des configurations de serveur est masquée, cliquez sur Afficher les options.
5. Sélectionnez une configuration de serveur dans la liste, puis cliquez sur Modifier.
6. Cliquez sur Connexion et saisissez une valeur dans le champ "La connexion expirera après __ minutes".

   La valeur par défaut est 120 secondes.

Forçage de l'accès LDAPv2 en lecture seule

Format de répertoire permet de forcer une connexion vers un serveur LDAP à utiliser le protocole LDAPv2 hérité. Cette connexion LDAPv2 forcée est en lecture seule (et non en lecture-écriture) et n'utilise pas SSL.

Pour forcer l'accès LDAPv2 en lecture seule vers un serveur LDAP :

1. Dans Format de répertoire, cliquez sur Services.
2. Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.
3. Sélectionnez LDAPv3 dans la liste des services, puis cliquez sur Configurer.
4. Si la liste des configurations de serveur est masquée, cliquez sur Afficher les options.
5. Sélectionnez la configuration de serveur dans la liste, puis cliquez sur Modifier.
6. Cliquez sur Connexion et cochez la case "Utiliser LDAPv2 (lecture seule)".

Ignorance des références de serveur LDAP

Format de répertoire permet de spécifier si l'ordinateur doit ignorer ou suivre les références d'un serveur LDAP pour rechercher des informations sur d'autres serveurs LDAP ou répliques. Les références de serveur peuvent aider un ordinateur à trouver des informations, mais peuvent aussi retarder la connexion ou provoquer d'autres délais si l'ordinateur finit par rechercher des références sur de nombreux serveurs LDAP.

Pour spécifier s'il faut ignorer les références de serveur LDAP :

1. Dans Format de répertoire, cliquez sur Services.
2. Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.
3. Sélectionnez LDAPv3 dans la liste des services, puis cliquez sur Configurer.
4. Si la liste des configurations de serveur est masquée, cliquez sur Afficher les options.
5. Sélectionnez une configuration de serveur dans la liste, puis cliquez sur Modifier.
6. Cliquez sur Connexion et cochez la case "Ignorer les références du serveur".

Authentification d'une connexion LDAP

Format de répertoire permet de configurer une connexion authentifiée vers un répertoire LDAP. Cette authentification est à un seul sens. L'ordinateur prouve son identité auprès d'un répertoire LDAP, mais le répertoire LDAP ne prouve pas son authenticité auprès de l'ordinateur. Pour une authentification mutuelle, consultez la section "Configuration d'une liaison sécurisée vers un répertoire LDAP" à la page 146.

Remarque : si la liaison sécurisée est déjà configurée entre l'ordinateur et le répertoire LDAP, une connexion authentifiée serait redondante ; vous ne pouvez donc pas en configurer une.

Pour configurer une connexion LDAPv3 authentifiée :

1. Dans Format de répertoire, cliquez sur Services.
2. Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.
3. Sélectionnez LDAPv3 dans la liste des services, puis cliquez sur Configurer.

4 Si la liste des configurations de serveur est masquée, cliquez sur Afficher les options.

5 Sélectionnez une configuration de serveur dans la liste, puis cliquez sur Modifier.

6 Cliquez sur Sécurité, cochez la case "Utiliser l'authentification lors de la connexion", puis saisissez un nom distinctif d'utilisateur et un mot de passe.

Le nom distinctif peut spécifier tout compte d'utilisateur ayant l'autorisation de voir les données dans le répertoire. Par exemple, un compte d'utilisateur dont le nom abrégé est "authentificateur" sur un serveur LDAP dont l'adresse est ods.exemple.com porterait le nom distinctif uid=authentificateur,cn=utilisateurs,dc=ods,dc=exemple,dc=com.

Important : si le nom distinctif ou le mot de passe est incorrecte personne ne pourra se connecter à l'ordinateur à l'aide de comptes d'utilisateur provenant du répertoire LDAP.

Modification du mot de passe utilisé pour authentifier une connexion LDAP

Format de répertoire permet de mettre à jour des connexions LDAP authentifiées pour qu'elles utilisent un nouveau mot de passe qui a été modifié sur le serveur LDAP. (Tous les ordinateurs disposant d'une connexion authentifiée vers un serveur LDAP doivent être mis à jour si le mot de passe utilisé pour authentifier la connexion LDAP est modifié sur le serveur).

Pour modifier le mot de passe pour une connexion LDAP :

1 Dans Format de répertoire, cliquez sur l'onglet Services.

2 Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.

3 Sélectionnez LDAPv3 dans la liste des services, puis cliquez sur Configurer.

4 Si la liste des configurations de serveur est masquée, cliquez sur Afficher les options.

5 Sélectionnez une configuration de serveur dans la liste, puis cliquez sur Modifier.

6 Cliquez sur Sécurité, puis modifiez le réglage de mot de passe.

- Si le réglage de mot de passe est estompé parce que la case à cocher "Utiliser l'authentification lors de la connexion" est désélectionnée, consultez la section "Authentification d'une connexion LDAP" à la page 150.
- Si le réglage de mot de passe est estompé parce que la case à cocher "Relié au répertoire en tant que" est sélectionnée (mais quand même estompée), la connexion n'est pas authentifiée avec un mot de passe d'utilisateur. La connexion utilise alors plutôt une fiche d'ordinateur authentifié ou la liaison sécurisée.

Mappage d'attributs d'enregistrement de configuration pour répertoires LDAP

Si vous souhaitez stocker des informations pour les utilisateurs Mac OS X gérés dans un répertoire LDAP non-Apple, assurez-vous que vous mappez les attributs suivants du type d'enregistrement de configuration : RealName et DataStamp. Si vous ne mappez pas ces attributs, le message d'erreur suivant s'affichera lorsque vous utiliserez Gestionnaire de groupe de travail pour modifier une enregistrement d'utilisateur situé dans le répertoire LDAP :

L'attribut nommé "dsRecTypeStandard:Config" n'est pas mappé.

Vous pouvez ignorer ce message si vous n'utilisez pas la gestion de client Mac OS X, qui dépend des attributs RealName et DataStamp du type Enregistrement de configuration pour la mémoire cache.

Modification du mappage RFC 2307 pour activer la création d'utilisateurs

Pour pouvoir utiliser Gestionnaire de groupe de travail pour créer des utilisateurs sur un serveur LDAP non-Apple qui utilise des mappages RFC 2307 (UNIX), vous devez modifiez le mappage du type de fiche Utilisateurs. Vous devez pour cela utiliser l'application Format de répertoire.

Pour activer la création d'enregistrements d'utilisateurs dans un répertoire LDAP avec mappages RFC 2307 :

1. Dans Format de répertoire, cliquez sur Services.
2. Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.
3. Sélectionnez LDAPv3 dans la liste des services, puis cliquez sur Configurer.
4. Si la liste des configurations de serveur est masquée, cliquez sur Afficher les options.
5. Sélectionnez la configuration de répertoire avec mappages RFC 2307, puis cliquez sur Modifier.
6. Cliquez sur Recherche et mappages.
7. Sélectionnez Utilisateurs dans la liste de gauche.

   Par défaut, "Mapper sur __ éléments listés" est réglé sur "N'importe quel" et la liste de droite contient posixAccount, inetOrgPerson et shadowAccount.
8. Réglez "Mapper sur __ éléments listés" sur "Tout", puis modifiez la liste de droite pour obtenir l'ensemble exact de classes d'objets LDAP vers lesquelles vous voulez mapper le type d'enregistrement Utilisateurs.

   Supprimez par exemple shadowAccount de la liste de sorte qu'Utilisateurs ne soit associé qu'à posixAccount et inetOrgPerson. Ou bien, vous pouvez mapper Utilisateurs vers account, posixAccount et shadowAccount.

- Pour modifier un élément de la liste, double-cliquez dessus.
- Pour ajouter un élément à la liste, cliquez sur Ajouter.
- Pour supprimer l'élément sélectionné de la liste, cliquez sur Supprimer.
- Pour modifier l'ordre des éléments, glissez ces derniers vers le haut ou le bas dans la liste.

Pour trouver les classes d'objets des enregistrements d'utilisateurs existants dans le répertoire LDAP, utilisez l'outil UNIX ldapsearch dans une fenêtre Terminal. L'exemple suivant affiche les classes d'objets d'un enregistrement d'utilisateur dont l'attribut cn est "Léonard de Vinci" :

```
ldapsearch -x -h ldapserver.exemple.com -b "dc=exemple, dc=com" 'cn=Léonard
     de Vinci' objectClass
```

Le résultat obtenu avec cet exemple de commande sera semblable à :

```
# Léonard de Vinci, exemple.com
dn: cn=Léonard de Vinci, dc=exemple, dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
```

Préparation d'un répertoire LDAP en lecture seule pour Mac OS X

Pour qu'un ordinateur Mac OS X puisse lire des données administratives dans un répertoire LDAP en lecture seule, ces données doivent exister dans le répertoire LDAP en lecture seule au format requis par Mac OS X. Il faudra peut-être ajouter, modifier ou réorganiser les données dans le répertoire LDAP en lecture seule. Mac OS X ne peut pas écrire des données dans un répertoire LDAP en lecture seule : il faut donc effectuer les modifications nécessaires à l'aide d'outils sur le serveur qui héberge le répertoire LDAP en lecture seule.

Pour préparer un répertoire LDAP en lecture seule pour Mac OS X :

1. Accédez au serveur qui héberge le répertoire LDAP en lecture seule et configurez-le pour qu'il gère l'authentification LDAP et la vérification des mots de passe.
2. Modifiez comme il se doit les classes d'objets et attributs du répertoire LDAP afin de fournir les données nécessaires à Mac OS X.

Pour obtenir des spécifications détaillées sur les données requises par les services de répertoire de Mac OS X, consultez l'annexe, "Données de répertoire Mac OS X".

Remplissage de répertoires LDAP avec des données pour Mac OS X

Après avoir configuré l'accès aux domaines de répertoire LDAP et configuré leur mappage de données, vous pouvez les remplir avec des enregistrements et des données pour Mac OS X. Pour les répertoires LDAP qui autorisent l'administration à distance (accès en lecture/écriture), vous pouvez utiliser l'application Gestionnaire de groupe de travail, livrée avec Mac OS X Server, de la manière suivante :

- Les points de partage d'identité et les domaines partagés que vous souhaitez monter automatiquement dans les navigateurs de Réseau des utilisateurs (ce que les utilisateurs voient lorsqu'ils cliquent sur Réseau dans la barre latérale d'une fenêtre du Finder). Utilisez les modules Partage et Réseau de Gestionnaire de groupe de travail. Pour plus d'instructions, consultez le guide d'administration de services de fichiers.
- Définissez les enregistrements d'utilisateurs et de groupes, puis configurez-les. Utilisez le module Comptes de Gestionnaire de groupe de travail. Pour plus d'instructions, consultez le guide de gestion des utilisateurs.
- Définissez les listes d'ordinateurs partageant les mêmes réglages de préférences et disponibles pour les mêmes utilisateurs et groupes. Utilisez le module Ordinateurs de Gestionnaire de groupe de travail. Pour plus d'instructions, consultez le guide de gestion des utilisateurs.

Dans tous les cas, cliquez sur la petite icône de globe au-dessus de la liste des utilisateurs, puis choisissez une option du menu local de Gestionnaire de groupe de travail pour ouvrir le domaine de répertoire LDAP. Si le répertoire LDAP ne figure pas dans le menu local, choisissez Autre pour le sélectionner.

Remarque : pour ajouter des enregistrements et des données à un serveur LDAP en lecture seule, vous devez utiliser des outils sur le serveur qui héberge.

Accès à un domaine Active Directory

Vous pouvez configurer un serveur équipé de Mac OS X Server ou un ordinateur doté de Mac OS X pour accéder à un domaine Active Directory sur un serveur Windows 2000 ou Windows 2003. Pour trouver les descriptions des tâches et des instructions, reportez-vous à :

- "À propos du module externe Active Directory" (ci-après).
- "Configuration de l'accès à un domaine Active Directory" à la page 157.
- "Configuration de comptes d'utilisateur mobiles dans Active Directory" à la page 159.
- "Configuration de dossiers de départ pour des comptes d'utilisateur Active Directory" à la page 160.
- "Configuration d'un shell UNIX pour des comptes d'utilisateur Active Directory" à la page 161.
- "Association de l'UID à un attribut Active Directory" à la page 161.
- "Mappage de l'identifiant de groupe principal vers un attribut Active Directory" à la page 162.
- "Mappage de l'identifiant de groupe des comptes de groupe vers un attribut Active Directory" à la page 163.
- "Spécification d'un serveur Active Directory préféré" à la page 164.
- "Modification des groupes Active Directory autorisés à administrer l'ordinateur" à la page 164.
- "Contrôle de l'authentification à partir de tous les domaines de la forêt Active Directory" à la page 165.
- "Rupture de la liaison avec le serveur Active Directory" à la page 166.

- “Modification de comptes d’utilisateur et d’autres enregistrements dans Active Directory” à la page 167.

Pour certains réseaux, d’autres méthodes s’avèrent appropriées pour l’accès à un domaine Active Directory. Consultez la section “Configuration de l’accès LDAP aux domaines Active Directory” à la page 167.

À propos du module externe Active Directory

Vous pouvez configurer Mac OS X pour accéder à des informations de compte d’utilisateur élémentaires dans un domaine Active Directory d’un serveur Windows 2000 ou Windows 2003. Cela est possible grâce au module externe Active Directory pour Format de répertoire. Ce module externe Active Directory figure dans la sous-fenêtre Services de Format de répertoire.

Il n’est pas nécessaire d’apporter des modifications de schéma au domaine Active Directory pour obtenir des informations élémentaires de compte d’utilisateur. Vous devrez éventuellement modifier la liste de contrôle d’accès (ACL) par défaut de certains attributs pour que les comptes d’ordinateur puissent lire les propriétés d’utilisateur. Le module externe Active Directory génère tous les attributs requis pour l’authentification Mac OS X à partir d’attributs standard dans les comptes d’utilisateur Active Directory. Le module externe gère également les politiques d’authentification Active Directory, y compris la modification, l’expiration et le changement forcé de mot de passe.

Le module externe Active Directory génère de manière dynamique un identifiant d’utilisateur unique et un identifiant de groupe principal, basés sur l’identifiant GUID (Globally Unique ID) du compte d’utilisateur dans le domaine Active Directory. L’identifiant d’utilisateur et l’identifiant de groupe principal générés sont toujours les mêmes pour chaque compte d’utilisateur, même si le compte est utilisé pour ouvrir une session sur différents ordinateurs Mac OS X. Vous pouvez également forcer le module externe Active Directory à associer l’identifiant d’utilisateur à des attributs Active Directory que vous spécifiez.

De même, le module externe Active Directory génère un identifiant de groupe d’après le GUID du compte de groupe Active Directory. Vous pouvez aussi forcer le module externe à mapper l’identifiant de groupe pour les comptes de groupe vers des attributs Active Directory que vous spécifiez.

Lorsque quelqu’un se connecte à Mac OS X à l’aide d’un compte d’utilisateur Active Directory, le module externe Active Directory peut monter automatiquement le répertoire de départ réseau Windows qui est spécifié comme étant le répertoire de départ Mac OS X de l’utilisateur dans le compte d’utilisateur Active Directory. Vous pouvez spécifier s’il faut utiliser le répertoire de départ réseau spécifié par l’attribut homeDirectory standard d’Active Directory ou par l’attribut HomeDirectory de Mac OS X, si le schéma Active Directory a été étendu pour le contenir.

Vous pouvez aussi configurer le module externe pour qu'il crée un dossier de départ local sur le volume de démarrage de l'ordinateur client Mac OS X. Dans ce cas, le module externe monte aussi le répertoire de départ Windows de l'utilisateur (spécifié dans le compte d'utilisateur Active Directory) comme volume de réseau, comme un point de partage. À l'aide du Finder, l'utilisateur peut copier des fichiers entre le volume réseau du répertoire de départ Windows et le répertoire de départ Mac OS X.

Le module externe Active Directory peut aussi créer des comptes mobiles pour les utilisateurs. Un compte mobile met les références d'authentification Active Directory de l'utilisateur en mémoire cache sur l'ordinateur client Mac OS X. Les références mises en mémoire cache permettent à l'utilisateur de se connecter à l'aide du nom et du mot de passe Active Directory alors que l'ordinateur client est déconnecté du serveur Active Directory. Un compte mobile dispose d'un dossier de départ local sur le volume de démarrage de l'ordinateur client Mac OS X. (L'utilisateur dispose d'un dossier de départ réseau, comme spécifié dans le compte Active Directory de l'utilisateur).

Si le schéma Active Directory a été étendu pour inclure les types d'enregistrements (classes d'objets) et les attributs Mac OS X, le module externe Active Directory les détecte et y accède automatiquement. Par exemple, le schéma Active Directory pourrait être modifié à l'aide d'outils d'administration Windows pour qu'il contienne des attributs de client géré Mac OS X. Cette modification du schéma permettrait au module externe Active Directory de prendre en charge les réglages de client géré définis à l'aide de l'application Gestionnaire de groupe de travail de Mac OS X Server. Les clients Mac OS X bénéficient d'un accès en lecture complet aux attributs ajoutés au répertoire. C'est pourquoi il peut s'avérer nécessaire de modifier la liste de contrôle d'accès de ces attributs pour autoriser les listes d'ordinateurs à lire ces attributs ajoutés.

Le module externe Active Directory détecte automatiquement tous les domaines dans une forêt Active Directory. Vous pouvez configurer le module externe afin de permettre aux utilisateurs de n'importe quel domaine de la forêt de s'authentifier sur un ordinateur Mac OS X. L'authentification multidomaine peut aussi être désactivée pour n'autoriser que l'authentification de domaines spécifiques sur le client.

Le module externe Active Directory prend entièrement en charge la réplication et le basculement Active Directory. Il détecte plusieurs contrôleurs de domaine et détermine le plus proche. Si un contrôleur de domaine devient indisponible, le module externe bascule automatiquement sur un autre contrôleur de domaine proche.

Le module externe Active Directory utilise LDAP pour accéder aux comptes d'utilisateur Active Directory et Kerberos pour les authentifier. Le module externe Active Directory n'utilise pas l'interface propriétaire ADSI (Active Directory Services Interface) de Microsoft pour accéder aux services de répertoire ou d'authentification.

Configuration de l'accès à un domaine Active Directory

À l'aide du module externe Active Directory répertorié dans Format de répertoire, vous pouvez configurer Mac OS X pour accéder aux informations élémentaires de compte d'utilisateur dans un domaine Active Directory sur un serveur Windows. Le module externe Active Directory génère tous les attributs requis pour l'authentification Mac OS X. Aucune modification du schéma Active Directory n'est nécessaire. Le module externe Active Directory détecte et accède aux types d'enregistrements et aux attributs Mac OS X standard, tels que les attributs requis pour la gestion de client Mac OS X, si le schéma Active Directory a été étendu pour les inclure.

> ***Avertissement :*** des options avancées du module externe Active Directory permettent de mapper l'identifiant d'utilisateur unique (UID) Mac OS X, l'identifiant de groupe (GID) principal et l'attribut d'identifiant de groupe vers les attributs appropriés qui ont été ajoutés au schéma Active Directory. Si vous changez ultérieurement le réglage de cette option de mappage, les utilisateurs risquent de perdre l'accès aux fichiers créés précédemment.

Pour configurer l'accès à un domaine Active Directory :

1. Dans Format de répertoire, cliquez sur Services.
2. Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.
3. Sélectionnez Active Directory dans la liste des services, puis cliquez sur Configurer.
4. Saisissez le nom DNS du domaine Active Directory auquel vous souhaitez lier l'ordinateur que vous êtes en train de configurer.

   L'administrateur du domaine Active Directory peut vous communiquer le nom DNS à saisir.
5. Si nécessaire, modifiez l'identifiant de l'ordinateur.

   L'identifiant de l'ordinateur est le nom sous lequel l'ordinateur sera connu dans le domaine Active Directory ; par défaut, il s'agit du nom de l'ordinateur. Il se peut que vous deviez le modifier pour vous conformer au schéma défini par votre organisation en matière de noms d'ordinateurs dans le domaine Active Directory. Si vous n'êtes pas sûr du nom à saisir, consultez l'administrateur du domaine Active Directory.
6. Définissez éventuellement les options avancées.

   Si les options avancées sont masquées, cliquez sur Afficher les options avancées et définissez des options dans les sous-fenêtres Expérience utilisateur, Mappages et Administratif. Vous pouvez aussi modifier des réglages d'options avancées ultérieurement. Pour obtenir des instructions détaillées sur les options avancées, consultez les sections :

   - "Configuration de comptes d'utilisateur mobiles dans Active Directory" à la page 159.
   - "Configuration de dossiers de départ pour des comptes d'utilisateur Active Directory" à la page 160.

- “Configuration d’un shell UNIX pour des comptes d’utilisateur Active Directory” à la page 161.
- “Association de l’UID à un attribut Active Directory” à la page 161.
- “Mappage de l’identifiant de groupe principal vers un attribut Active Directory” à la page 162.
- “Mappage de l’identifiant de groupe des comptes de groupe vers un attribut Active Directory” à la page 163.
- “Spécification d’un serveur Active Directory préféré” à la page 164.
- “Modification des groupes Active Directory autorisés à administrer l’ordinateur” à la page 164.
- “Contrôle de l’authentification à partir de tous les domaines de la forêt Active Directory” à la page 165.

7 Cliquez sur Relier, authentifiez-vous comme un utilisateur qui a le droit de relier un ordinateur au domaine Active Directory, sélectionnez les politiques de recherche auxquelles vous souhaitez ajouter Active Directory et cliquez sur OK.

- *Nom d’utilisateur et mot de passe :* vous pouvez vous authentifier en saisissant les nom et mot de passe de votre compte d’utilisateur Active Directory, sinon, il se peut que l’administrateur du domaine Active Directory doive vous fournir un nom et un mot de passe.
- *Clé OU ordinateur :* saisissez l’unité organisationnelle (UO) de l’ordinateur que vous êtes en train de configurer.
- *Utiliser pour l’authentification :* détermine si Active Directory est ajouté automatiquement à la politique de recherche d’authentification de l’ordinateur.
- *Utiliser pour les contacts :* détermine si Active Directory est ajouté automatiquement à la politique de recherche de contacts de l’ordinateur.

Lorsque vous cliquez sur OK, Format de répertoire configure la liaison sécurisée entre l’ordinateur que vous êtes en train de configurer et le serveur Active Directory. Les politiques de recherche de l’ordinateur sont configurées en fonction des options que vous avez sélectionnées lorsque vous vous êtes authentifié et Active Directory est activé dans la sous-fenêtre Services de Format de répertoire.

Avec les réglages par défaut pour les options avancées d’Active Directory, la forêt Active Directory est ajoutée à la politique de recherche d’authentification et/ou à la politique de recherche de contacts de l’ordinateur si vous avez sélectionné l’option “Utiliser pour l’authentification” et/ou l’option “Utiliser pour les contacts”. Mais si vous désélectionnez l’option “Autoriser l’authentification depuis n’importe quel domaine de la forêt” dans la sous-fenêtre d’options avancées Administratif avant de cliquer sur Relier, c’est le domaine Active Directory le plus proche qui est ajouté plutôt que la forêt. Vous pouvez modifier les politiques de recherche ultérieurement en ajoutant ou en supprimant la forêt Active Directory ou des domaines individuels. Pour obtenir des instructions, consultez la section “Définition de politiques de recherche personnalisées” à la page 128.

8 Si vous configurez un serveur pour l'accès à un domaine Active Directory, vous pouvez aussi relier le serveur au royaume Kerberos Active Directory.

Sur le serveur ou sur un ordinateur administrateur qui peut se connecter au serveur, ouvrez Admin Serveur et sélectionnez Open Directory pour le serveur. Cliquez sur Réglages, puis sur Général. Cliquez sur Se connecter à Kerberos, puis choisissez le royaume Kerberos Active Directory dans le menu local et saisissez les références d'un administrateur local sur ce serveur. Pour obtenir des instructions détaillées, consultez la section "Connecter un serveur à un royaume Kerberos" à la page 95..

Configuration de comptes d'utilisateur mobiles dans Active Directory

Vous pouvez lancer ou arrêter l'utilisation de comptes d'utilisateur Active Directory mobiles sur un ordinateur configuré pour utiliser le module externe Active Directory de Format de répertoire. Les utilisateurs qui disposent de comptes mobiles peuvent se connecter à l'aide de leurs références Active Directory lorsque l'ordinateur n'est pas connecté au serveur Active Directory. Le module externe Active Directory met en mémoire cache les références d'un compte mobile d'utilisateur lorsque l'utilisateur se connecte alors que l'ordinateur est connecté au domaine Active Directory. Cette mise en cache des références ne requiert aucune modification du schéma Active Directory. Si le schéma Active Directory a été étendu pour inclure les attributs de client géré Mac OS X, les réglages de leur compte mobile seront utilisés à la place des réglages de compte mobile mis en mémoire cache du module externe Active Directory.

Vous pouvez faire créer les comptes mobiles automatiquement ou obliger les utilisateurs Active Directory à confirmer la création des comptes mobiles.

Pour activer ou désactiver les comptes mobiles à partir d'un domaine Active Directory :

1 Dans Format de répertoire, cliquez sur Services.

2 Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.

3 Sélectionnez Active Directory dans la liste des services, puis cliquez sur Configurer.

4 Si les options avancées sont masquées, cliquez sur Afficher les options avancées.

5 Cliquez sur Expérience utilisateur, puis sur "Créer un compte mobile lors de l'ouverture de session" et, facultativement, sur "Exiger une confirmation avant de créer un compte mobile".

- Si vous sélectionnez les deux options, chaque utilisateur décide de créer ou non un compte mobile à l'ouverture de session. Lorsqu'un utilisateur se connecte à Mac OS X à l'aide d'un compte d'utilisateur Active Directory, l'utilisateur voit apparaître une zone de dialogue contenant des commandes pour la création immédiate d'un compte mobile et la connexion en tant qu'utilisateur réseau.

- Si la première option est sélectionnée et la seconde ne l'est pas, les comptes mobiles sont créés automatiquement à la connexion.
- Si la première option est désélectionnée, la seconde n'est pas accessible.

6 Cliquez sur OK.

Configuration de dossiers de départ pour des comptes d'utilisateur Active Directory

Sur un ordinateur qui est configuré pour utiliser le module externe Active Directory de Format de répertoire, vous pouvez lancer ou arrêter l'utilisation de dossiers de départ réseau ou de dossiers de départ locaux pour les comptes d'utilisateur Active Directory. Avec les dossiers de départ réseau, le répertoire de départ réseau Windows d'un utilisateur est monté comme le dossier de départ Mac OS X lorsque l'utilisateur se connecte. Vous pouvez spécifier s'il faut utiliser le répertoire de départ réseau spécifié par l'attribut HomeDirectory standard d'Active Directory ou par l'attribut HomeDirectory de Mac OS X, si le schéma Active Directory a été étendu pour le contenir.

Avec les dossiers de départ locaux, chaque utilisateur Active Directory qui se connecte dispose d'un dossier de départ sur le disque de démarrage de Mac OS X. De plus, le dossier de départ réseau de l'utilisateur est monté comme un volume réseau, comme un point de partage. L'utilisateur peut copier des fichiers entre ce volume réseau et le dossier de départ local.

Pour configurer des dossiers de départ pour des comptes d'utilisateur Active Directory :

1 Dans Format de répertoire, cliquez sur Services.

2 Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.

3 Sélectionnez Active Directory dans la liste des services, puis cliquez sur Configurer.

4 Si les options avancées sont masquées, cliquez sur Afficher les options avancées.

5 Cliquez sur Expérience utilisateur.

6 Cliquez sur "Forcer l'utilisation du répertoire de départ local sur le disque de démarrage" si vous souhaitez que les comptes d'utilisateur Active Directory aient des dossiers de départ locaux dans le dossier /Utilisateurs de l'ordinateur.

Cette option n'est pas disponible si la case "Créer un compte mobile lors de l'ouverture de session" est cochée.

7 Pour utiliser l'attribut standard d'Active Directory pour l'emplacement du dossier de départ, cochez la case "Utiliser le chemin UNC depuis Active Directory pour déduire l'emplacement du répertoire de départ réseau" et choisissez le protocole à utiliser pour accéder au dossier de départ.

- Choisissez "smb:" pour utiliser le protocole Windows standard, SMB/CIFS.
- Choisissez "afp:" pour utiliser le protocole Macintosh standard, AFP.

8 Pour utiliser l'attribut Mac OS X pour l'emplacement du dossier de départ, décochez la case "Utiliser le chemin UNC depuis Active Directory pour déduire l'emplacement du répertoire de départ réseau".

Pour utiliser l'attribut Mac OS X, le schéma Active Directory doit être étendu pour le contenir.

9 Cliquez sur OK.

Si vous changez le nom d'un compte d'utilisateur dans le domaine Active Directory, le serveur créera un nouveau dossier de départ (et des sous-dossiers) pour le compte d'utilisateur la prochaine fois qu'il sera utilisé pour la connexion à un ordinateur Mac OS X.

L'utilisateur peut naviguer dans l'ancien dossier de départ et voir son contenu dans le Finder.

Vous pouvez empêcher la création d'un nouveau dossier de départ en renommant l'ancien dossier avant la prochaine connexion de l'utilisateur.

Configuration d'un shell UNIX pour des comptes d'utilisateur Active Directory

Sur un ordinateur configuré pour utiliser le module externe Active Directory de Format de répertoire, vous pouvez définir le shell de ligne de commande que les utilisateurs disposant de comptes Active Directory vont utiliser par défaut lorsqu'ils interagiront avec Mac OS X dans l'application Terminal. Le shell par défaut est aussi utilisé pour l'interaction à distance via SSH (Secure Shell) ou Telnet. Chaque utilisateur peut redéfinir le shell par défaut en changeant une préférence de Terminal.

Pour définir un shell UNIX pour des comptes d'utilisateur Active Directory :

1 Dans Format de répertoire, cliquez sur Services.

2 Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.

3 Sélectionnez Active Directory dans la liste des services, puis cliquez sur Configurer.

4 Si les options avancées sont masquées, cliquez sur Afficher les options avancées.

5 Cliquez sur Expérience utilisateur, puis saisissez le chemin du shell utilisateur par défaut.

6 Cliquez sur OK.

Association de l'UID à un attribut Active Directory

Sur un ordinateur configuré pour utiliser le module externe Active Directory de Format de répertoire, vous pouvez spécifier l'attribut Active Directory à mapper vers l'attribut d'identifiant d'utilisateur unique (UID) de Mac OS X.

Généralement, le schéma Active Directory doit être étendu pour contenir un attribut qui convient au mappage vers l'UID.

- Si l'administrateur Active Directory étend le schéma Active Directory en installant les services pour UNIX de Microsoft, vous pouvez mapper l'UID vers l'attribut msSFU-30-Uid-Number.
- Si l'administrateur Active Directory étend manuellement le schéma Active Directory pour qu'il contienne les attributs RFC 2307, vous pouvez mapper l'UID vers uidNumber.
- Si l'administrateur Active Directory étend manuellement le schéma Active Directory pour qu'il contienne l'attribut UniqueID de Mac OS X, vous pouvez mapper l'UID vers ce dernier.

Si le mappage du UID est désactivé, le module externe Active Directory génère automatiquement un UID en fonction de l'attribut GUID standard d'Active Directory.

Avertissement : si vous modifiez ultérieurement le mappage de l'UID, les utilisateurs risquent de perdre l'accès aux fichiers créés précédemment.

Pour mapper l'UID à un attribut d'un schéma Active Directory étendu :

1. Dans Format de répertoire, cliquez sur Services.
2. Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.
3. Sélectionnez Active Directory dans la liste des services, puis cliquez sur Configurer.
4. Si les options avancées sont masquées, cliquez sur Afficher les options avancées.
5. Cliquez sur Mappages, puis cochez la case "Mappage UID à attribuer" et saisissez le nom de l'attribut Active Directory à mapper vers l'UID.

Mappage de l'identifiant de groupe principal vers un attribut Active Directory

Sur un ordinateur qui est configuré pour utiliser le module externe Active Directory de Format de répertoire, vous pouvez spécifier l'attribut Active Directory à mapper vers l'attribut d'identifiant de groupe principal (GID) de Mac OS X dans les comptes d'utilisateur.

Généralement, le schéma Active Directory doit être étendu pour contenir un attribut qui convient au mappage vers le GID principal.

- Si l'administrateur Active Directory étend le schéma Active Directory en installant les services pour UNIX de Microsoft, vous pouvez mapper le GID principal vers l'attribut msSFU-30-Gid-Number.
- Si l'administrateur Active Directory étend manuellement le schéma Active Directory pour qu'il contienne les attributs RFC 2307, vous pouvez mapper le GID principal vers gidNumber.
- Si l'administrateur Active Directory étend manuellement le schéma Active Directory pour qu'il contienne l'attribut PrimaryGroupID de Mac OS X, vous pouvez mapper le GID principal vers ce dernier.

Si le mappage du GID principal est désactivé, le module externe Active Directory génère automatiquement un GID principal en fonction de l'attribut GUID standard d'Active Directory.

> ***Avertissement :*** si vous modifiez ultérieurement le mappage du GID, les utilisateurs risquent de perdre l'accès aux fichiers créés précédemment.

Pour mapper le GID principal à un attribut d'un schéma Active Directory étendu :

1. Dans Format de répertoire, cliquez sur Services.
2. Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.
3. Sélectionnez Active Directory dans la liste des services, puis cliquez sur Configurer.
4. Si les options avancées sont masquées, cliquez sur Afficher les options avancées.
5. Cliquez sur Mappages, puis cochez la case "Mappage du GID d'utilisateur à attribuer" et saisissez le nom de l'attribut Active Directory à mapper vers l'identifiant de groupe principal dans les comptes d'utilisateur.

Mappage de l'identifiant de groupe des comptes de groupe vers un attribut Active Directory

Sur un ordinateur qui est configuré pour utiliser le module externe Active Directory de Format de répertoire, vous pouvez spécifier l'attribut Active Directory à mapper vers l'attribut d'identifiant de groupe principal (GID) de Mac OS X dans les comptes de groupe.

Généralement, le schéma Active Directory doit être étendu pour contenir un attribut qui convient au mappage vers le GID de groupe.

- Si l'administrateur Active Directory étend le schéma Active Directory en installant les services pour UNIX de Microsoft, vous pouvez mapper le GID de groupe vers l'attribut msSFU-30-Gid-Number.
- Si l'administrateur Active Directory étend manuellement le schéma Active Directory pour qu'il contienne les attributs RFC 2307, vous pouvez mapper le GID de groupe vers gidNumber.
- Si l'administrateur Active Directory étend manuellement le schéma Active Directory pour qu'il contienne l'attribut gidNumber de Mac OS X, vous pouvez mapper le GID de groupe vers ce dernier.

Si le mappage du GID de groupe est désactivé, le module externe Active Directory génère automatiquement un GID de groupe en fonction de l'attribut GUID standard d'Active Directory.

> ***Avertissement :*** si vous modifiez ultérieurement le mappage du GID de groupe, les utilisateurs risquent de perdre l'accès aux fichiers créés précédemment.

Pour mapper le GID de groupe vers un attribut d'un schéma Active Directory étendu :

1. Dans Format de répertoire, cliquez sur Services.
2. Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.
3. Sélectionnez Active Directory dans la liste des services, puis cliquez sur Configurer.
4. Si les options avancées sont masquées, cliquez sur Afficher les options avancées.
5. Cliquez sur Mappages, puis cochez la case "Mappage du GID de groupe à attribuer" et saisissez le nom de l'attribut Active Directory à mapper vers l'identifiant de groupe dans les comptes de groupe.

Spécification d'un serveur Active Directory préféré

Sur un ordinateur configuré pour utiliser le module externe Active Directory de Format de répertoire, vous pouvez spécifier le nom DNS du serveur auquel l'ordinateur doit accéder au domaine Active Directory par défaut. Si le serveur devient indisponible, le module externe Active Directory basculera automatiquement sur un autre serveur proche dans la forêt. Si cette option n'est pas sélectionnée, le module externe Active Directory détermine automatiquement le domaine Active Directory le plus proche dans la forêt.

Pour spécifier un serveur auquel le module externe Active Directory doit accéder par défaut :

1. Dans Format de répertoire, cliquez sur Services.
2. Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.
3. Sélectionnez Active Directory dans la liste des services, puis cliquez sur Configurer.
4. Si les options avancées sont masquées, cliquez sur Afficher les options avancées.
5. Cliquez sur Administratif, puis cochez la case "Préférer ce serveur de domaine" et saisissez le nom DNS du serveur Active Directory.

Modification des groupes Active Directory autorisés à administrer l'ordinateur

Sur un ordinateur configuré pour utiliser le module externe Active Directory de Format de répertoire, vous pouvez identifier les comptes de groupe Active Directory dont les membres doivent avoir des autorisations d'administrateur pour l'ordinateur. Les utilisateurs qui sont membres de ces comptes de groupe Active Directory peuvent effectuer des tâches administratives comme, par exemple, installer des logiciels sur l'ordinateur Mac OS X que vous êtes en train de configurer.

Pour ajouter ou supprimer des comptes de groupe Active Directory dont les membres ont des autorisations d'administrateur :

1. Dans Format de répertoire, cliquez sur Services.
2. Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.
3. Sélectionnez Active Directory dans la liste des services, puis cliquez sur Configurer.
4. Si les options avancées sont masquées, cliquez sur Afficher les options avancées.
5. Cliquez sur Administratif, cochez la case "Permettre l'administration par", puis modifiez la liste des comptes de groupe Active Directory dont les membres doivent avoir des autorisations d'administrateur.
   - Pour ajouter un groupe, cliquez sur le bouton Ajouter (+) et saisissez le nom de domaine Active Directory, une barre oblique inverse et le nom du compte de groupe (par exemple, ADS\Domain Admins,IL2\Domain Admins).
   - Pour supprimer un groupe, sélectionnez-le dans la liste, puis cliquez sur le bouton Supprimer (–).

Contrôle de l'authentification à partir de tous les domaines de la forêt Active Directory

Sur un ordinateur configuré pour utiliser le module externe Active Directory de Format de répertoire, vous pouvez autoriser les utilisateurs provenant de tous les domaines de la forêt Active Directory à s'authentifier ou à restreindre l'authentification aux utilisateurs de domaines individuels.

Pour contrôler si les utilisateurs peuvent s'authentifier depuis tous les domaines de la forêt :

1. Dans Format de répertoire, cliquez sur Services.
2. Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.
3. Sélectionnez Active Directory dans la liste des services, puis cliquez sur Configurer.
4. Si les options avancées sont masquées, cliquez sur Afficher les options avancées.
5. Cliquez sur Administratif, puis cochez la case "Autoriser l'authentification depuis n'importe quel domaine de la forêt".
6. Une fois que vous avez changé le réglage de cette option, vous devez changer la politique de recherche personnalisée dans la sous-fenêtre Authentification et/ou Contacts pour inclure la forêt Active Directory ou des domaines sélectionnés, selon ce qui convient.

   Pour obtenir des instructions sur le changement de politique de recherche personnalisée, consultez la section "Définition de politiques de recherche personnalisées" à la page 128.

- Si vous cochez la case “Autoriser l’authentification depuis n’importe quel domaine de la forêt”, vous pouvez ajouter la forêt Active Directory aux politiques de recherche personnalisées pour l’authentification et les contacts de l’ordinateur. Lorsque vous ajoutez des éléments à une politique de recherche personnalisée, la forêt apparaît dans la liste des domaines de répertoire disponibles sous la forme “/Active Directory/All Domains”. (Il s’agit du réglage par défaut).
- Si vous désélectionnez la case “Autoriser l’authentification depuis n’importe quel domaine de la forêt”, vous pouvez ajouter des domaines Active Directory aux politiques de recherche personnalisées pour l’authentification et les contacts de l’ordinateur individuellement. Lorsque vous ajoutez des éléments à une politique de recherche personnalisée, chaque domaine Active Directory apparaît séparément dans la liste des domaines de répertoire disponibles.

Rupture de la liaison avec le serveur Active Directory

Si l’ordinateur utilise le module externe Active Directory pour se lier à un serveur Active Directory, vous pouvez rompre la liaison de l’ordinateur avec le serveur Active Directory. Vous pouvez forcer la rupture de la liaison si l’ordinateur ne peut pas contacter le serveur ou si la fiche d’ordinateur a déjà été supprimée du serveur.

Pour rompre la liaison de l’ordinateur avec le serveur Active Directory :

1. Dans Format de répertoire, cliquez sur Services.
2. Si l’icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d’un administrateur.
3. Sélectionnez Active Directory dans la liste des services, puis cliquez sur Configurer.
4. Cliquez sur Rompre la liaison, puis authentifiez-vous comme un utilisateur disposant des droits nécessaires pour rompre une connexion avec le domaine Active Directory, puis cliquez sur OK.

   Si vous voyez apparaître un avertissement disant que les références ne sont pas acceptées ou que l’ordinateur ne peut pas contacter Active Directory, vous pouvez cliquer sur “Forcer à rompre le lien” pour forcer la rupture de la connexion.

   Si vous forcez la rupture de la connexion, Active Directory disposera toujours d’une fiche d’ordinateur pour cet ordinateur. Prévenez l’administrateur d’Active Directory pour qu’il supprime la fiche d’ordinateur.
5. Dans la sous-fenêtre Services, désélectionnez le réglage Activer d’Active Directory, puis cliquez sur Appliquer.

Modification de comptes d'utilisateur et d'autres enregistrements dans Active Directory

Vous pouvez utiliser Gestionnaire de groupe de travail pour modifier les comptes d'utilisateur, les comptes de groupe, les listes d'ordinateurs et d'autres enregistrements dans un domaine Active Directory. Vous pouvez également utiliser Gestionnaire de groupe de travail pour supprimer des enregistrements dans un domaine Active Directory. Si le schéma Active Directory a été étendu pour contenir les types d'enregistrement (les classes d'objets) et les attributs Mac OS X standard, vous pouvez utiliser Gestionnaire de groupe de travail pour créer et modifier des listes d'ordinateurs dans le domaine Active Directory. Pour obtenir des instructions sur l'utilisation de comptes d'utilisateur, de comptes de groupe et de listes d'ordinateurs, consultez la section guide de gestion des utilisateurs.

Pour créer des comptes d'utilisateur, des comptes de groupe dans un domaine Active Directory, utilisez les outils d'administration Active Directory de Microsoft sur un ordinateur d'administration serveur Windows.

Configuration de l'accès LDAP aux domaines Active Directory

Format de répertoire vous permet de définir une configuration LDAPv3 afin d'accéder à un domaine Active Directory situé sur un serveur Windows. Une configuration LDAPv3 vous donne un contrôle total sur le mappage des types et attributs d'enregistrements Mac OS X vers les classes d'objets, bases de recherche et attributs Active Directory. Le mappage de certains attributs et types d'enregistrements Mac OS X importants, tels que l'UID (l'identifiant d'utilisateur unique), nécessite l'extension du schéma Active Directory.

De nombreuses fonctions du module externe Active Directory figurant dans Format de répertoire sont absentes des configurations LDAPv3. Il s'agit de la génération dynamique d'un identifiant d'utilisateur unique et d'un identifiant de groupe principal, de la création d'un répertoire de départ Mac OS X local, du montage automatique du répertoire de départ Windows, de comptes d'utilisateur mobiles avec références d'authentification mises en cache, de la détection de tous les domaines d'une forêt Active Directory et de la prise en charge de la duplication et du basculement Active Directory. Pour plus de détails, consultez la section "À propos du module externe Active Directory" à la page 155.

Pour créer une configuration de serveur Active Directory :

1. Dans Format de répertoire, cliquez sur Services.
2. Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.
3. Sélectionnez LDAPv3 dans la liste des services, puis cliquez sur Configurer.
4. Cliquez sur Nouveau et saisissez le nom DNS ou l'adresse IP du serveur Active Directory.

5 Sélectionnez les options pour l'accès au répertoire, puis cliquez sur Continuer pour que Format de répertoire obtienne les informations du serveur Active Directory.

- Cochez la case "Crypter via SSL" si vous souhaitez qu'Open Directory utilise Secure Sockets Layer (SSL) pour les connexions avec le serveur Active Directory.
- Cochez la case "Utiliser pour l'authentification" si ce répertoire contient des comptes d'utilisateur que quelqu'un va utiliser pour la connexion ou pour l'authentification à des services.
- Cochez la case "Utiliser pour les contacts" si ce répertoire contient des adresses électroniques et d'autres informations que vous souhaitez utiliser dans Carnet d'adresses.

Si Format de répertoire ne peut pas contacter le serveur Active Directory, il affiche un message et vous devez alors configurer l'accès manuellement ou annuler le processus de configuration. Pour obtenir des instructions sur la configuration, consultez la section "Configuration manuelle de l'accès à un répertoire LDAP" à la page 135.

6 Si la zone de dialogue se développe pour afficher des options de mappage, choisissez Active Directory dans le menu local, saisissez la base de recherche, puis cliquez sur Continuer.

Le modèle de mappage Active Directory pour une configuration LDAPv3 mappe certains attributs et types d'enregistrements Mac OS X vers des classes d'objets et des attributs qui ne font pas partie d'un schéma Active Directory standard. Il est possible de modifier les mappages définis par le modèle ou d'étendre le schéma Active Directory. (Sinon, vous pouvez éventuellement aussi accéder à votre domaine Active Directory via le module externe Active Directory plutôt que via LDAPv3. Pour obtenir des instructions, consultez la section "Configuration de l'accès à un domaine Active Directory").

7 Lorsque la zone de dialogue se développe pour afficher des options de connexion, saisissez le nom distinctif et le mot de passe d'un compte d'utilisateur Active Directory.

8 Cliquez sur OK pour clôturer la création de la nouvelle connexion LDAP, puis sur OK pour clôturer la configuration des options LDAPv3.

Si vous avez coché la case "Utiliser pour l'authentification" ou la case "Utiliser pour les contacts" à l'étape 5, la connexion LDAPv3 vers le domaine Active Directory est ajoutée automatiquement à une politique de recherche personnalisée dans la sous-fenêtre Authentification ou Contacts de Format de répertoire.

Vous devez vous assurer que LDAPv3 est activé dans la sous-fenêtre Services afin que l'ordinateur utilise la connexion que vous venez de configurer. Pour obtenir des instructions, consultez la section "Activation ou désactivation des services de répertoires LDAP" à la page 124.

Accès à un domaine NIS

Format de répertoire vous permet de créer une configuration qui spécifie comment Mac OS X accède à un domaine NIS.

Pour créer une configuration d'accès à un domaine NIS :

1. Dans Format de répertoire, cliquez sur Services.
2. Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.
3. Sélectionnez "BSD fichier plat et NIS" dans la liste des services, puis cliquez sur Configurer.
4. Tapez le nom de domaine NIS.
5. Saisissez éventuellement le nom DNS ou l'adresse IP du serveur ou des serveurs sur lesquels se trouve le domaine NIS.

   Incluez le nom d'hôte ou l'adresse IP du serveur NIS s'il est nécessaire pour des raisons de sécurité ou si le serveur n'est pas sur le même sous-réseau que l'ordinateur que vous êtes en train de configurer.

   Si vous ne spécifiez pas de serveur, NIS utilise un protocole broadcast pour détecter un serveur NIS sur le sous-réseau.
6. Cochez la case "Utiliser le domaine NIS pour l'authentification", puis cliquez sur OK.

   Le domaine NIS est ajouté à la politique de recherche d'authentification de l'ordinateur comme /BSD/*domaine*, où *domaine* est ce que vous avez entré à l'étape 4.

Utilisation de fichiers de configuration BSD

Les ordinateurs UNIX stockent traditionnellement les données administratives dans des fichiers de configuration tels que /etc/master.passwd, /etc/group et /etc/hosts. Mac OS X est basé sur une version BSD d'UNIX, mais reçoit les données administratives normalement de systèmes de répertoire.

Dans Mac OS X versions 10.2 et ultérieures (y compris Mac OS X Server versions 10.2 et ultérieures), Open Directory peut lire des données administratives à partir de fichiers de configuration BSD. Cette fonction permet aux organisations disposant déjà de fichiers de configuration BSD d'utiliser des copies des fichiers existants sur les ordinateurs Mac OS X. Les fichiers de configuration BSD peuvent servir seuls ou avec d'autres domaines de répertoire.

Pour utiliser des fichiers de configuration BSD :

1. Assurez-vous que les fichiers de configuration BSD contiennent les données requises par les services de répertoire Mac OS X.

   Pour obtenir des instructions, consultez la section "Configuration de données dans des fichiers de configuration BSD" à la page 170.
2. Dans Format de répertoire, cliquez sur Services.

3 Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.

4 Sélectionnez "BSD fichier plat et NIS" dans la liste des services, puis cliquez sur Configurer.

5 Cochez la case "Utiliser les fichiers locaux BSD (/etc) pour l'authentification", puis cliquez sur OK.

Le domaine des fichiers de configuration BSD est ajouté à la politique de recherche d'authentification de l'ordinateur comme /BSD/local.

Mac OS X Server prend en charge un jeu fixe de fichiers de configuration BSD. Vous ne pouvez pas spécifier les fichiers de configuration à utiliser, ni mapper leur contenu vers des attributs et types d'enregistrements Mac OS X.

Configuration de données dans des fichiers de configuration BSD

Si vous voulez qu'un ordinateur Mac OS X lise des données administratives à partir de fichiers de configuration BSD, ces données doivent être présentes dans ces fichiers et doivent être au format requis par Mac OS X. Vous pouvez être amené à ajouter, modifier ou réorganiser des données dans les fichiers. Gestionnaire de groupe de travail ne pouvant modifier les données des fichiers de configuration BSD, vous devez procéder aux modifications nécessaires à l'aide d'un éditeur de texte ou d'un autre outil.

Fichier de configuration BSD	Contenu
/etc/master.passwd ;	Noms d'utilisateur, mots de passe, identifiants, identifiants de groupe principal, etc.
/etc/group ;	Noms de groupe, identifiants et membres
/etc/fstab.	Montages NFS
/etc/hosts ;	Noms et adresses d'ordinateur
/etc/networks	Noms et adresses de réseau
/etc/services	Noms de service, ports et protocoles
/etc/protocols	Noms et numéros des protocoles IP
/etc/rpcs	Serveurs RPC Open Network Computing
/etc/printcap	Noms et fonctionnalités d'imprimante
/etc/bootparams	Réglages Bootparam
/etc/bootp	Réglages Bootp
/etc/aliases	Alias et listes de distribution de courrier électronique
/etc/netgroup	Noms de groupe et membres à l'échelle du réseau

Pour obtenir des spécifications détaillées sur les données requises par les services de répertoire de Mac OS X, consultez l'annexe, "Données de répertoire Mac OS X".

Accès aux domaines NetInfo hérités

Les domaines de répertoire partagés créés à l'aide des versions de Mac OS X Server antérieures à 10.3 utilisaient le protocole NetInfo (et de manière facultative le protocole LDAPv3). Il est encore possible d'utiliser NetInfo pour accéder à ces domaines NetInfo hérités. Cela signifie que :

- Mac OS X 10.4 et Mac OS X Server 10.4 peuvent accéder à tout domaine NetInfo partagé existant.
- Tout serveur Mac OS X Server ou autre ordinateur Mac OS X peut accéder à un domaine NetInfo partagé hébergé sur un serveur qui a été mis à niveau avec Mac OS X Server version 10.4. Toutefois, un domaine NetInfo partagé d'un serveur mis à jour peut être converti au format LDAP. Les autres ordinateurs et serveurs doivent alors utiliser LDAP au lieu de NetInfo pour accéder au répertoire partagé du serveur.

Remarque : il est impossible de créer un nouveau domaine NetInfo partagé à l'aide de Mac OS X Server version 10.4, sauf si l'on utilise des utilitaires à ligne de commande. Si vous utilisez Assistant du serveur ou Admin Serveur pour configurer Mac OS X Server version 10.4 comme maître Open Directory (c'est-à-dire pour héberger un répertoire LDAP partagé), les autres ordinateurs ne pourront accéder à ce nouveau répertoire partagé qu'en utilisant LDAP.

Pour plus d'instructions sur la configuration de l'accès à un domaine NetInfo partagé, consultez les sections "À propos de la liaison NetInfo" et "Configuration d'une liaison NetInfo" à la suite de cette rubrique.

Les administrateurs système expérimentés peuvent gérer les domaines NetInfo de la manière suivante :

- Créez des enregistrements d'ordinateur pour établir une liaison broadcast vers un domaine NetInfo partagé existant. Pour obtenir des instructions, consultez la section "Ajout d'un enregistrement d'ordinateur à un domaine NetInfo parent" à la page 173.
- Configuration d'un domaine NetInfo partagé pour utiliser un numéro de port particulier plutôt qu'affecté dynamiquement. Pour obtenir des instructions, consultez la section "Configuration de ports statiques pour domaines NetInfo partagés" à la page 174.

À propos de la liaison NetInfo

Lorsqu'un ordinateur Mac OS X démarre, il peut lier son domaine de répertoire local à un domaine NetInfo partagé. Le domaine NetInfo partagé peut être lié à un autre domaine NetInfo partagé. Le processus de liaison crée une hiérarchie de domaines NetInfo.

Une hiérarchie NetInfo a une structure arborescente. Les domaines locaux situés en bas de la hiérarchie sont liés aux domaines partagés qui, à leur tour, peuvent être liés à d'autres domaines partagés, etc. Chaque domaine est lié à un seul domaine partagé, mais un domaine partagé peut être lié à plusieurs domaines. Un domaine partagé est appelé domaine *parent* et chaque domaine qui s'y lie est un domaine *enfant*. Un domaine partagé lié à aucun autre domaine se situe en haut de la structure : il s'agit du domaine root.

Un ordinateur Mac OS X peut se lier à un domaine NetInfo partagé au moyen de toute combinaison de trois protocoles : à savoir statique, Broadcast ou DHCP.

- La liaison statique permet de spécifier l'adresse et la balise NetInfo du domaine NetInfo partagé. Elle est utilisée la plupart du temps lorsque l'ordinateur du domaine partagé ne se situe pas sur le même sous-réseau IP que l'ordinateur devant y accéder.
- Avec la liaison DHCP, un serveur DHCP fournit automatiquement l'adresse et la balise NetInfo du domaine NetInfo partagé. Pour recourir à la liaison DHCP, le serveur DHCP doit être configuré en vue de fournir l'adresse et la balise d'un NetInfo parent.
- Avec la liaison Broadcast, l'ordinateur localise un domaine NetInfo partagé en envoyant une requête de diffusion IP. L'ordinateur hébergeant le domaine partagé répond avec son adresse et sa balise.
  Dans le cadre de la liaison de diffusion, les deux ordinateurs doivent se situer sur le même sous-réseau IP ou sur un réseau configuré pour le transfert de diffusion IP.

  Le domaine parent doit être doté de la balise NetInfo "réseau".

  Le domaine parent doit posséder un enregistrement d'ordinateur pour chaque ordinateur susceptible de se lier à lui via la liaison broadcast.

Si vous configurez un ordinateur en vue d'utiliser plusieurs protocoles de liaison et si un parent ne se situe pas sur l'un d'eux, un autre protocole est utilisé. Les protocoles sont utilisés dans l'ordre suivant : protocole statique, protocole DHCP, puis protocole Broadcast.

Configuration d'une liaison NetInfo

Format de répertoire vous permet de configurer Mac OS X ou Mac OS X Server pour se lier à un domaine NetInfo parent en utilisant une combinaison quelconque des protocoles statique, broadcast ou DHCP. L'ordinateur tente de se lier à un domaine NetInfo parent lorsqu'il démarre.

Remarque : si votre réseau ne possède pas de domaine NetInfo partagé, la configuration d'un ordinateur pour se lier à un domaine NetInfo parent ralentit le démarrage de l'ordinateur.

Important : si vous configurez Mac OS X pour qu'il utilise une politique de recherche automatique d'authentification et un serveur LDAP fourni par DHCP ou un domaine NetInfo fourni par DHCP, vous augmenterez le risque de voir un utilisateur malveillant prendre le contrôle de votre ordinateur. Le risque est encore plus élevé si votre ordinateur est configuré pour se connecter à réseau un sans fil. Pour plus de détails, consultez la section "Protection d'ordinateurs contre un serveur DHCP malveillant" à la page 130.

Pour lier un ordinateur Mac OS X à un domaine NetInfo partagé :

1. Dans Format de répertoire, cliquez sur Services.
2. Si l'icône représentant le cadenas est verrouillée, cliquez dessus et tapez le nom et le mot de passe d'un administrateur.
3. Sélectionnez NetInfo dans la liste des services, puis cliquez sur Configurer.

4 Sélectionnez les protocoles de liaison devant être utilisés par l'ordinateur.

- Pour la liaison de diffusion, sélectionnez l'option Se connecter avec le protocole Broadcast.
- Pour la liaison DHCP, sélectionnez l'option Se connecter avec le protocole DHCP.
- Pour la liaison statique, sélectionnez l'option Se connecter à un serveur NetInfo particulier. Tapez ensuite l'adresse IP de l'ordinateur de domaine parent dans le champ Adresse du serveur et la balise NetInfo du domaine parent dans le champ Balise du serveur.

5 Cliquez sur OK, puis sur Appliquer.

6 Redémarrez l'ordinateur.

7 Si vous avez sélectionné le protocole de liaison DHCP pour NetInfo à l'étape 4, assurez-vous que le serveur DHCP est configuré pour fournir l'adresse et la balise NetInfo du domaine NetInfo partagé.

8 Si vous avez sélectionné le protocole de liaison Broadcast pour NetInfo à l'étape 4, assurez-vous que le domaine NetInfo parent dispose bien d'un enregistrement d'ordinateur pour l'ordinateur que vous êtes en train de configurer.

Pour obtenir des instructions, consultez la section "Ajout d'un enregistrement d'ordinateur à un domaine NetInfo parent" (ci-après).

Ajout d'un enregistrement d'ordinateur à un domaine NetInfo parent

Les ordinateurs Mac OS X peuvent lier leurs domaines de répertoire à un domaine NetInfo parent à l'aide de la liaison broadcast. Le domaine NetInfo parent doit posséder un enregistrement d'ordinateur pour chaque ordinateur Mac OS X pouvant se lier à lui par liaison broadcast. Vous pouvez créer une fiche d'ordinateur grâce à l'application Gestionnaire NetInfo.

Ajout d'un enregistrement d'ordinateur à un domaine NetInfo parent

1 Ouvrez Gestionnaire NetInfo sur l'ordinateur hébergeant le domaine parent, puis ouvrez le domaine.

2 Cliquez sur le cadenas et authentifiez-vous à l'aide du nom et du mot de passe d'un administrateur du domaine de répertoire.

3 Sélectionnez le répertoire "ordinateurs" dans la liste de l'explorateur de répertoires.

4 Dans le menu Répertoire, choisissez Nouveau sous-répertoire.

5 Double-cliquez sur nouveau_rép dans la liste du bas, puis saisissez le nom DNS de l'ordinateur enfant.

6 Dans le menu Répertoire, choisissez Nouvelle propriété.

7 Dans la liste du bas, changez nouvelle_propriété par adresse_ip et nouvelle_valeur par l'adresse IP de l'ordinateur enfant.

8 Dans le menu Répertoire, choisissez Nouvelle propriété.

9 Remplacez nouvelle_propriété par "serves" et nouvelle_valeur par le nom et la balise NetInfo du domaine local de l'enfant, en insérant une barre oblique (/) entre le nom et la balise.

Par exemple, changez nouvelle_valeur par marketing.demo/local pour le domaine local de l'ordinateur nommé marketing.demo.

10 Choisissez Enregistrer les modifications dans le menu Domaine, puis cliquez sur l'option Mettre à jour cette copie.

Configuration de ports statiques pour domaines NetInfo partagés

Par défaut, Mac OS X sélectionne de manière dynamique un port dans la plage 600 à 1023 lorsqu'il accède à un domaine NetInfo partagé. Vous pouvez configurer un domaine partagé pour l'accès NetInfo à des ports spécifiques. Pour ce faire, recourez à l'application Gestionnaire NetInfo.

Pour configurer des ports spécifiques en vue d'un accès NetInfo à des domaines partagés :

1 Ouvrez Gestionnaire NetInfo sur l'ordinateur hébergeant le domaine partagé, puis ouvrez le domaine.

2 Cliquez sur le cadenas et authentifiez-vous à l'aide du nom et du mot de passe d'un administrateur du domaine de répertoire.

3 Sélectionnez la barre oblique "/" pour parcourir.

4 Pour changer la valeur d'une propriété de port existant, double-cliquez sur la valeur située dans la colonne Valeur(s), puis apportez votre modification.

5 Pour supprimer une propriété de port, sélectionnez-la, puis choisissez Supprimer dans le menu Modifier.

6 Pour ajouter une propriété, choisissez Nouvelle propriété dans le menu Répertoire, puis procédez de la manière suivante :

- Pour utiliser un même port pour les paquets TCP et UDP, double-cliquez sur nouvelle_propriété et remplacez cette valeur par "port". Changez ensuite nouvelle_valeur par le numéro de port souhaité.
- Pour disposer de ports TCP et UDP séparés, double-cliquez sur nouvelle_propriété, puis remplacez cette valeur par tcp_port. Changez ensuite nouvelle_valeur par le numéro de port TCP souhaité. Double-cliquez ensuite sur nouvelle_propriété, puis modifiez cette valeur par port_udp. Cette fois, remplacez nouvelle_valeur par le numéro de port UDP souhaité.

Maintenance et résolution des problèmes

8

Vous pouvez contrôler les services Open Directory, afficher et modifier les données brutes des domaines Open Directory et effectuer une sauvegarde des fichiers Open Directory. Vous pouvez aussi résoudre certains problèmes courants concernant Open Directory.

Parmi les tâches régulières de gestion et de dépannage des services Open Directory que vous serez amené à effectuer, vous trouverez les suivantes :

Contrôle de l'accès aux serveurs Open Directory

Vous pouvez contrôler l'accès à un maître ou à une réplique Open Directory en contrôlant quelles personnes peuvent se connecter à l'aide de la fenêtre de connexion ou de l'outil de ligne de commande `ssh`. Pour obtenir des instructions, consultez les sections suivantes :

Contrôle de l'accès à la fenêtre de connexion d'un serveur

Vous pouvez utiliser Admin Serveur pour contrôler quels utilisateurs peuvent se connecter à Mac OS X Server à l'aide de la fenêtre de connexion. Les utilisateurs disposant d'autorisations d'administrateur de serveur sont toujours autorisés à se connecter au serveur.

Pour restreindre l'utilisation de la fenêtre de connexion sur un serveur :

1. Ouvrez Admin Serveur, connectez-vous au serveur sur lequel vous souhaitez contrôler l'accès à la fenêtre de connexion et sélectionnez le serveur dans la liste Ordinateurs et services.

   Sélectionnez le serveur, et non un service sous le serveur.
2. Cliquez sur Réglages, puis sur Accès.
3. Désélectionnez la case "Utiliser le même accès pour tous les services" et sélectionnez "Fenêtre d'ouverture de session" dans la liste de gauche.
4. Cochez la case "Autoriser uniquement les utilisateurs et groupes ci-dessous" et modifiez la liste des utilisateurs et des groupes que vous souhaitez autoriser à se connecter à l'aide de la fenêtre de connexion du serveur.
   - Ajoutez les utilisateurs et/ou groupes qui peuvent utiliser la fenêtre de connexion en cliquant sur le bouton Ajouter (+) et en fournissant les informations requises.
   - Supprimez des utilisateurs ou des groupes de la liste en en sélectionnant un ou plusieurs, puis en cliquant sur le bouton Supprimer (–).
5. Cliquez sur Enregistrer.

Si la case "Autoriser tous les utilisateurs et groupes" est cochée lorsque vous désélectionnez "Utiliser le même accès pour tous les services" à l'étape 3, tous les services à l'exception de la fenêtre de connexion autoriseront l'accès à tous les utilisateurs et groupes. Si vous souhaitez restreindre l'accès à un service énuméré dans la liste en plus de la fenêtre de connexion, sélectionnez le service dans la liste, cochez la case "Autoriser uniquement les utilisateurs et groupes ci-dessous" et ajoutez des utilisateurs et/ou groupes à la liste des utilisateurs et groupes.

Si vous souhaitez que tous les utilisateurs puissent se connecter à l'aide de la fenêtre de connexion du serveur, sélectionnez Fenêtre d'ouverture de session, puis cochez la case "Autoriser tous les utilisateurs et groupes".

Contrôle de l'accès au service SSH

Vous pouvez utiliser Admin Serveur pour contrôler les utilisateurs qui peuvent ouvrir une connexion par la ligne de commande à Mac OS X Server à l'aide de la commande `ssh` dans Terminal. Les utilisateurs disposant d'autorisations d'administrateur de serveur sont toujours autorisés à se connecter au serveur à l'aide de la commande `ssh`. La commande ssh utilise le service Secure Shell (SSH). Pour en savoir plus sur l'utilisation de la commande `ssh`, consultez le guide de l'administration en ligne de commande.

Pour restreindre l'ouverture d'une connexion SSH à un serveur distant :

1. Ouvrez Admin Serveur, connectez-vous au serveur sur lequel vous souhaitez contrôler l'accès SSH et sélectionnez le serveur dans la liste Ordinateurs et services.

   Sélectionnez le serveur, et non un service sous le serveur.
2. Cliquez sur Réglages, puis sur Accès.
3. Désélectionnez la case "Utiliser le même accès pour tous les services" et sélectionnez SSH dans la liste de gauche.

4 Cochez la case "Autoriser uniquement les utilisateurs et groupes ci-dessous" et modifiez la liste des utilisateurs et des groupes que vous souhaitez autoriser à ouvrir une connexion SSH au serveur.

- Ajoutez les utilisateurs et/ou groupes qui peuvent ouvrir des connexions SSH en cliquant sur le bouton Ajouter (+) et en fournissant les informations requises.
- Supprimez des utilisateurs ou des groupes de la liste en en sélectionnant un ou plusieurs, puis en cliquant sur le bouton Supprimer (–).

5 Cliquez sur Enregistrer.

Si la case "Autoriser tous les utilisateurs et groupes" est cochée lorsque vous désélectionnez "Utiliser le même accès pour tous les services" à l'étape 3, tous les services à l'exception de SSH autorisent l'accès à tous les utilisateurs et groupes. Si vous souhaitez restreindre l'accès à un service énuméré dans la liste en plus de SSH, sélectionnez le service dans la liste, cochez la case "Autoriser uniquement les utilisateurs et groupes ci-dessous" et ajoutez des utilisateurs et/ou groupes à la liste des utilisateurs et groupes.

Si vous souhaitez que tous les utilisateurs puissent ouvrir une connexion SSH avec le serveur, sélectionnez SSH, puis cochez la case "Autoriser tous les utilisateurs et groupes".

Contrôle d'Open Directory

Vous pouvez afficher les états et les historiques d'Open Directory. Vous pouvez également examiner les historiques d'authentification Open Directory pour y chercher des traces d'activités suspectes.

Pour obtenir des instructions, consultez les sections suivantes :

- "Contrôle de l'état d'un maître ou d'une réplique Open Directory" (ci-après).
- "Contrôle des répliques d'un maître Open Directory" à la page 178.
- "Affichage des états et des historiques Open Directory" à la page 178.
- "Contrôle de l'authentification Open Directory" à la page 178.

Contrôle de l'état d'un maître ou d'une réplique Open Directory

Vous pouvez confirmer que le maître Open Directory fonctionne correctement.

1 Ouvrez Admin Serveur et sélectionnez Open Directory pour un serveur dans la liste Ordinateurs et services.

2 Cliquez sur Aperçu (dans le bas de la fenêtre).

3 Assurez-vous que l'état de tous les éléments listés dans la sous-fenêtre d'aperçu Open Directory est bien "En service".

Si l'un ou l'autre élément listé est arrêté, cliquez sur Réactualiser (ou choisissez Présentation > Réactualiser). Si Kerberos reste arrêté, consultez la section "Kerberos est arrêté sur un maître ou une réplique Open Directory" à la page 188.

Contrôle des répliques d'un maître Open Directory

Grâce à Admin Serveur, vous pouvez contrôler l'état de la création de répliques et de la réplication en cours.

Pour contrôler les répliques d'un maître Open Directory :

1. Ouvrez Admin Serveur sélectionnez Open Directory pour le maître dans la liste Ordinateurs et services.
2. Cliquez sur Réglages pour afficher la liste des répliques et l'état de chacune d'entre elles.

   L'état d'une nouvelle réplique indique si sa création a réussi. Ensuite, l'état indique si la dernière tentative de réplication a réussi.

Affichage des états et des historiques Open Directory

Vous pouvez utiliser l'application Admin Serveur pour afficher les informations d'état et les historiques des services Open Directory. Les historiques suivants sont disponibles :

- Historique du serveur de services de répertoires
- Historique des erreurs des services de répertoires
- Historique `kadmin`
- Historique `kdc`
- Historique lookupd
- Historique NetInfo
- Historique LDAP
- Historique du serveur du service de mot de passe
- Historique des erreurs du service de mot de passe
- Historique de réplication du service de mot de passe
- Historique `slapconfig`

Pour visualiser des historiques ou des états de services de répertoires :

1. Ouvrez Admin Serveur et sélectionnez Open Directory pour un des serveurs de la liste Ordinateurs et services.
2. Cliquez sur Vue d'ensemble pour afficher les informations d'état.
3. Cliquez sur Historiques et utilisez le menu local Afficher pour choisir l'historique que vous souhaitez consulter.

   Le chemin au fichier d'historique est affiché sous le menu local.
4. Accessoirement, vous pouvez aussi saisir du texte dans le champ Filtre et appuyer sur Retour pour n'afficher que les lignes contenant le texte que vous avez saisi.

Contrôle de l'authentification Open Directory

Vous pouvez utiliser les historiques du service de mot de passe, visibles à l'aide d'Admin Serveur, pour contrôler les tentatives de connexion ayant échoué et identifier ainsi les activités suspectes.

Open Directory consigne l'ensemble des échecs d'authentification, y compris les adresses IP qui les ont générés. Réexaminez régulièrement les historiques afin de déterminer s'il existe un grand nombre de tentatives infructueuses pour un même identifiant de mot de passe, ce qui indiquerait qu'une personne est peut-être en train d'essayer de deviner des mots de passe.

Pour afficher les historiques d'authentification Open Directory :

1. Ouvrez Admin Serveur et sélectionnez Open Directory pour un des serveurs de la liste Ordinateurs et services.
2. Cliquez sur Historiques, puis choisissez l'historique `kdc` ou un historique du service de mot de passe dans le menu local Afficher.

Affichage et modification directs des données de répertoire

Vous pouvez afficher ou modifier les données de répertoire brutes à l'aide de l'Inspecteur dans Gestionnaire de groupe de travail. L'Inspecteur vous permet d'afficher les données de répertoires qui ne sont pas visibles dans Gestionnaire de groupe de travail. L'Inspecteur vous permet en outre de modifier des données de répertoire que vous ne pouvez pas modifier dans Gestionnaire de groupe de travail. Vous pouvez, par exemple, utiliser l'Inspecteur pour modifier le nom abrégé d'un utilisateur.

Pour obtenir des instructions, consultez les sections :

- "Affichage de l'Inspecteur de répertoire" à la page 179.
- "Masquage de l'inspecteur de répertoire" à la page 180.
- "Modification du nom abrégé d'un utilisateur" à la page 180.
- "Suppression d'enregistrements" à la page 181.

Affichage de l'Inspecteur de répertoire

Vous pouvez afficher l'Inspecteur dans Gestionnaire de groupe de travail en sélectionnant une option dans les Préférences de Gestionnaire de groupe de travail. Vous pouvez ensuite accéder à l'Inspecteur pour visualiser ou modifier des données de répertoire brutes.

> ***Avertissement :*** la modification de données de répertoire brutes peut avoir des conséquences imprévisibles et indésirables. Vous pourriez involontairement désactiver un utilisateur ou un ordinateur ou autoriser les utilisateurs à accéder à un nombre plus élevé de ressources que prévu.

Pour afficher l'Inspecteur :

1. Ouvrez Gestionnaire de groupe de travail et choisissez Gestionnaire de groupe de travail > Préférences.
2. Sélectionnez "Afficher l'inspecteur et l'onglet Toutes les fiches", puis cliquez sur OK.

3 Pour afficher les attributs d'utilisateur, de groupe ou de liste d'ordinateurs, cliquez sur le bouton Utilisateurs, Groupe ou Listes des ordinateurs (à gauche), puis sur Inspecteur (à droite).

4 Pour afficher d'autres types d'enregistrements, cliquez sur le bouton Toutes les fiches, à côté du bouton Listes des ordinateurs, puis choisissez un type de fiche dans le menu local situé en haut de la liste.

Le menu local affiche tous les types d'enregistrement standard qui existent dans le domaine de répertoire. Vous pouvez également choisir Natif dans le menu local, puis saisir le nom d'un type d'enregistrement natif dans le champ qui apparaît sous le menu local. La liste affiche tous les enregistrements, y compris les enregistrements prédéfinis, du type d'enregistrement actuellement sélectionné.

Masquage de l'inspecteur de répertoire

Si l'Inspecteur est visible dans Gestionnaire de groupe de travail, vous pouvez le masquer en modifiant une option dans les Préférences de Gestionnaire de groupe de travail.

Pour masquer l'Inspecteur :

1 Ouvrez Gestionnaire de groupe de travail et choisissez Gestionnaire de groupe de travail > Préférences.

2 Désélectionnez "Afficher l'inspecteur et l'onglet Toutes les fiches", puis cliquez sur OK.

Modification du nom abrégé d'un utilisateur

Vous pouvez utiliser l'Inspecteur de Gestionnaire de groupe de travail pour modifier le ou les noms abrégés d'un utilisateur, y compris son premier nom abrégé.

Avertissement : la modification du nom abrégé d'un utilisateur peut avoir des conséquences inattendues et indésirables. D'autres services utilisent le nom abrégé des utilisateurs pour les identifier de manière unique et persistante. Ainsi, la modification du nom abrégé d'un utilisateur n'affecte pas le nom de son répertoire de départ. L'utilisateur dispose du même répertoire de départ (bien que le nom de ce dernier ne corresponde plus au nouveau nom abrégé de l'utilisateur) sauf s'il accède à son répertoire de départ par l'intermédiaire d'une appartenance à un groupe.

Pour modifier le nom abrégé d'un compte d'utilisateur :

1 Ouvrez Gestionnaire de groupe de travail et affichez l'Inspecteur s'il est masqué.

2 Cliquez sur le bouton Comptes, puis sur le bouton Utilisateurs.

3 Ouvrez le domaine de répertoire contenant le compte d'utilisateur dont vous voulez changer le nom abrégé, puis authentifiez-vous en tant qu'administrateur du domaine.

Pour ouvrir un domaine de répertoire, cliquez sur l'icône de globe au-dessus de la liste des utilisateurs, puis choisissez un domaine dans le menu local.

4 Sélectionnez le compte dont vous voulez changer le nom abrégé, puis cliquez sur Inspecteur (à droite).

5 Trouvez RecordName dans la liste des attributs ; si un triangle est visible à côté de RecordName, cliquez dessus pour afficher toutes les valeurs de RecordName.

L'attribut RecordName stocke le ou les noms abrégés de l'utilisateur.

6 Double-cliquez sur la valeur RecordName correspondant au nom abrégé que vous souhaitez changer, puis saisissez un autre nom abrégé et appuyez sur la touche Retour.

Vous pouvez aussi cliquer sur une valeur RecordName, puis cliquer sur Modifier pour modifier la valeur dans une fenêtre de modification.

7 Cliquer sur Enregistrer.

Définition de contrôles d'accès aux répertoires (DAC, Directory Access Controls)

Open Directory permet de définir des contrôles d'accès aux répertoires (DAC) pour toutes les parties du répertoire LDAP, fournissant ainsi un contrôle précis de qui peut modifier quoi. Open Directory stocke les contrôles d'accès aux répertoires dans un enregistrement apple-acl que vous pouvez modifier à l'aide de l'Inspecteur dans Gestionnaire de groupe de travail.

Pour changer les contrôles d'accès aux répertoires :

1 Ouvrez Gestionnaire de groupe de travail et affichez l'Inspecteur s'il est masqué.

2 Ouvrez le domaine de répertoire pour lequel vous souhaitez définir des contrôles d'accès et authentifiez-vous comme administrateur du domaine.

Pour ouvrir un domaine de répertoire, cliquez sur l'icône de globe au-dessus de la liste des utilisateurs, puis choisissez un domaine dans le menu local.

3 Cliquez sur le bouton Toutes les fiches (près du bouton Listes des ordinateurs), puis choisissez AccessControls dans le menu local au-dessus de la liste.

4 Sélectionnez "Par défaut" dans la liste des enregistrements.

5 Trouvez AccessControlEntry dans la liste des attributs ; si un triangle est visible à côté de AccessControlEntry, cliquez dessus pour afficher toutes les entrées de contrôle d'accès.

6 Sélectionnez AccessControlEntry, puis cliquez sur Modifier pour changer la valeur ou cliquez sur Nouvelle valeur pour ajouter une valeur AccessControlEntry.

Vous pouvez aussi double-cliquer sur une valeur pour la modifier.

7 Cliquer sur Enregistrer.

Suppression d'enregistrements

Vous pouvez utiliser l'Inspecteur dans Gestionnaire de groupe de travail pour supprimer des enregistrements de tous types.

> ***Avertissement :*** la suppression d'enregistrements peut provoquer un comportement désordonné du serveur ou son arrêt. Ne supprimez pas un enregistrement avant d'être sûr qu'il n'est pas requis pour le bon fonctionnement du serveur.

Pour supprimer des enregistrements avec l'Inspecteur :

1. Ouvrez Gestionnaire de groupe de travail et affichez l'Inspecteur s'il est masqué.
2. Ouvrez le domaine de répertoire dans lequel vous souhaitez supprimer des enregistrements et authentifiez-vous comme administrateur du domaine.

   Pour ouvrir un domaine de répertoire, cliquez sur l'icône de globe au-dessus de la liste des utilisateurs, puis choisissez un domaine dans le menu local.
3. Cliquez sur le bouton Toutes les fiches (près du bouton Listes des ordinateurs), puis choisissez le type d'enregistrement souhaité dans le menu local au-dessus de la liste.
4. Sélectionnez le ou les enregistrements à supprimer dans la liste des enregistrements.
5. Cliquez sur Supprimer (ou choisissez Serveur > Supprimer les fiches sélectionnées).

Importation d'enregistrements de tous types

Gestionnaire de groupe de travail peut importer tous les types d'enregistrements dans le répertoire LDAP d'un maître Open Directory. Cela couvre les utilisateurs, les groupes, les listes d'ordinateurs, les ordinateurs et tous les autres types d'enregistrements Mac OS X standard. Pour obtenir des informations sur les types d'enregistrements et les attributs les plus courants, consultez la section "Types d'enregistrements et attributs Open Directory standard" à la page 236.

Pour obtenir une liste des types d'enregistrements et des attributs qui peuvent être importés, consultez le fichier suivant :

/System/Library/Frameworks/DirectoryService.framework/Headers/DirServicesConst.h

Pour obtenir des instructions sur l'importation d'enregistrements de tous types, consultez le guide de gestion des utilisateurs.

Gestion de la réplication Open Directory

Vous pouvez planifier la réplication Open Directory ou répliquer à la demande, promouvoir une réplique en maître ou mettre une réplique hors service. Pour obtenir des instructions, consultez les sections :

- "Planification de la réplication d'un maître Open Directory" (ci-après).
- "Synchronisation d'une réplique Open Directory à la demande" à la page 183.
- "Promotion d'une réplique Open Directory" à la page 183.
- "Mise hors service d'une réplique Open Directory" à la page 185.

Planification de la réplication d'un maître Open Directory

A l'aide d'Admin Serveur, vous pouvez spécifier la fréquence avec laquelle le maître Open Directory met à jour ses répliques en y intégrant les modifications apportées aux répertoires et aux informations d'authentification. Le maître peut mettre à jour les répliques soit dès qu'une modification a lieu dans son domaine de répertoire, soit en fonction d'un calendrier que vous définissez.

Pour indiquer la fréquence de la mise à jour des répliques par le maître Open Directory :

1. Ouvrez Admin Serveur et sélectionnez Open Directory pour un serveur maître Open Directory dans la liste des Ordinateurs et services.
2. Cliquez sur Réglages (vers le bas de la fenêtre), puis cliquez sur Général (vers le haut).
3. Spécifiez une fréquence de duplication.

   "Répliquer vers les clients chaque fois que le répertoire est modifié :" garde les répliques à jour, mais augmente la charge sur le réseau. Peut affecter les performances du maître si une réplique est connectée via une liaison réseau lente.

   "Répliquer vers les clients tous/toutes les__ :" permet de planifier des mises à jour moins fréquentes (en spécifiant un intervalle plus long). Les mises à jour moins fréquentes présentent l'inconvénient de générer des répliques moins exactes mais offrent l'avantage de réduire le nombre de connexions réseau entre le maître et ses répliques. La réduction des connexions peut s'avérer souhaitable si les répliques ne font pas toutes partie du même réseau local que le maître.
4. Cliquer sur Enregistrer.

Synchronisation d'une réplique Open Directory à la demande

Bien qu'un maître Open Directory synchronise automatiquement ses données de répertoire et d'authentification avec les répliques enregistrées, vous pouvez utiliser Admin Serveur pour synchroniser les données avec une réplique sélectionnée à la demande.

Pour synchroniser une réplique Open Directory à la demande :

1. Ouvrez Admin Serveur et sélectionnez Open Directory pour un serveur maître Open Directory dans la liste des Ordinateurs et services.
2. Cliquez sur Réglages (vers le bas de la fenêtre), puis cliquez sur Général (vers le haut).
3. Sélectionnez une réplique dans la liste, puis cliquez sur Répliquer.

Promotion d'une réplique Open Directory

Si un maître Open Directory tombe en panne et que vous ne pouvez pas le récupérer à partir d'une copie de sauvegarde, vous pouvez transformer une réplique en maître. Le maître ainsi promu utilise le répertoire et les bases de données d'authentification existantes de la réplique. Une fois que c'est fait, vous devez convertir toutes les autres répliques de l'ancien maître en serveurs autonomes, puis en faire des répliques du nouveau maître.

Important : n'utilisez cette procédure que pour remplacer un maître Open Directory par sa réplique. Si vous souhaitez garder le maître Open Directory en service et faire de sa réplique un autre maître, n'utilisez pas cette procédure. Mettez plutôt le réplique hors service, puis transformez-la en maître comme décrit dans les sections "Mise hors service d'une réplique Open Directory" à la page 185 et "Configuration d'un maître Open Directory" à la page 83.

Pour promouvoir une réplique Open Directory :

1. Dans Admin Serveur, connectez-vous à la réplique que vous souhaitez promouvoir en tant que maître et sélectionnez Open Directory pour ce serveur dans la liste Ordinateurs et services.
2. Cliquez sur Réglages (vers le bas de la fenêtre), puis sur Général (vers le haut).
3. Sélectionnez Maître Open Directory dans le menu local Rôle et saisissez les informations demandées.
   - "*Nom abrégé de l'administrateur du domaine :*" le nom abrégé d'un administrateur du domaine de répertoire LDAP du serveur.
   - "*Mot de passe de l'administrateur du domaine :*" le mot de passe du compte d'administrateur dont vous avez saisi le nom abrégé.
4. Cliquez sur OK, puis sur Enregistrer.
5. Dans Admin Serveur, connectez-vous à une autre réplique de l'ancien maître et sélectionnez Open Directory pour ce serveur dans la liste Ordinateurs et services.
6. Cliquez sur Réglages, puis sur Général.
7. Choisissez Autonome dans le menu local Rôle, puis cliquez sur Enregistrer.
8. Sélectionnez Réplique Open Directory dans le menu local Rôle et saisissez les informations demandées.
   - "*Adresse IP du maître Open Directory :*" saisissez l'adresse IP du serveur qui est le nouveau maître Open Directory.
   - "*Mot de passe root sur maître Open Directory :*" saisissez le mot de passe de l'utilisateur root du système du nouveau maître Open Directory (nom d'utilisateur de l'administrateur système).
   - "*Nom abrégé de l'administrateur de domaine sur le maître :*" saisissez le nom d'un administrateur de domaine de répertoire LDAP.
   - "*Mot de passe de l'administrateur de domaine sur le maître :*" saisissez le mot de passe de l'administrateur de domaine dont vous avez saisi le nom.
9. Cliquez sur OK, puis sur Enregistrer.
10. Répétez les étapes 5 – 9 pour chaque réplique supplémentaire de l'ancien maître.
11. Assurez-vous que la date, l'heure et le fuseau horaire sont exacts sur les répliques et sur le maître.

Les répliques et le maître doivent utiliser le même service d'horloge de réseau pour que leurs horloges restent synchronisées.

Si d'autres ordinateurs sont connectés au domaine LDAP de l'ancien maître Open Directory, vous devez reconfigurer leurs connexions pour qu'elles utilisent le répertoire LDAP du nouveau maître :

- Chaque ordinateur Mac OS X et Mac OS X Server disposant d'une politique de recherche personnalisée qui contenait le répertoire LDAP de l'ancien maître doit être reconfiguré pour se connecter au répertoire LDAP du nouveau maître. Utilisez les sous-fenêtres Services et Authentification de Format de répertoire. Pour obtenir des instructions, consultez les sections "Suppression d'une configuration pour l'accès à un répertoire LDAP" à la page 140 et "Configuration de l'accès à un répertoire LDAP" à la page 133.
- Si le service DHCP fournissait l'URL LDAP de l'ancien maître aux ordinateurs disposant de politiques de recherche automatique, vous devez reconfigurer le service DHCP pour qu'il fournisse l'URL LDAP du nouveau maître. Les ordinateurs Mac OS X et Mac OS X Server disposant de politiques de recherche automatique ne requièrent pas de reconfiguration ; ils recevront l'URL LDAP correcte du service DHCP mis à jour à leur prochain démarrage. Consultez le chapitre consacré au DHCP dans le guide d'administration de services réseau.

Mise hors service d'une réplique Open Directory

Vous pouvez mettre une réplique Open Directory hors service en la transformant en un serveur autonome ou en vous connectant à un autre système pour les services de répertoire et d'authentification.

Pour mettre hors service une réplique Open Directory :

1. Vérifiez que la connexion réseau fonctionne entre le maître Open Directory et la réplique à mettre hors service.

   Le port 389 ou 636 doit être ouvert entre le maître et la réplique pendant la mise hors service de la réplique. LDAP utilise le port 389 si SSL est désactivé ou le port 636 si SSL est activé sur le maître. (Le port 22, utilisé pour SSH, ne doit pas être ouvert pour mettre hors service une réplique).

   Important : si vous mettez une réplique hors service alors qu'il n'y a pas de connectivité réseau entre la réplique et le maître, la réplique mise hors service restera dans la liste de répliques du maître. De plus, le maître tentera de répliquer vers la réplique mise hors service spécifiée dans la sous-fenêtre de réglages Général pour le service Open Directory sur le serveur maître.

2. Dans Admin Serveur, connectez-vous à la réplique à mettre hors service en et sélectionnez Open Directory pour ce serveur dans la liste Ordinateurs et services.
3. Cliquez sur Réglages (vers le bas de la fenêtre), puis cliquez sur Général (vers le haut).

4 Cliquez sur le menu local Rôle et choisissez Serveur autonome ou "Connecté à un système de répertoire" et saisissez les informations requises.

- *"Nom abrégé de l'administrateur de domaine :"* le nom abrégé d'un administrateur du répertoire LDAP du maître Open Directory.
- *"Mot de passe de l'administrateur de domaine :"* le mot de passe du compte d'administrateur dont vous avez saisi le nom abrégé.
- *"Mot de passe root sur maître Open Directory :"* saisissez le mot de passe de l'utilisateur root du système du maître Open Directory (nom d'utilisateur de l'administrateur système).

5 Cliquez sur OK, puis sur Enregistrer.

En supposant qu'il y ait une connexion réseau entre le maître Open Directory et la réplique, le maître est mis à jour pour ne plus se connecter à la réplique.

6 Si vous choisissez "Connecté à un système de répertoire" dans le menu local Rôle, cliquez sur le bouton Ouvrir Format de répertoire pour configurer l'accès à un ou plusieurs systèmes de répertoire.

Pour obtenir des instructions sur la configuration de l'accès à un type particulier de service de répertoire, consultez le chapitre 7, "Gestion de Format de répertoire".

Archivage d'un maître Open Directory

Vous pouvez utiliser Admin Serveur pour archiver une copie de données de répertoire et d'authentification d'un maître Open Directory. Vous pouvez archiver une copie des données pendant que le maître Open Directory est en service.

Les fichiers suivants sont archivés :

- Base de données de répertoires et fichiers de configuration LDAP
- Base de données du serveur de mots de passe Open Directory
- Base de données et fichiers de configuration Kerberos
- Domaine NetInfo local et base de données de mots de passe shadow

Si vous disposez d'une archive fiable d'un maître Open Directory, vous disposez de fait d'une archive de toutes ses répliques. En cas de problèmes avec une réplique, vous pouvez simplement lui donner un rôle Open Directory de serveur autonome. Configurez ensuite le serveur comme s'il s'agissait d'un nouveau serveur, en lui donnant un nouveau nom d'hôte, puis configurez-le comme une copie du même maître qu'auparavant.

Important : protégez soigneusement le support d'archivage qui contient une copie de la base de données de mots de passe Open Directory, de la base de données Kerberos et du fichier keytab de Kerberos. Cette archive contient les mots de passe de tous les utilisateurs qui possèdent un mot de passe Open Directory, tant dans le domaine de répertoire LDAP partagé que dans le domaine de répertoire NetInfo local. Les mesures de sécurité que vous prenez pour le support d'archivage doivent être aussi strictes que celles prises pour le serveur maître Open Directory.

Pour archiver un maître Open Directory :

1. Ouvrez Admin Serveur et la liste Ordinateurs et services, puis sélectionnez Open Directory pour un serveur maître Open Directory.
2. Cliquez sur Archiver (au bas de la fenêtre).
3. Saisissez le chemin au dossier dans lequel vous souhaitez archiver les données Open Directory, puis cliquez sur le bouton Archiver.

   Vous pouvez taper le chemin au dossier ou cliquer sur le bouton Parcourir (•••) pour le sélectionner.
4. Saisissez le nom et le mot de passe à utiliser pour crypter l'archive, puis cliquez sur OK.

Restauration d'un maître Open Directory

Vous pouvez utiliser Admin Serveur pour restaurer des données de répertoire et d'authentification d'un maître Open Directory à partir d'une archive. Les fichiers suivants sont restaurés :

- Base de données de répertoires et fichiers de configuration LDAP
- Base de données du serveur de mots de passe Open Directory
- Base de données et fichiers de configuration Kerberos
- Domaine NetInfo local et base de données de mots de passe shadow

Restaurer une archive en serveur autonome Open Directory en fait un maître Open Directory avec les mêmes données que le maître à partir duquel l'archive a été créée.

Restaurer une archive en serveur Open Directory fusionne les données de l'archive avec les données du maître existantes. Si des conflits surviennent pendant la fusion, l'enregistrement existant prime sur les données de l'archive ; l'enregistrement de l'archive est ignoré. Les conflits sont consignés dans le fichier d'historique slapconfig (/Library/Logs/slapconfig.log), que vous pouvez visionner à l'aide d'Admin Serveur. Consultez la section "Affichage des états et des historiques Open Directory" à la page 178.

Plutôt que de restaurer un maître Open Directory à partir d'une archive, vous pouvez obtenir de meilleurs résultats en transformant une réplique en maître. Il se peut en effet que la réplique ait des données de répertoire et d'authentification plus récentes que l'archive.

Après avoir restauré un maître Open Directory à partir d'une archive, vous devez recréer les répliques Open Directory.

Important : il ne faut pas utiliser le restauration d'une archive comme un moyen de porter des données de répertoire et d'authentification d'un système à un autre. Exportez plutôt les données du répertoire source et importez-les dans le répertoire cible. Pour plus d'informations sur l'exportation et l'importation de données de répertoire, consultez le guide de gestion des utilisateurs.

Pour restaurer un maître Open Directory à partir d'une archive :

1. Ouvrez Admin Serveur, puis, dans la liste Ordinateurs et services, sélectionnez Open Directory pour un serveur autonome Open Directory ou pour un serveur maître Open Directory.

   Si vous sélectionnez un serveur autonome Open Directory comme cible d'une opération de restauration, le serveur deviendra un maître Open Directory avec les données de répertoire et d'authentification que contient l'archive.

   Si vous sélectionnez un serveur maître Open Directory comme cible d'une opération de restauration, les données de répertoire et d'authentification que contient l'archive sont fusionnées avec les données de répertoire et d'authentification de la cible. Le serveur cible doit porter le même nom de royaume Kerberos que le maître à partir duquel l'archive a été créée.

2. Cliquez sur Archiver (dans le bas de la fenêtre).

3. Saisissez le chemin au fichier d'archive Open Directory, puis cliquez sur le bouton Restaurer.

   Vous pouvez taper le chemin ou cliquer sur le bouton Parcourir (•••) pour sélectionner le fichier d'archive.

4. Saisissez le mot de passe qui a été utilisé pour crypter l'archive lorsqu'elle a été créée, puis cliquez sur OK.

5. Convertissez tous les serveurs de répliques Open Directory en serveurs autonomes Open Directory, puis faites-en des répliques du nouveau maître.

   Pour obtenir des instructions, consultez les sections "Configuration d'un serveur autonome" à la page 81 et "Configuration d'une réplique Open Directory" à la page 85.

Résolution de problèmes liés aux maîtres et aux répliques Open Directory

Kerberos est arrêté sur un maître ou une réplique Open Directory

Un maître Open Directory requiert un DNS configuré correctement pour fournir une authentification Kerberos par signature unique.

Pour vérifier que le DNS est configuré correctement pour Kerberos :

1. Assurez-vous que le service DNS est configuré pour résoudre les noms DNS complets et fournir les recherches inverses correspondantes.

   Le DNS doit résoudre le nom DNS complet et fournir les recherches inverses au serveur maître Open Directory, à tous les serveurs répliques et aux autres serveurs qui sont membres du royaume Kerberos.

   Vous pouvez utiliser la sous-fenêtre Recherche d'Utilitaire de réseau (dans /Applications/Utilitaires/) pour faire une recherche DNS d'un nom DNS d'un serveur et une recherche inverse de l'adresse IP du serveur.

Pour obtenir des instructions sur la configuration du service DNS, consultez le guide d'administration de services réseau.

2 Assurez-vous que le nom d'hôte du serveur maître Open Directory est bien le nom DNS complet correct, et non le nom d'hôte local du serveur.

Par exemple, le nom d'hôte pourrait être ods.exemple.com, mais ne peut pas être ods.local.

Vous pouvez voir le nom d'hôte en ouvrant Terminal, en tapant `hostname`, puis en appuyant sur Retour.

Si le nom d'hôte du serveur Open Directory n'est pas son nom DNS complet, essayez d'effacer temporairement la liste des serveurs DNS et de cliquer sur Appliquer dans l es préférences Réseau du serveur Open Directory. Saisissez ensuite à nouveau une ou plusieurs adresses IP de serveur DNS, en commençant par le serveur DNS principal qui résout le nom du serveur Open Directory, puis en cliquant à nouveau sur Appliquer dans les préférences Réseau.

Si le nom d'hôte du serveur Open Directory n'est toujours pas son nom DNS complet, essayez de redémarrer le serveur.

3 Assurez-vous que les préférences Réseau du serveur maître Open Directory sont configurées pour utiliser le serveur DNS qui résout le nom du serveur.

Si le serveur maître Open Directory fournit son propre service DNS, les préférences Réseau du serveur doivent être configurées pour s'utiliser lui-même comme serveur DNS.

Après avoir confirmé la configuration DNS correcte pour le serveur, vous pouvez essayer de démarrer Kerberos. Consultez la section "Démarrage de Kerberos après la configuration d'un maître Open Directory" à la page 91.

Impossible de créer une réplique Open Directory

Si vous essayez de créer deux répliques simultanément, une tentative va réussir, l'autre va échouer. Une nouvelle tentative de création de la seconde réplique devrait réussir. Si vous ne pouvez toujours pas créer la seconde réplique, allez dans le dossier /var/run/, localisez le fichier slapconfig.lock et supprimez-le s'il existe. Vous pouvez aussi redémarrer le serveur.

Résolution de problèmes liés à l'accès au répertoire

Les problèmes d'accès aux services de répertoire lors du démarrage peuvent avoir plusieurs causes.

Un ralentissement se produit lors du démarrage

Si Mac OS X ou Mac OS X Server rencontre un problème de ralentissement au démarrage alors qu'un message concernant NetInfo, LDAP ou les services de répertoire s'affiche au-dessus de la barre de progression, il est possible que l'ordinateur essaie d'accéder à un domaine NetInfo ou à un répertoire LDAP qui n'est pas disponible sur votre réseau.

- Une pause pendant le démarrage est normale lorsque vous déconnectez un ordinateur portable du réseau auquel le serveur LDAP est connecté.
- Utilisez Format de répertoire pour vous assurer que les configurations NetInfo et LDAP sont correctes.
- Utilisez le tableau Réseau des Préférences Système pour vous assurer que la configuration réseau de l'ordinateur et les autres paramètres de réseau sont corrects.
- Examinez le réseau physique pour détecter d'éventuels problèmes de connexion.

Résolution des problèmes d'authentification

Vous pouvez résoudre certains problèmes courants des services d'authentification.

Vous ne pouvez pas modifier le mot de passe Open Directory d'un utilisateur

Pour modifier le mot de passe d'un utilisateur dont le type de mot de passe est Open Directory, vous devez être un administrateur du domaine de répertoire dans lequel l'enregistrement de l'utilisateur réside. De plus, votre compte d'utilisateur doit posséder un mot de passe de type Open Directory.

Normalement, le compte d'utilisateur spécifié lors de la configuration du maître Open Directory (à l'aide d'Assistant du serveur ou des réglages de services Open Directory dans Admin Serveur) être doté d'un mot de passe Open Directory. Ce compte peut être utilisé pour configurer d'autres comptes d'utilisateur en tant qu'administrateur de domaine de répertoire avec des mots de passe Open Directory.

Si tout le reste échoue, essayez d'utiliser le compte d'utilisateur root pour configurer un compte d'utilisateur en tant qu'administrateur de répertoire avec un mot de passe Open Directory. (Le nom du compte d'utilisateur root est "root" et le mot de passe est généralement le même que le mot de passe attribué initialement au compte d'administrateur créé pendant la configuration initiale du serveur).

Un utilisateur ne peut pas accéder à certains services

Si un utilisateur peut accéder à certains services qui requièrent une authentification, mais pas à d'autres, essayez de changer temporairement le mot de passe de l'utilisateur en une suite de caractères simples, comme, par exemple, "mdp". Si cela résout le problème, cela signifie que le mot de passe précédent de l'utilisateur contenait des caractères qui n'étaient pas autorisés par tous les services. Par exemple, certains services autorisent les espaces dans les mots de passe, d'autres pas.

Un utilisateur ne parvient pas à s'authentifier pour le service VPN

Les utilisateurs, dont les comptes sont stockés sur un serveur sous Mac OS X Server 10.2 ne peuvent pas s'authentifier pour le service VPN fourni par Mac OS X Server 10.3–10.4. Le service VPN requiert la méthode d'authentification MS-CHAPv2, qui n'est pas gérée par Mac OS X Server version 10.2. Pour permettre aux utilisateurs concernés de se connecter, vous pouvez transférer leurs comptes d'utilisateur sur un serveur sous Mac OS X Server 10.3–10.4. Une autre solution consiste à mettre à niveau les anciens serveurs vers Mac OS X Server 10.4 ou ultérieur.

Vous ne pouvez pas changer le type de mot de passe d'un utilisateur en Open Directory

Pour changer le mot de passe d'un utilisateur en authentification Open Directory, vous devez être un administrateur du domaine de répertoire dans lequel l'enregistrement de l'utilisateur réside. De plus, votre compte d'utilisateur doit être configuré pour une authentification Open Directory. Le compte d'utilisateur spécifié lors de la configuration du maître Open Directory (à l'aide d'Assistant du serveur ou des réglages de services Open Directory dans Admin Serveur) possède un mot de passe Open Directory. Ce compte peut être utilisé pour configurer d'autres comptes d'utilisateur en tant qu'administrateur de domaine de répertoire avec des mots de passe Open Directory.

Les utilisateurs dépendant d'un Serveur de mots de passe ne parviennent pas à se connecter

Si votre réseau contient un serveur sous Mac OS X Server 10.2, il peut être configuré pour obtenir l'authentification d'un serveur de mots de passe Open Directory hébergé par un autre serveur. Si l'ordinateur du Serveur de mots de passe est déconnecté du réseau, par exemple parce que vous avez débranché la câble du port Ethernet de l'ordinateur, les utilisateurs dont les mots de passe sont validés à l'aide du Serveur de mots de passe ne peuvent pas se connecter parce que son adresse IP n'est pas accessible.

Les utilisateurs peuvent se connecter à Mac OS X Server si vous rebranchez l'ordinateur du Serveur de mots de passe au réseau. Pendant que l'ordinateur du serveur de mots de passe est hors ligne, les utilisateurs peuvent se connecter avec des comptes d'utilisateur dont le type de mot de passe est un mot de passe crypté ou un mot de passe Shadow.

Les utilisateurs ne peuvent pas se connecter à l'aide de comptes dans un domaine de répertoire partagé

Les utilisateurs ne peuvent pas se connecter à l'aide de comptes dans un domaine de répertoire partagé si le serveur hébergeant le répertoire n'est pas accessible. Un serveur peut devenir inaccessible à cause d'un problème lié au réseau, au logiciel de serveur ou au matériel du serveur. Les problèmes liés au matériel ou au logiciel du serveur affectent les utilisateurs qui tentent de se connecter à des ordinateurs Mac OS X et les utilisateurs qui tentent de se connecter au domaine Windows d'un PDC Mac OS X Server. Les problèmes liés au réseau peuvent affecter certains utilisateurs et pas d'autres, en fonction de là où se situe le problème lié au réseau.

Les utilisateurs qui disposent de comptes d'utilisateur mobiles peuvent toujours se connecter aux ordinateurs Mac OS X qu'ils utilisaient précédemment. Et les utilisateurs affectés par ces problèmes peuvent se connecter à l'aide d'un compte d'utilisateur local défini sur l'ordinateur, comme, par exemple, le compte d'utilisateur créé pendant la configuration initiale, après l'installation de Mac OS X.

Impossible de se connecter comme utilisateur Active Directory

Après avoir configuré une connexion vers un domaine Active Directory dans la sous-fenêtre Service de Format de répertoire et après l'avoir ajouté à une politique de recherche personnalisée dans la sous-fenêtre Authentification, vous devez attendre 10 ou 15 secondes pour que le changement entre en vigueur. Les tentatives de connexion immédiates avec un compte Active Directory échoueront.

Les utilisateurs ne peuvent pas s'authentifier à l'aide de la signature unique ou de Kerberos

En cas d'échec de l'authentification d'un utilisateur ou d'un service utilisant Kerberos, essayez les solutions suivantes :

- L'authentification Kerberos est basée sur des horodatages cryptés. S'il existe un écart de plus de 5 minutes entre le centre de distribution de clés, l'ordinateur client et l'ordinateur du service, l'authentification peut échouer. Assurez-vous que les horloges de tous les ordinateurs sont synchronisées à l'aide du service Network Time Protocol (NTP) et Mac OS X Server ou de tout autre serveur horloge de réseau. Pour en savoir plus sur le service NTP de Mac OS X Server, consultez le guide d'administration de services réseau.
- Assurez-vous que Kerberos est exécuté sur le maître Open Directory et les répliques. Consultez la section "Kerberos est arrêté sur un maître ou une réplique Open Directory" à la page 188.
- Si un serveur Kerberos servant à la validation de mot de passe est indisponible, réinitialisez le mot de passe de l'utilisateur afin de recourir à un serveur disponible.
- Assurez-vous que le serveur fournissant le service kerbérisé dispose d'un accès au domaine de répertoire du serveur Kerberos et que ce domaine de répertoire contient les comptes des utilisateurs qui tentent de s'authentifier à l'aide de Kerberos. Pour en savoir plus sur la configuration de l'accès à des domaines de répertoire, consultez le chapitre 7, "Gestion de Format de répertoire".
- Pour un royaume Kerberos d'un serveur Open Directory, assurez-vous que l'ordinateur du client est configuré pour accéder au répertoire LDAP du serveur Open Directory à l'aide du bon suffixe de base de recherche. Le réglage du suffixe de base de recherche LDAPv3 du client doit correspondre au réglage de base de recherche du répertoire LDAP. Le suffixe de base de recherche LDAPv3 du client peut être vide s'il reçoit ses mappages LDAP du serveur. Dans ce cas, le client utilise le suffixe de base de recherche par défaut du répertoire LDAP.

- Pour vérifier le réglage en matière de suffixe de base de recherche, ouvrez Format de répertoire, affichez la liste des configurations LDAPv3 et choisissez l'élément dans le menu local Mappages LDAP qui est déjà sélectionné dans le menu. Pour obtenir des instructions, consultez la section "Modification d'une configuration pour l'accès à un répertoire LDAP" à la page 137.
- Pour contrôler les réglages de base de recherche du répertoire LDAP, ouvrez Admin Serveur et recherchez le service Open Directory dans la sous-fenêtre Protocole de la sous-fenêtre Réglages.

- Pour obtenir des informations pouvant vous aider à résoudre des problèmes, consultez l'historique du centre de distribution de clés. Consultez la section "Affichage des états et des historiques Open Directory" à la page 178.
- Si Kerberos ne tournait pas quand les enregistrements d'utilisateur ont été créés, importés ou mis à jour à partir d'une version de Mac OS X plus ancienne, il se peut qu'ils ne soient pas activés pour l'authentification Kerberos.
  - Un enregistrement n'est pas activé pour Kerberos s'il manque une valeur ; Kerberosv5; à son attribut d'autorité d'authentification. Vous pouvez utiliser l'Inspecteur de Gestionnaire de groupe de travail pour voir la ou les valeurs d'un attribut d'autorité d'authentification d'un enregistrement d'utilisateur.
  - Vous pouvez activer Kerberos pour un enregistrement d'utilisateur en changeant son type de mot de passe. Réglez d'abord le type de mot de passe sur l'option de mot de passe crypté, puis sur Open Directory. Pour obtenir des instructions détaillées, consultez les sections "Changement du type de mot en Mot de passe crypté" à la page 108 et "Choix du type de mot de passe Open Directory" à la page 107.
- Si des utilisateurs ne peuvent pas s'authentifier à l'aide de la signature unique ou de Kerberos pour des services fournis par un serveur connecté à un royaume Kerberos d'un maître Open Directory, l'enregistrement d'ordinateur du serveur est peut-être mal configuré dans le répertoire LDAP du maître Open Directory. En particulier, le nom du serveur qui figure dans le compte de liste d'ordinateurs doit être le nom DNS complet du serveur, et pas juste le nom d'hôte du serveur. Par exemple, le nom pourrait être serveur2.exemple.com, mais pas juste serveur2.

Pour reconfigurer un enregistrement d'ordinateur d'un serveur pour l'authentification Kerberos à signature unique :

1. Supprimez le serveur du compte de liste d'ordinateurs dans le répertoire LDAP.

   Pour obtenir des instructions sur cette opération et sur l'étape suivante, consultez le guide de gestion des utilisateurs.
2. Ajoutez à nouveau le serveur à la liste d'ordinateurs.
3. Déléguez à nouveau l'autorité pour connecter le serveur au royaume Kerberos du maître Open Directory.

   Pour obtenir des instructions, consultez la section "Délégation d'autorité pour connecter des serveurs à un royaume Kerberos Open Directory" à la page 92.
4. Connectez à nouveau le serveur au royaume Kerberos Open Directory.

Pour obtenir des instructions, consultez la section “Connecter un serveur à un royaume Kerberos” à la page 95.

Certains utilisateurs ne peuvent pas changer leur mot de passe

Les utilisateurs dont les comptes résident dans un répertoire LDAP qui n’est pas hébergé par Mac OS X Server et qui ont un mot de passe de type mot de passe crypté ne peuvent pas changer leur mot de passe après s’être connecté à partir d’un ordinateur client sous Mac OS X 10.3. Ces utilisateurs peuvent changer leur mot de passe si vous utilisez la sous-fenêtre Avancé de Gestionnaire de groupe de travail pour changer le réglage Type du mot de passe de leur compte en Open Directory. Lorsque vous apportez cette modification, vous devez aussi saisir un nouveau mot de passe. Expliquez ensuite aux utilisateurs qu’ils doivent se connecter à l’aide de ce nouveau mot de passe et le changer dans la sous-fenêtre Comptes des Préférences Système.

Impossible de connecter un serveur à un royaume Kerberos Open Directory

Si un utilisateur possédant une autorité Kerberos délégué ne peut pas connecter un serveur à un royaume Kerberos d’un maître Open Directory, il se peut que l’enregistrement d’ordinateur du serveur soit mal configuré dans le répertoire LDAP du maître Open Directory. En particulier, l’adresse du serveur dans le compte de liste d’ordinateurs doit être l’adresse Ethernet principale du serveur. L’adresse Ethernet principale du serveur est l’identifiant Ethernet du premier port Ethernet qui apparaît dans la liste des configurations de ports réseau qui est affichée dans la sous-fenêtre des préférences Réseau du serveur.

Pour reconfigurer un enregistrement d’ordinateur d’un serveur pour se connecter à un royaume Kerberos :

1. Supprimez le serveur du compte de liste d’ordinateurs dans le répertoire LDAP.

   Pour obtenir des instructions sur cette opération et sur l’étape suivante, consultez le guide de gestion des utilisateurs.

2. Ajoutez à nouveau le serveur à la liste d’ordinateurs.
3. Déléguez à nouveau l’autorité pour connecter le serveur au royaume Kerberos du maître Open Directory.

   Vous pouvez passer cette étape si vous pouvez utiliser un compte d’administrateur Kerberos (un compte d’administrateur de répertoire LDAP) pour connecter à nouveau le serveur au royaume Kerberos. À défaut, consultez la section “Délégation d’autorité pour connecter des serveurs à un royaume Kerberos Open Directory” à la page 92 pour obtenir des instructions.

4. Connectez à nouveau le serveur au royaume Kerberos Open Directory.

   Pour obtenir des instructions, consultez la section “Connecter un serveur à un royaume Kerberos” à la page 95.

Réinitialisation d'un mot de passe d'administrateur

Le disque d'installation de Mac OS X Server vous permet de changer le mot de passe d'un compte d'utilisateur disposant d'autorisations d'administrateur, y compris le compte de l'Administrateur système (root ou superuser).

Important : dans la mesure où un utilisateur disposant du disque d'installation peut accéder sans restriction à votre serveur, il est conseillé de limiter l'accès physique à l'ordinateur hébergeant le logiciel de serveur.

Pour modifier le mot de passe d'un compte d'administrateur :

1. Démarrez à partir du disque d'installation 1 de Mac OS X Server.
2. Dans le programme d'installation, choisissez Installation > Réinitialiser le mot de passe.
3. Sélectionnez le volume de disque dur contenant le compte d'administrateur dont vous voulez réinitialiser le mot de passe.
4. Choisissez le compte d'administrateur dans le menu local, tapez un nouveau mot de passe, puis cliquez sur Enregistrer.

   L'Administrateur système correspond au compte d'utilisateur racine (root ou superuser). Ne confondez pas ce compte avec un compte d'administrateur normal.

   Évitez de modifier les mots de passe des comptes d'utilisateur prédéfinis. Pour plus d'informations sur les comptes d'utilisateur prédéfinis, lisez le guide de gestion des utilisateurs.

   Remarque : cette procédure modifie le mot de passe du compte d'administrateur stocké dans le domaine de répertoire local du serveur. Il ne modifie pas le mot de passe d'un compte d'administrateur stocké dans le domaine de répertoire partagé du serveur, si le serveur dispose d'un tel domaine.

   Si vous connaissez le mot de passe d'un compte d'administrateur stocké dans le domaine local, vous pouvez modifier le mot de passe de tous les autres comptes d'administrateur du domaine de répertoire local en utilisant Gestionnaire de groupe de travail plutôt que cette procédure. Pour plus d'instructions, consultez le guide de gestion des utilisateurs.

Données de répertoire Mac OS X

La connaissance du schéma LDAP Open Directory et des attributs et types d'enregistrements des domaines de répertoire Mac OS X vous aidera pour le mappage sur d'autres domaines de répertoire, ainsi que pour l'importation ou l'exportation des comptes d'utilisateur et de groupe.

La présente annexe liste les extensions Open Directory au schéma LDAP, les mappages d'attributs Open Directory sur des attributs LDAP et Active Directory et les attributs standard de divers types d'enregistrements. Utilisez ces informations pour :

- Mapper des classes d'objets et des attributs de répertoires LDAP non-Apple ou des domaines Active Directory sur des types et attributs d'enregistrements Open Directory, comme décrit dans la section "Configuration des recherches et mappages LDAP" à la page 143.
- Importer ou exporter des comptes d'utilisateur ou de groupe vers un domaine Open Directory, comme décrit dans le guide de gestion des utilisateurs.
- Travailler dans la sous-fenêtre Inspecteur de Gestionnaire de groupe de travail, comme décrit dans la section "Affichage et modification directs des données de répertoire" à la page 179.

Pour plus de détails, consultez les sections suivantes :

Extensions Open Directory au schéma LDAP

Le schéma des répertoires LDAP Open Directory est basé sur les attributs et classes d'objets standard définis dans les documents RFC (Request for Comments) de l'IETF (Internet Engineering Task Force) :

- RFC 2307 "An Approach for Using LDAP as a Network Information Service"
- RFC 2798 "Definition of the inetOrgPerson LDAP Object Class"

Les définitions de schéma LDAP spécifient les identifiants de syntaxe et les règles de mise en correspondance qui sont définies dans :

- RFC 2252 "LDAPv3 Attributes"

Ces RFC sont disponibles sur le site Web de l'IETF :

www.ietf.org/rfc.html

Les attributs et classes d'objets définis dans ces RFC forment la base du schéma LDAP Open Directory.

Le schéma étendu pour les répertoires LDAP Open Directory inclut les attributs et classes d'objets définis dans :

- "Classes d'objets du schéma LDAP Open Directory" (ci-après).
- "Attributs du schéma LDAP Open Directory" à la page 205.

Remarque: Apple est susceptible d'étendre le schéma LDAP Open Directory à l'avenir, par exemple, pour prendre en charge de nouvelles versions de Mac OS X et Mac OS X Server. Le schéma le plus récent est disponible sous forme de fichiers texte sur tout ordinateur doté de Mac OS X Server. Les fichiers de schéma se trouvent dans le répertoire /etc/openldap/schema. En particulier, le fichier apple.schema contient les dernières extensions de schéma pour répertoires LDAP Open Directory.

Classes d'objets du schéma LDAP Open Directory

Cette section définit les classes d'objets Open Directory LDAP qui étendent le schéma LDAP standard.

Classe d'objets structurelle de conteneur (container)

Container est une classe d'objets structurelle utilisée pour les conteneurs d'enregistrements de premier niveau comme cn=users, cn=groups et cn=mounts. Il n'existe pas de services de répertoires analogues à cette classe d'objets, mais le nom de conteneur fait partie de la base de recherche pour chaque type d'enregistrement.

```
#objectclass (
# 1.2.840.113556.1.3.23
# NAME 'container'
# SUP top
# STRUCTURAL
# MUST (  cn ) )
```

Classe d'objets de durée de vie (Time To Live)

```
attributetype (
  1.3.6.1.4.1.250.1.60
  NAME 'ttl'
  EQUALITY integerMatch
  SYNTAX '1.3.6.1.4.1.1466.115.121.1.27' SINGLE-VALUE )
```

Classe d'objets d'utilisateur (User)

La classe d'objets apple-user est une classe auxiliaire servant à stocker des attributs spécifiques Mac OS X qui ne font pas partie d'inetOrgPerson ou de posixAccount. Cette classe d'objets est utilisée avec les enregistrements kDSStdRecordTypeUsers.

```
objectclass (
  1.3.6.1.4.1.63.1000.1.1.2.1
  NAME 'apple-user'
  SUP top
  AUXILIARY
  DESC 'compte d'utilisateur apple'
  MAY (   apple-user-homeurl $ apple-user-class $
          apple-user-homequota $ apple-user-mailattribute $
          apple-user-printattribute $ apple-mcxflags $
          apple-mcxsettings $ apple-user-adminlimits $
          apple-user-picture $ apple-user-authenticationhint $
          apple-user-homesoftquota $ apple-user-passwordpolicy $
          apple-keyword $ apple-generateduid $ apple-imhandle $
          apple-webloguri $
          authAuthority $ acctFlags $ pwdLastSet $ logonTime $
          logoffTime $ kickoffTime $ homeDrive $ scriptPath $
          profilePath $ userWorkstations $ smbHome $ rid $
          primaryGroupID $ sambaSID $ sambaPrimaryGroupSID $
          userCertificate ) )
```

Classe d'objets auxiliaire de groupe (group)

La classe d'objets apple-group est une classe auxiliaire utilisée pour stocker des attributs spécifiques Mac OS X qui ne font pas partie de posixGroup. Cette classe d'objets est utilisée avec les enregistrements kDSStdRecordTypeGroups.

```
objectclass (
  1.3.6.1.4.1.63.1000.1.1.2.14
  NAME 'apple-group'
  SUP top
  AUXILIARY
  DESC 'compte de groupe'
  MAY (   apple-group-homeurl $
          apple-group-homeowner $
          apple-mcxflags $
          apple-mcxsettings $
          apple-group-realname $
          apple-user-picture $
          apple-keyword $
          apple-generateduid $
          apple-group-nestedgroup $
          apple-group-memberguid $
          mail $
          rid $
          sambaSID $
          ttl ) )
```

Classe d'objets auxiliaire de machine (machine)

```
objectclass (
  1.3.6.1.4.1.63.1000.1.1.2.3
  NAME 'apple-machine'
  SUP top
  AUXILIARY
  MAY (   apple-machine-software $
          apple-machine-hardware $
          apple-machine-serves $
          apple-machine-suffix $
          apple-machine-contactperson ) )
```

Classe d'objets de montage (mount)

```
objectclass (
  1.3.6.1.4.1.63.1000.1.1.2.8
  NAME 'mount'
  SUP top STRUCTURAL
  MUST (  cn )
  MAY (   mountDirectory $
          mountType $
          mountOption $
          mountDumpFrequency $
          mountPassNo ) )
```

Classe d'objets d'imprimante (printer)

```
objectclass (
  1.3.6.1.4.1.63.1000.1.1.2.9
  NAME 'apple-printer'
  SUP top STRUCTURAL
  MUST (  cn )
  MAY (   apple-printer-attributes $
          apple-printer-lprhost $
          apple-printer-lprqueue $
          apple-printer-type $
          apple-printer-note ) )
```

Classe d'objets d'ordinateur (computer)

```
objectclass (
  1.3.6.1.4.1.63.1000.1.1.2.10
  NAME 'apple-computer'
  DESC 'ordinateur'
  SUP top STRUCTURAL
  MUST (  cn )
  MAY (   apple-realname $
          description $
          macAddress $
          apple-category $
          apple-computer-list-groups $
          apple-keyword $
          apple-mcxflags $
          apple-mcxsettings $
          apple-networkview $
          apple-xmlplist $
          apple-service-url $
          authAuthority $
          uidNumber $ gidNumber $ apple-generateduid $ ttl $
          acctFlags $ pwdLastSet $ logonTime $
          logoffTime $ kickoffTime $ rid $ primaryGroupID $
          sambaSID $ sambaPrimaryGroupSID ) )
```

Classe d'objets de liste d'ordinateurs (ComputerList)

```
objectclass (
  1.3.6.1.4.1.63.1000.1.1.2.11
  NAME 'apple-computer-list'
  DESC 'liste d'ordinateurs'
  SUP top STRUCTURAL
  MUST (  cn )
  MAY (   apple-mcxflags $
          apple-mcxsettings $
          apple-computer-list-groups $
          apple-computers $
```

```
        apple-generateduid $
        apple-keyword ) )
```

Classe d'objets de configuration (Configuration)

```
objectclass (
  1.3.6.1.4.1.63.1000.1.1.2.12
  NAME 'apple-configuration'
  DESC 'configuration'
  SUP top STRUCTURAL
  MAY (   cn $ apple-config-realname $
          apple-data-stamp $ apple-password-server-location $
          apple-password-server-list $ apple-ldap-replica $
          apple-ldap-writable-replica $ apple-keyword $
          apple-kdc-authkey $ apple-kdc-configdata $ apple-xmlplist $
          ttl ) )
```

Classe d'objets de liste d'ordinateurs préréglés (Preset Computer List)

```
objectclass (
  1.3.6.1.4.1.63.1000.1.1.2.13
  NAME 'apple-preset-computer-list'
  DESC 'liste d'ordinateurs préréglés'
  SUP top STRUCTURAL
  MUST (  cn )
  MAY (   apple-mcxflags $
          apple-mcxsettings $
          apple-computer-list-groups $
          apple-keyword ) )
```

Classe d'objets de groupe préréglé (Preset Group)

```
objectclass (
  1.3.6.1.4.1.63.1000.1.1.3.14
  NAME 'apple-preset-group'
  DESC 'groupe préréglé'
  SUP top STRUCTURAL
  MUST (  cn )
  MAY (   memberUid $
          gidNumber $
          apple-group-homeurl $
          apple-group-homeowner $
          apple-mcxflags $
          apple-mcxsettings $
          apple-group-realname $
          apple-keyword $
          apple-group-nestedgroup $
          apple-group-memberguid $
          ttl ) )
```

Classe d'objets d'utilisateur préréglé (Preset User)

```
objectclass (
  1.3.6.1.4.1.63.1000.1.1.2.15
  NAME 'apple-preset-user'
  DESC 'utilisateur préréglé'
  SUP top STRUCTURAL
  MUST (  cn )
  MAY (   uid $
          memberUid $
          gidNumber $
          homeDirectory $
          apple-user-homeurl $
          apple-user-homequota $
          apple-user-homesoftquota $
          apple-user-mailattribute $
          apple-user-printattribute $
          apple-mcxflags $
          apple-mcxsettings $
          apple-user-adminlimits $
          apple-user-passwordpolicy $
          userPassword $
          apple-user-picture $
          apple-keyword $
          loginShell $
          description $
          shadowLastChange $
          shadowExpire $
          authAuthority $
          homeDrive $ scriptPath $ profilePath $ smbHome $
          apple-preset-user-is-admin ) )
```

Classe d'objets d'autorité d'authentification (Authentication Authority)

```
objectclass (
  1.3.6.1.4.1.63.1000.1.1.2.16
  NAME 'authAuthorityObject'
  SUP top AUXILIARY
  MAY (   authAuthority ) )
```

Classe d'objets de configuration d'assistant du serveur (Server Assistant Configuration)

```
objectclass (
  1.3.6.1.4.1.63.1000.1.1.2.17
  NAME 'apple-serverassistant-config'
  SUP top AUXILIARY
  MUST (  cn )
  MAY (   apple-xmlplist ) )
```

Classe d'objets d'emplacement (Location)

```
objectclass (
  1.3.6.1.4.1.63.1000.1.1.2.18
  NAME 'apple-location'
  SUP top AUXILIARY
  MUST (  cn )
  MAY (   apple-dns-domain $ apple-dns-nameserver ) )
```

Classe d'objets de service (Service)

```
objectclass (
  1.3.6.1.4.1.63.1000.1.1.2.19
  NAME 'apple-service'
  SUP top STRUCTURAL
  MUST (  cn $
          apple-service-type )
  MAY (   ipHostNumber $
          description $
          apple-service-location $
          apple-service-url $
          apple-service-port $
          apple-dnsname $
          apple-keyword ) )
```

Classe d'objets de voisinage (Neighborhood)

```
objectclass (
  1.3.6.1.4.1.63.1000.1.1.2.20
  NAME 'apple-neighborhood'
  SUP top STRUCTURAL
  MUST (  cn )
  MAY (   description $
          apple-generateduid $
          apple-category $
          apple-nodepathxml $
          apple-neighborhoodalias $
          apple-computeralias $
          apple-keyword $
          apple-realname $
          apple-xmlplist $
          ttl ) )
```

Classe d'objets de liste de contrôle d'accès (ACL)

```
objectclass (
  1.3.6.1.4.1.63.1000.1.1.2.21
  NAME 'apple-acl'
  SUP top STRUCTURAL
  MUST (  cn $
          apple-acl-entry ) )
```

Attributs du schéma LDAP Open Directory

Cette section définit les attributs LDAP Open Directory qui étendent le schéma LDAP standard.

Attribut de durée de vie (Time-to-Live)

```
objectclass (
  1.3.6.1.4.1.250.3.18
  NAME 'cacheObject'
  AUXILIARY
  SUP top
  DESC 'Auxiliary object class to hold TTL caching information'
  MAY (   ttl ) )
```

Attributs d'utilisateur (User)

apple-user-homeurl

Stocke les informations de répertoire de départ sous la forme d'une URL et d'un chemin d'accès. Cela permet d'établir une correspondance avec le type d'attribut kDS1AttrHomeDirectory des services de répertoires.

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.1.6
  NAME 'apple-user-homeurl'
  DESC 'URL du répertoire de départ'
  EQUALITY caseExactIA5Match
  SUBSTR caseExactIA5SubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )
```

apple-user-class

Inutilisé.

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.1.7
  NAME 'apple-user-class'
  DESC 'classe d'utilisateur'
  EQUALITY caseExactIA5Match
  SUBSTR caseExactIA5SubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )
```

apple-user-homequota

Spécifie le quota du répertoire de départ en kilo-octets.

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.1.8
  NAME 'apple-user-homequota'
  DESC 'quota du répertoire de départ'
  EQUALITY caseExactIA5Match
  SUBSTR caseExactIA5SubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )
```

apple-user-mailattribute

Stocke les réglages de courrier au format XML.

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.1.9
  NAME 'apple-user-mailattribute'
  DESC 'attribut de courrier'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
```

apple-mcxflags

Stocke les informations de client géré. Cet attribut se trouve dans les enregistrements d'utilisateur, de groupe, d'ordinateur et de listes d'ordinateurs.

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.1.10
  NAME 'apple-mcxflags'
  DESC 'indicateurs mcx'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
```

apple-mcxsettings

Stocke les informations de client géré. Cet attribut se trouve dans les enregistrements d'utilisateur, de groupe, d'ordinateur et de listes d'ordinateurs.

```
#attributetype (
# 1.3.6.1.4.1.63.1000.1.1.1.1.11
# NAME 'apple-mcxsettings'
# DESC 'réglages mcx'
# EQUALITY caseExactMatch
# SUBSTR caseExactSubstringsMatch
# SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.1.16
  NAME ( 'apple-mcxsettings' 'apple-mcxsettings2' )
  DESC 'réglages mcx'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

apple-user-picture

Stocke un chemin d'accès vers l'image à afficher dans la fenêtre d'ouverture de session pour cet enregistrement d'utilisateur. Utilisé lorsque l'utilisateur est affiché dans la liste déroulante de la fenêtre d'ouverture de session (sur les réseaux gérés).

Les utilisateurs ont la possibilité de modifier leur image par défaut.

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.1.12
  NAME 'apple-user-picture'
  DESC 'image'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
```

apple-user-printattribute

Stocke les réglages de quota d'impression sous forme de plist XML.

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.1.13
  NAME 'apple-user-printattribute'
  DESC 'attribut d'impression'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
```

apple-user-adminlimits

Cet attribut est utilisé par Gestionnaire de groupe de travail pour stocker une plist XML décrivant les capacités d'un administrateur. Ces réglages sont respectés et actualisés par Gestionnaire de groupe de travail, mais n'affectent pas les autres éléments du système.

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.1.14
  NAME 'apple-user-adminlimits'
  DESC 'capacités d'administrateur'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
```

apple-user-authenticationhint

L'attribut apple-user-authenticationhint est utilisé par la fenêtre d'ouverture de session pour afficher un indice lorsque l'utilisateur effectue successivement trois tentatives ratées d'ouverture de session.

Chaque utilisateur peut modifier son indice d'authentification.

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.1.15
  NAME 'apple-user-authenticationhint'
  DESC 'indice de mot de passe'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
```

apple-user-homesoftquota

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.1.17
  NAME 'apple-user-homesoftquota'
  DESC 'quota (soft) du répertoire de départ'
  EQUALITY caseExactIA5Match
  SUBSTR caseExactIA5SubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )
```

apple-user-passwordpolicy

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.1.18
  NAME 'apple-user-passwordpolicy'
  DESC 'options de politique de mot de passe'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
```

apple-keyword

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.1.19
  NAME ( 'apple-keyword' )
  DESC 'mots clés'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

apple-imhandle

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.1.21
  NAME ( 'apple-imhandle' )
  DESC 'IM handle (service:account name)'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

apple-webloguri

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.1.22
  NAME ( 'apple-webloguri' )
  DESC 'Weblog URI'
  EQUALITY caseExactIA5Match
  SUBSTR caseExactIA5SubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )
```

apple-generateduid

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.1.20
  NAME ( 'apple-generateduid' )
  DESC 'identifiant unique généré'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
```

apple-user-homeDirectory

Il n'est pas utilisé par le serveur Open Directory mais fourni comme exemple d'OID et d'attribut à employer comme alternative à l'attribut homeDirectory de la RFC 2307. Il est particulièrement intéressant pour Active Directory puisqu'il utilise un attribut homeDirectory différent de celui de la RFC 2307.

```
#attributetype (
# 1.3.6.1.4.1.63.1000.1.1.1.1.100
# NAME 'apple-user-homeDirectory'
# DESC 'Le chemin d'accès absolu au répertoire de départ'
# EQUALITY caseExactIA5Match
# SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )
```

Attributs de groupe (Group)

apple-group-homeurl

Spécifie le répertoire de départ associé à un groupe de travail de clients gérés. Monté lors de l'ouverture de session de tous les utilisateurs de ce groupe de travail.

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.14.1
  NAME 'apple-group-homeurl'
  DESC 'url du répertoire de départ du groupe'
  EQUALITY caseExactIA5Match
  SUBSTR caseExactIA5SubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )
```

apple-group-homeowner

L'attribut apple-group-homeowner détermine le propriétaire du répertoire de départ du groupe de travail lorsqu'il est créé dans le système de fichiers. Le groupe du répertoire est le groupe de travail auquel il est associé.

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.14.2
  NAME 'apple-group-homeowner'
  DESC 'réglages du propriétaire du répertoire de départ du groupe'
  EQUALITY caseExactIA5Match
  SUBSTR caseExactIA5SubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )
```

apple-group-realname

Permet d'associer un nom d'utilisateur plus long et plus convivial aux groupes. Ce nom apparaît dans Gestionnaire de groupe de travail et peut contenir des caractères non-ASCII.

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.14.5
  NAME 'apple-group-realname'
  DESC 'nom réel du groupe'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
```

apple-group-nestedgroup

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.14.6
  NAME 'apple-group-nestedgroup'
  DESC 'nom réel du groupe'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

apple-group-memberguid

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.14.7
  NAME 'apple-group-memberguid'
  DESC 'nom réel du groupe'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

apple-group-memberUid

Inutilisé par le serveur Open Directory, mais défini comme exemple d'attribut et d'OID pouvant être ajoutés à un autre serveur LDAP pour gérer les clients Mac OS X.

```
# Alternative à l'emploi de l'attribut memberUid de la RFC 2307.
#attributetype (
# 1.3.6.1.4.1.63.1000.1.1.1.14.1000
# NAME 'apple-group-memberUid'
# DESC 'liste des membres du groupe'
# EQUALITY caseExactIA5Match
# SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
# can also use OID 1.3.6.1.4.1.63.1000.1.1.2.1000
```

Attributs de machine (Machine)

apple-machine-software

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.3.8
  NAME 'apple-machine-software'
  DESC 'logiciel système installé'
  EQUALITY caseIgnoreIA5Match
  SUBSTR caseIgnoreIA5SubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

apple-machine-hardware

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.3.9
  NAME 'apple-machine-hardware'
  DESC 'description matérielle du système'
  EQUALITY caseIgnoreIA5Match
  SUBSTR caseIgnoreIA5SubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

apple-machine-serves

```
attributeType (
  1.3.6.1.4.1.63.1000.1.1.1.3.10
  NAME 'apple-machine-serves'
  DESC 'Liaison de serveur de domaine NetInfo'
  EQUALITY caseExactIA5Match
  SUBSTR caseExactIA5SubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

apple-machine-suffix

```
attributeType (
  1.3.6.1.4.1.63.1000.1.1.1.3.11
  NAME 'apple-machine-suffix'
  DESC 'suffixe DIT'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

apple-machine-contactperson

```
attributeType (
  1.3.6.1.4.1.63.1000.1.1.1.3.12
  NAME 'apple-machine-contactperson'
  DESC 'Name of contact person/owner of this machine'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

Attributs de montage (Mount)

mountDirectory

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.8.1
  NAME 'mountDirectory'
  DESC 'chemin d'accès de montage'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
```

mountType

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.8.2
  NAME 'mountType'
  DESC 'type VFS du montage'
  EQUALITY caseIgnoreIA5Match
  SUBSTR caseIgnoreIA5SubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )
```

mountOption

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.8.3
  NAME 'mountOption'
  DESC 'options de montage'
  EQUALITY caseIgnoreIA5Match
  SUBSTR caseIgnoreIA5SubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

mountDumpFrequency

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.8.4
  NAME 'mountDumpFrequency'
  DESC 'fréquence de vidage du montage'
  EQUALITY caseIgnoreIA5Match
  SUBSTR caseIgnoreIA5SubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )
```

mountPassNo

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.8.5
  NAME 'mountPassNo'
  DESC 'passno du montage'
  EQUALITY caseIgnoreIA5Match
  SUBSTR caseIgnoreIA5SubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )
```

apple-mount-name

```
# Alternative to using 'cn' when adding mount record schema to other LDAP
     servers
#attributetype (
# 1.3.6.1.4.1.63.1000.1.1.1.8.100
# NAME ( 'apple-mount-name' )
# DESC 'mount name'
# SUP name )
```

Attributs d'imprimante (Printer)

apple-printer-attributes

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.9.1
  NAME 'apple-printer-attributes'
  DESC 'attributs d'imprimante au format /etc/printcap'
  EQUALITY caseIgnoreIA5Match
  SUBSTR caseIgnoreIA5SubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

apple-printer-lprhost

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.9.2
  NAME 'apple-printer-lprhost'
  DESC 'nom d'hôte LPR d'imprimante'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

apple-printer-lprqueue

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.9.3
  NAME 'apple-printer-lprqueue'
  DESC 'liste d'attente LPR d'imprimante'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

apple-printer-type

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.9.4
  NAME 'apple-printer-type'
  DESC 'type d'imprimante'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

apple-printer-note

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.9.5
  NAME 'apple-printer-note'
  DESC 'note d'imprimante'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

Attributs d'ordinateur (Computer)

apple-realname

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.10.2
  NAME 'apple-realname'
  DESC 'nom réel'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

apple-networkview

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.10.3
  NAME 'apple-networkview'
  DESC 'Network view for the computer'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

apple-category

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.10.4
  NAME 'apple-category'
  DESC 'Category for the computer or neighborhood'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

Attributs de liste d'ordinateurs (ComputerList)

apple-computers

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.11.3
  NAME 'apple-computers'
  DESC 'ordinateurs'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

apple-computer-list-groups

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.11.4
  NAME 'apple-computer-list-groups'
  DESC 'groupes'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

Attribut de Plist XML

apple-xmlplist

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.17.1
  NAME 'apple-xmlplist'
  DESC 'données de plist XML'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
```

Attributs d'URL de service (Service URL)

apple-service-url

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.19.2
  NAME 'apple-service-url'
  DESC 'URL of service'
  EQUALITY caseExactIA5Match
  SUBSTR caseExactIA5SubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

Attributs de configuration (Configuration)

apple-password-server-location

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.12.1
  NAME 'apple-password-server-location'
  DESC 'emplacement du serveur de mots de passe'
  EQUALITY caseExactIA5Match
  SUBSTR caseExactIA5SubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )
```

apple-data-stamp

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.12.2
  NAME 'apple-data-stamp'
  DESC 'data stamp'
  EQUALITY caseExactIA5Match
  SUBSTR caseExactIA5SubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )
```

apple-config-realname

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.12.3
  NAME 'apple-config-realname'
  DESC 'nom réel de configuration'
  EQUALITY caseExactIA5Match
  SUBSTR caseExactIA5SubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )
```

apple-password-server-list

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.12.4
  NAME 'apple-password-server-list'
  DESC 'plist de duplication de serveur de mots de passe'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
```

apple-ldap-replica

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.12.5
  NAME 'apple-ldap-replica'
  DESC 'liste de duplication LDAP'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

apple-ldap-writable-replica

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.12.6
  NAME 'apple-ldap-writable-replica'
  DESC 'liste de duplication LDAP modifiable'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

apple-kdc-authkey

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.12.7
  NAME 'apple-kdc-authkey'
  DESC 'clé maîtresse KDC cryptée au format RSA avec clé publique de
     royaume'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

apple-kdc-configdata

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.12.8
  NAME 'apple-kdc-configdata'
  DESC 'Contenu du fichier kdc.conf'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
```

Attribut d'utilisateur préréglé (PresetUser)

apple-preset-user-is-admin

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.15.1
  NAME 'apple-preset-user-is-admin'
  DESC 'indicateur signalant si l'utilisateur préréglé est un
     administrateur'
  EQUALITY caseExactIA5Match
  SUBSTR caseExactIA5SubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )
```

Attributs d'autorité d'authentification (Authentication Authority)

authAuthority

```
#attributetype (
# 1.3.6.1.4.1.63.1000.1.1.2.16.1
# NAME 'authAuthority'
# DESC 'autorité d'authentification du serveur de mots de passe'
# EQUALITY caseExactIA5Match
# SUBSTR caseExactIA5SubstringsMatch
# SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

authAuthority2

```
#attributetype (
# 1.3.6.1.4.1.63.1000.1.1.2.16.2
# NAME ( 'authAuthority' 'authAuthority2' )
# DESC 'autorité d'authentification du serveur de mots de passe'
# EQUALITY caseExactMatch
# SUBSTR caseExactSubstringsMatch
# SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

Attributs d'emplacement (Location)

apple-dns-domain

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.18.1
  NAME 'apple-dns-domain'
  DESC 'domaine DNS'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

apple-dns-nameserver

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.18.2
  NAME 'apple-dns-nameserver'
  DESC 'liste de serveurs de noms DNS'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

Attributs de service (Service)

apple-service-type

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.19.1
  NAME 'apple-service-type'
  DESC 'type of service'
  EQUALITY caseExactIA5Match
  SUBSTR caseExactIA5SubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

apple-service-url

```
#attributetype (
# 1.3.6.1.4.1.63.1000.1.1.1.19.2
# NAME 'apple-service-url'
# DESC 'URL of service'
# EQUALITY caseExactIA5Match
# SUBSTR caseExactIA5SubstringsMatch
# SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

apple-service-port

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.19.3
  NAME 'apple-service-port'
  DESC 'Service port number'
  EQUALITY integerMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 )
```

apple-dnsname

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.19.4
  NAME 'apple-dnsname'
  DESC 'DNS name'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

apple-service-location

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.19.5
  NAME 'apple-service-location'
  DESC 'Service location'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

Attributs de voisinage (Neighborhood)

apple-nodepathxml

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.20.1
  NAME 'apple-nodepathxml'
  DESC 'XML plist of directory node path'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

apple-neighborhoodalias

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.20.2
  NAME 'apple-neighborhoodalias'
  DESC 'XML plist referring to another neighborhood record'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

apple-computeralias

```
attributetype (
  1.3.6.1.4.1.63.1000.1.1.1.20.3
  NAME 'apple-computeralias'
  DESC 'XML plist referring to a computer record'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

Attribut de liste de contrôle d'accès (ACL)

apple-acl-entry

```
#attributetype (
# 1.3.6.1.4.1.63.1000.1.1.1.21.1
# NAME 'apple-acl-entry'
# DESC 'acl entry'
# EQUALITY caseExactMatch
# SUBSTR caseExactSubstringsMatch
# SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

Attributs de schéma (Schema)

apple-apple-attributeTypesConfig

```
#attributetype (
# 1.3.6.1.4.1.63.1000.1.1.1.22.1
# NAME 'attributeTypesConfig'
# DESC 'attribute type configuration'
# EQUALITY objectIdentifierFirstComponentMatch
# SYNTAX 1.3.6.1.4.1.1466.115.121.1.3 )
```

apple-objectClassesConfig

```
#attributetype (
# 1.3.6.1.4.1.63.1000.1.1.1.22.2
# NAME 'objectClassesConfig'
# DESC 'object class configuration'
# EQUALITY objectIdentifierFirstComponentMatch
# SYNTAX 1.3.6.1.4.1.1466.115.121.1.37 )
```

Mappage de types d'enregistrements et d'attributs standard vers LDAP et Active Directory

Cette section décrit le mappage des types d'enregistrements et attributs Open Directory vers les classes d'objets et attributs LDAP. Elle décrit également le mappage des catégories et attributs d'objet Active Directory vers les types d'enregistrements et attributs Open Directory, et comment les premiers sont générés à partir des derniers.

Mappages d'utilisateurs (Users)

Les tableaux suivants décrivent la manière dont le module LDAPv3 de Format de répertoire mappe le type d'enregistrement et les attributs Users Open Directory vers les classes d'objets et les attributs LDAP. Les tableaux spécifient également la manière dont le module Active Directory de Format de répertoire mappe et génère des attributs et des catégories d'objets Active Directory à partir d'attributs et de types d'enregistrements Open Directory.

Mappages des types d'enregistrements d'utilisateurs (Users)

Nom Open Directory, RFC/classe	OID de nom de classe d'objets LDAP	Module externe Active Directory
Users, RFC 2798	inetOrgPerson 2.16.840.1.113730.3.2.2	ObjectCategory = Person
Users, RFC 2307	posixAccount 1.3.6.1.1.1.2.0	
Users, RFC 2307	shadowAccount 1.3.6.1.1.1.2.1	
Users, enregistré par Apple	apple-user 1.3.6.1.4.1.63.1000.1.1.2.1	schéma étendu Apple

Mappages des attributs d'utilisateurs (Users)

Nom Open Directory, RFC/classe, emploi spécial	OID de nom d'attribut LDAP	Module externe Active Directory
HomeDirectory, enregistré par Apple	apple-user-homeurl 1.3.6.1.4.1.63.1000.1.1.1.6	Généré à partir de homeDirectory
HomeDirectoryQuota, enregistré par Apple	apple-user-homequota 1.3.6.1.4.1.63.1000.1.1.1.8	schéma étendu Apple
HomeDirectorySoftQuota, enregistré par Apple	apple-user-homesoftquota 1.3.6.1.4.1.63.1000.1.1.1.17	schéma étendu Apple
MailAttribute, enregistré par Apple	apple-user-mailattribute 1.3.6.1.4.1.63.1000.1.1.1.9	schéma étendu Apple
PrintServiceUserData, enregistré par Apple	apple-user-printattribute 1.3.6.1.4.1.63.1000.1.1.1.13	schéma étendu Apple
MCXFlags, enregistré par Apple	apple-mcxflags 1.3.6.1.4.1.63.1000.1.1.1.10	schéma étendu Apple
MCXSettings, enregistré par Apple	apple-mcxsettings 1.3.6.1.4.1.63.1000.1.1.1.16	schéma étendu Apple
AdminLimits, enregistré par Apple	apple-user-adminlimits 1.3.6.1.4.1.63.1000.1.1.1.14	schéma étendu Apple
AuthenticationAuthority, enregistré par Apple	authAuthority 1.3.6.1.4.1.63.1000.1.1.2.16.1	Généré en tant qu'autorité Kerberos
AuthenticationHint, enregistré par Apple	apple-user-authenticationhint 1.3.6.1.4.1.63.1000.1.1.1.15	schéma étendu Apple
PasswordPolicyOptions, enregistré par Apple	apple-user-passwordpolicy 1.3.6.1.4.1.63.1000.1.1.1.18	schéma étendu Apple
Keywords, enregistré par Apple	apple-keyword 1.3.6.1.4.1.63.1000.1.1.1.19	schéma étendu Apple
Picture, enregistré par Apple	apple-user-picture 1.3.6.1.4.1.63.1000.1.1.1.12	schéma étendu Apple
GeneratedUID, enregistré par Apple	apple-generateduid 1.3.6.1.4.1.63.1000.1.1.1.20	À partir de GUID — formaté
RecordName, RFC 2256	cn 2.5.4.3	Généré à partir de cn, userPrincipal, mail, sAMAccoutName
RecordName, RFC 1274	uid 0.9.2342.19200300.100.1.1	n/d
EMailAddress, RFC 1274	mail 0.9.2342.19200300.100.1.3	Standard RFC
RealName, RFC 2256	cn 2.5.4.3	1.2.840.113556.1.2.13 (Microsoft)
Password, RFC 2256	userPassword 2.5.4.35	Pas de mappage

Nom Open Directory, RFC/classe, emploi spécial	OID de nom d'attribut LDAP	Module externe Active Directory
Comment, RFC 2256	description 2.5.4.13	Standard RFC
LastName, RFC 2256	sn 2.5.4.4	Standard RFC
FirstName, RFC 2256	givenName 2.5.4.42	Standard RFC
PhoneNumber, RFC 2256	telephoneNumber 2.5.4.20	Standard RFC
AddressLIne1, RFC 2256	street 2.5.4.9	Standard RFC
PostalAddress, RFC 2256	postalAddress 2.5.4.16	Standard RFC
PostalCode, RFC 2256	postalCode 2.5.4.17	Standard RFC
OrganizationName, RFC 2256	o 2.5.4.10	1.2.840.113556.1.2.146 (Microsoft)
UserShell, RFC 2307	loginShell 1.3.6.1.1.1.1.4	Étendu à l'aide de RFC
Change, RFC 2307	shadowLastChange 1.3.6.1.1.1.1.5	Pas de mappage
Expire, RFC 2307	shadowExpire 1.3.6.1.1.1.1.10	Pas de mappage
UniqueID, RFC 2307	uidNumber 1.3.6.1.1.1.1.0	Généré à partir de GUID
NFSHomeDirectory, RFC 2307	homeDirectory 1.3.6.1.1.1.1.3	Généré à partir de homeDirectory
PrimaryGroupID, RFC 2307	gidNumber 1.3.6.1.1.1.1.1	Étendu à l'aide de RFC ou généré à partir de GUID
SMBAccountFlags, enregistré par Samba, Apple PDC	acctFlags 1.3.6.1.4.1.7165.2.1.4	1.2.840.113556.1.4.302 (Microsoft)
SMBPasswordLastSet, enregistré par Samba, Apple PDC	pwdLastSet 1.3.6.1.4.1.7165.2.1.3	1.2.840.113556.1.4.96 (Microsoft)
SMBLogonTime, enregistré par Samba, Apple PDC	logonTime 1.3.6.1.4.1.7165.2.1.5	1.2.840.113556.1.4.52 (Microsoft)
SMBLogoffTime, enregistré par Samba, Apple PDC	logoffTime 1.3.6.1.4.1.7165.2.1.6	1.2.840.113556.1.4.51 (Microsoft)

Nom Open Directory, RFC/classe, emploi spécial	OID de nom d'attribut LDAP	Module externe Active Directory
SMBKickoffTime, enregistré par Samba, Apple PDC	kickoffTime 1.3.6.1.4.1.7165.2.1.7	Pas de mappage
SMBHomeDrive, enregistré par Samba, Apple PDC	homeDrive 1.3.6.1.4.1.7165.2.1.10	1.2.840.113556.1.4.45 (Microsoft)
SMBScriptPath, enregistré par Samba, Apple PDC	scriptPath 1.3.6.1.4.1.7165.2.1.11	1.2.840.113556.1.4.62 (Microsoft)
SMBProfilePath, enregistré par Samba, Apple PDC	profilePath 1.3.6.1.4.1.7165.2.1.12	1.2.840.113556.1.4.139 (Microsoft)
SMBUserWorkstations, enregistré par Samba, Apple PDC	userWorkstations 1.3.6.1.4.1.7165.2.1.13	1.2.840.113556.1.4.86 (Microsoft)
SMBHome, enregistré par Samba, Apple PDC	smbHome 1.3.6.1.4.1.7165.2.1.17	1.2.840.113556.1.4.44 (Microsoft)
SMBRID, enregistré par Samba, Apple PDC	rid 1.3.6.1.4.1.7165.2.1.14	1.2.840.113556.1.4.153 (Microsoft)
SMBGroupRID, enregistré par Samba, Apple PDC	primaryGroupID 1.3.6.1.4.1.7165.2.1.15	1.2.840.113556.1.4.98 (Microsoft)
FaxNumber, RFC 2256	fax 2.5.4.23	Standard RFC
MobileNumber, RFC 1274	mobile 0.9.2342.19200300.100.1.41	Standard RFC
PagerNumber, RFC 1274	pager 0.9.2342.19200300.100.1.42	Standard RFC
Department, RFC 2798,	departmentNumber 2.16.840.1.113730.3.1.2	1.2.840.113556.1.2.141 (Microsoft)
NickName, Microsoft Attribute		1.2.840.113556.1.2.447 (Microsoft)
JobTitle, RFC 2256	title 2.5.4.12	Standard RFC
Building, RFC 2256	buildingName 2.5.4.19	Standard RFC
Country, RFC 2256	c 2.5.4.6	Standard RFC
Street, RFC 2256	street 2.5.4.9	1.2.840.113556.1.2.256 (Microsoft)

Nom Open Directory, RFC/classe, emploi spécial	OID de nom d'attribut LDAP	Module externe Active Directory
City, RFC 2256	locality 2.5.4.7	Standard RFC
State, RFC 2256	st 2.5.4.8	Standard RFC

Mappages de groupes (Groups)

Les tableaux suivants spécifient la manière dont le module LDAPv3 de Format de répertoire mappe le type d'enregistrements et les attributs de groupes Open Directory sur les classes d'objets LDAP. Les tableaux spécifient également la manière dont le module Active Directory de Format de répertoire mappe et génère des attributs et des catégories d'objets Active Directory à partir d'attributs et de types d'enregistrements Open Directory.

Mappages des types d'enregistrements de groupes (Groups)

Nom Open Directory, RFC/classe	OID de nom de classe d'objets LDAP	Module externe Active Directory
Groups, RFC 2307	posixGroup 1.3.6.1.1.1.2.2	objectCategory = Group
Groups, enregistré par Apple	apple-group 1.3.6.1.4.1.63.1000.1.1.2.14	schéma étendu Apple

Mappage des attributs de groupes (Groups)

Nom Open Directory, RFC/classe	OID de nom d'attribut LDAP	Module externe Active Directory
RecordName, RFC 2256	cn 2.5.4.3	Standard RFC
HomeDirectory, enregistré par Apple	apple-group-homeurl 1.3.6.1.4.1.63.1000.1.1.1.14.1	schéma étendu Apple
HomeLocOwner, enregistré par Apple	apple-group-homeowner 1.3.6.1.4.1.63.1000.1.1.1.14.2	schéma étendu Apple
MCXFlags, enregistré par Apple	apple-mcxflags 1.3.6.1.4.1.63.1000.1.1.1.1.10	schéma étendu Apple
MCXSettings, enregistré par Apple	apple-mcxsettings 1.3.6.1.4.1.63.1000.1.1.1.1.16	schéma étendu Apple
RealName, enregistré par Apple	apple-group-realname 1.3.6.1.4.1.63.1000.1.1.1.14.5	1.2.840.113556.1.2.13 (Microsoft)
Picture, enregistré par Apple	apple-user-picture 1.3.6.1.4.1.63.1000.1.1.1.1.12	schéma étendu Apple
Keywords, enregistré par Apple	apple-keyword 1.3.6.1.4.1.63.1000.1.1.1.1.19	schéma étendu Apple

Nom Open Directory, RFC/classe	OID de nom d'attribut LDAP	Module externe Active Directory
GeneratedUID, enregistré par Apple	apple-generateduid 1.3.6.1.4.1.63.1000.1.1.1.20	À partir de GUID — formaté
GroupMembership, RFC 2307	memberUid 1.3.6.1.1.1.1.12	Généré à partir de member
Member, RFC 2307	memberUid 1.3.6.1.1.1.1.12	Idem GroupMembership
PrimaryGroupID, RFC 2307	gidNumber 1.3.6.1.1.1.1.1	Étendu à l'aide de RFC ou généré à partir de GUID

Mappages de montages (Mounts)

Les tableaux suivants spécifient la manière dont le module LDAPv3 de Format de répertoire mappe le type d'enregistrements et les attributs de montage (Mounts) Open Directory sur les classes d'objets et attributs LDAP. Les tableaux spécifient également la manière dont le module Active Directory de Format de répertoire mappe et génère des attributs et des catégories d'objets Active Directory à partir d'attributs et de types d'enregistrements Open Directory.

Mappages des types d'enregistrements de montages (Mounts)

Nom Open Directory, RFC/classe	OID de nom de classe d'objets LDAP	Module externe Active Directory
Mounts, enregistré par Apple	mount 1.3.6.1.4.1.63.1000.1.1.2.8	schéma étendu Apple

Mappages des attributs de montages (Mounts)

Nom Open Directory, RFC/classe	OID de nom d'attribut LDAP	Module externe Active Directory
RecordName, RFC 2256	cn 2.5.4.3	Standard RFC
VFSLinkDir, enregistré par Apple	mountDirectory 1.3.6.1.4.1.63.1000.1.1.1.8.1	schéma étendu Apple
VFSOpts, enregistré par Apple	mountOption 1.3.6.1.4.1.63.1000.1.1.1.8.3	schéma étendu Apple
VFSType, enregistré par Apple	mountType 1.3.6.1.4.1.63.1000.1.1.1.8.2	schéma étendu Apple
VFSDumpFreq, enregistré par Apple	mountDumpFrequency 1.3.6.1.4.1.63.1000.1.1.1.8.4	schéma étendu Apple
VFSPassNo, enregistré par Apple	mountPassNo 1.3.6.1.4.1.63.1000.1.1.1.8.5	schéma étendu Apple

Mappages d'ordinateurs (Computers)

Les tableaux suivants spécifient la manière dont le module LDAPv3 de Format de répertoire mappe le type d'enregistrements et les attributs d'ordinateurs (Computers) Open Directory sur les classes d'objets LDAP. Les tableaux spécifient également la manière dont le module Active Directory de Format de répertoire mappe et génère des attributs et des catégories d'objets Active Directory à partir d'attributs et de types d'enregistrements Open Directory.

Mappages des types d'enregistrements d'ordinateurs (Computers)

Nom Open Directory, RFC/classe	OID de nom de classe d'objets LDAP	Module externe Active Directory
Computers, enregistré par Apple	apple-computer 1.3.6.1.4.1.63.1000.1.1.2.10	objectCategory = Computer

Mappages des attributs d'ordinateurs (Computers)

Nom Open Directory, RFC/classe, emploi spécial	OID de nom d'attribut LDAP	Module externe Active Directory
RecordName, RFC 2256	cn 2.5.4.3	Standard RFC
RealName, enregistré par Apple	apple-realname 1.3.6.1.4.1.63.1000.1.1.1.10.2	1.2.840.113556.1.2.13 (Microsoft)
MCXFlags, enregistré par Apple	apple-mcxflags 1.3.6.1.4.1.63.1000.1.1.1.1.10	schéma étendu Apple
MCXSettings, enregistré par Apple	apple-mcxsettings 1.3.6.1.4.1.63.1000.1.1.1.1.16	schéma étendu Apple
Group, enregistré par Apple	apple-computer-list-groups 1.3.6.1.4.1.63.1000.1.1.1.11.4	schéma étendu Apple
AuthenticationAuthority, enregistré par Apple	authAuthority 1.3.6.1.4.1.63.1000.1.1.2.16.1	schéma étendu Apple
GeneratedUID, enregistré par Apple	apple-generateduid 1.3.6.1.4.1.63.1000.1.1.1.1.20	À partir de GUID — formaté
XMLPlist, enregistré par Apple	apple-xmlplist 1.3.6.1.4.1.63.1000.1.1.1.17.1	schéma étendu Apple
Comment, RFC 2256	description 2.5.4.13	Standard RFC
ENetAddress, RFC 2307	macAddress 1.3.6.1.1.1.1.22	Étendu à l'aide de RFC
UniqueID, RFC 2307	uidNumber 1.3.6.1.1.1.1.0	Généré à partir de GUID
PrimaryGroupID, RFC 2307	gidNumber 1.3.6.1.1.1.1.1	Étendu à l'aide de RFC ou généré
SMBAccountFlags, enregistré par Samba, Apple PDC	acctFlags 1.3.6.1.4.1.7165.2.1.4	1.2.840.113556.1.4.302 (Microsoft)

Nom Open Directory, RFC/classe, emploi spécial	OID de nom d'attribut LDAP	Module externe Active Directory
SMBPasswordLastSet, enregistré par Samba, Apple PDC	pwdLastSet 1.3.6.1.4.1.7165.2.1.3	1.2.840.113556.1.4.96 (Microsoft)
SMBLogonTime, enregistré par Samba, Apple PDC	logonTime 1.3.6.1.4.1.7165.2.1.5	1.2.840.113556.1.4.52 (Microsoft)
SMBLogoffTime, enregistré par Samba, Apple PDC	logoffTime 1.3.6.1.4.1.7165.2.1.6	1.2.840.113556.1.4.51 (Microsoft)
SMBKickoffTime, enregistré par Samba, Apple PDC	kickoffTime 1.3.6.1.4.1.7165.2.1.7	Pas de mappage
SMBRID, enregistré par Samba, Apple PDC	rid 1.3.6.1.4.1.7165.2.1.14	1.2.840.113556.1.4.153 (Microsoft)
SMBGroupID, enregistré par Samba, Apple PDC	primaryGroupID 1.3.6.1.4.1.7165.2.1.15	1.2.840.113556.1.4.98 (Microsoft)

Mappages de listes d'ordinateurs (ComputerLists)

Les tableaux suivants spécifient la manière dont le module LDAPv3 de Format de répertoire mappe le type d'enregistrements et les attributs de listes d'ordinateurs (ComputerLists) Open Directory sur les classes d'objets LDAP. Les tableaux spécifient également la manière dont le module Active Directory de Format de répertoire mappe et génère des attributs et des catégories d'objets Active Directory à partir d'attributs et de types d'enregistrements Open Directory.

Mappages des types d'enregistrements de listes d'ordinateurs (ComputerLists)

Nom Open Directory, RFC/classe	OID de nom de classe d'objets LDAP	Module externe Active Directory
ComputerLists, enregistré par Apple	apple-computer-list 1.3.6.1.4.1.63.1000.1.1.2.11	schéma étendu Apple

Mappages des attributs pour listes d'ordinateurs (ComputerLists)

Nom Open Directory, RFC/classe,	OID de nom d'attribut LDAP	Module externe Active Directory
RecordName, RFC 2256	cn 2.5.4.3	Standard RFC
MCXFlags, enregistré par Apple	apple-mcxflags 1.3.6.1.4.1.63.1000.1.1.1.1.10	schéma étendu Apple
MCXSettings, enregistré par Apple	apple-mcxsettings 1.3.6.1.4.1.63.1000.1.1.1.1.16	schéma étendu Apple

Nom Open Directory, RFC/classe,	OID de nom d'attribut LDAP	Module externe Active Directory
Computers, enregistré par Apple	apple-computers 1.3.6.1.4.1.63.1000.1.1.1.11.3	schéma étendu Apple
Group, enregistré par Apple	apple-computer-list-groups 1.3.6.1.4.1.63.1000.1.1.1.11.4	schéma étendu Apple
Keywords, enregistré par Apple	apple-keyword 1.3.6.1.4.1.63.1000.1.1.1.1.19	schéma étendu Apple

Mappages de configurations (Config)

Les tableaux suivants spécifient la manière dont le module LDAPv3 de Format de répertoire mappe le type d'enregistrements et les attributs de configurations (Config) Open Directory sur les classes d'objets LDAP. Les tableaux spécifient également la manière dont le module Active Directory de Format de répertoire mappe et génère des attributs et des catégories d'objets Active Directory à partir d'attributs et de types d'enregistrements Open Directory.

Mappages des types d'enregistrements de configurations (Config)

Nom Open Directory, RFC/classe	OID de nom de classe d'objets LDAP	Module externe Active Directory
Config, enregistré par Apple	apple-configuration 1.3.6.1.4.1.63.1000.1.1.2.12	schéma étendu Apple

Mappages des attributs de configurations (Config)

Nom Open Directory, RFC/classe, emploi spécial	OID de nom d'attribut LDAP	Module externe Active Directory
RecordName, RFC 2256	cn 2.5.4.3	Standard RFC
RealName, enregistré par Apple	apple-config-realname 1.3.6.1.4.1.63.1000.1.1.1.12.3	1.2.840.113556.1.2.13 (Microsoft)
DataStamp, enregistré par Apple	apple-data-stamp 1.3.6.1.4.1.63.1000.1.1.1.12.2	schéma étendu Apple
KDCAuthKey, enregistré par Apple, Apple KDC	apple-kdc-authkey 1.3.6.1.4.1.63.1000.1.1.1.12.7	Pas de mappage
KDCConfigData, enregistré par Apple, Apple KDC	apple-kdc-configdata 1.3.6.1.4.1.63.1000.1.1.1.12.8	Pas de mappage
Keywords, enregistré par Apple	apple-keyword 1.3.6.1.4.1.63.1000.1.1.1.1.19	schéma étendu Apple
LDAPReadReplicas, enregistré par Apple, Apple LDAP Server	apple-ldap-replica 1.3.6.1.4.1.63.1000.1.1.1.12.5	Pas de mappage

Nom Open Directory, RFC/classe, emploi spécial	OID de nom d'attribut LDAP	Module externe Active Directory
LDAPWriteReplicas, enregistré par Apple, Apple LDAP Server	apple-ldap-writable-replica 1.3.6.1.4.1.63.1000.1.1.1.12.6	Pas de mappage
PasswordServerList, enregistré par Apple, Serveur de mots de passe	apple-password-server-list 1.3.6.1.4.1.63.1000.1.1.1.12.4	Pas de mappage
PasswordServerLocation, enregistré par Apple, Serveur de mots de passe	apple-password-server-location 1.3.6.1.4.1.63.1000.1.1.1.12.1	Pas de mappage
XMLPlist, enregistré par Apple	apple-xmlplist 1.3.6.1.4.1.63.1000.1.1.1.17.1	schéma étendu Apple

Mappages de personnes (People)

Les tableaux suivants spécifient la manière dont le module LDAPv3 de Format de répertoire mappe le type d'enregistrement et les attributs de personnes (People) Open Directory sur les classes d'objets LDAP. Les tableaux spécifient également la manière dont le module Active Directory de Format de répertoire mappe et génère des attributs et des catégories d'objets Active Directory à partir d'attributs et de types d'enregistrements Open Directory.

Mappages des types d'enregistrements de personnes (People)

Nom Open Directory, RFC/classe	OID de nom de classe d'objets LDAP	Module externe Active Directory
People, RFC 2798	inetOrgPerson 2.16.840.1.113730.3.2.2	Standard RFC

Mappage des attributs de personnes (People)

Nom Open Directory, RFC/classe	OID de nom d'attribut LDAP	Module externe Active Directory
RecordName, RFC 2256	cn 2.5.4.3	Standard RFC
EMailAddress, RFC 1274	mail 0.9.2342.19200300.100.1.3	Standard RFC
RealName, RFC 2256	cn 1.2.840.113556.1.3.23	Standard RFC
LastName, RFC 2256	sn 2.5.4.4	Standard RFC
FirstName, RFC 2256	givenName 2.5.4.42	Standard RFC
FaxNumber, RFC 2256	fax 2.5.4.23	Standard RFC

Nom Open Directory, RFC/classe	OID de nom d'attribut LDAP	Module externe Active Directory
MobileNumber, RFC 1274	mobile 0.9.2342.19200300.100.1.41	Standard RFC
PagerNumber, RFC 1274	pager 0.9.2342.19200300.100.1.42	Standard RFC
Department, RFC 2798,	departmentNumber 2.16.840.1.113730.3.1.2	1.2.840.113556.1.2.141 (Microsoft)
JobTitle, RFC 2256	title 2.5.4.12	Standard RFC
PhoneNumber, RFC 2256	telephoneNumber 2.5.4.20	Standard RFC
AddressLine1, RFC 2256	street 2.5.4.9	Standard RFC
Street, RFC 2256	street 2.5.4.9	Standard RFC
PostalAddress, RFC 2256	postalAddress 2.5.4.16	Standard RFC
City, RFC 2256	locality 2.5.4.7	Standard RFC
State, RFC 2256	st 2.5.4.8	Standard RFC
Country, RFC 2256	c 2.5.4.6	Standard RFC
PostalCode, RFC 2256	postalCode 2.5.4.17	Standard RFC
OrganizationName, RFC 2256	o 2.5.4.10	1.2.840.113556.1.2.146 (Microsoft)

Mappages de listes d'ordinateurs préréglés (PresetComputerLists)

Les tableaux suivants spécifient la manière dont le module LDAPv3 de Format de répertoire mappe le type d'enregistrements et les attributs de listes d'ordinateurs préréglés (PresetComputerLists) Open Directory sur les classes d'objets LDAP. Les tableaux spécifient également la manière dont le module Active Directory de Format de répertoire mappe et génère des attributs et des catégories d'objets Active Directory à partir d'attributs et de types d'enregistrements Open Directory.

Mappages des types d'enregistrements de listes d'ordinateurs préréglés (PresetComputerLists)

Nom Open Directory, RFC/classe	OID de nom de classe d'objets LDAP	Module externe Active Directory
PresetComputerLists, enregistré par Apple	apple-preset-computer-list 1.3.6.1.4.1.63.1000.1.1.2.13	schéma étendu Apple

Mappages des attributs de listes d'ordinateurs préréglés (PresetComputerLists)

Nom Open Directory, RFC/classe	OID de nom d'attribut LDAP	Module externe Active Directory
RecordName, RFC 2256	cn 2.5.4.3	Standard RFC
MCXFlags, enregistré par Apple	apple-mcxflags 1.3.6.1.4.1.63.1000.1.1.1.10	schéma étendu Apple
MCXSettings, enregistré par Apple	apple-mcxsettings 1.3.6.1.4.1.63.1000.1.1.1.16	schéma étendu Apple
Keywords, enregistré par Apple	apple-keyword 1.3.6.1.4.1.63.1000.1.1.1.19	schéma étendu Apple

Mappages de groupes préréglés (PresetGroups)

Les tableaux suivants spécifient la manière dont le module LDAPv3 de Format de répertoire mappe le type d'enregistrements et les attributs de groupes préréglés (PresetGroups) Open Directory sur les classes d'objets LDAP. Les tableaux spécifient également la manière dont le module Active Directory de Format de répertoire mappe et génère des attributs et des catégories d'objets Active Directory à partir d'attributs et de types d'enregistrements Open Directory.

Mappages des types d'enregistrements de groupes préréglés (PresetGroups)

Nom Open Directory, RFC/classe	OID de nom de classe d'objets LDAP	Module externe Active Directory
PresetGroups, enregistré par Apple	apple-preset-group 1.3.6.1.4.1.63.1000.1.1.3.14	schéma étendu Apple

Mappages des attributs de groupes préréglés (PresetGroups)

Nom Open Directory, RFC/classe	OID de nom d'attribut LDAP	Module externe Active Directory
HomeDirectory, enregistré par Apple	apple-group-homeurl 1.3.6.1.4.1.63.1000.1.1.1.6	schéma étendu Apple
HomeLocOwner, enregistré par Apple	apple-group-homeowner 1.3.6.1.4.1.63.1000.1.1.1.14.2	schéma étendu Apple
MCXFlags, enregistré par Apple	apple-mcxflags 1.3.6.1.4.1.63.1000.1.1.1.10	schéma étendu Apple
MCXSettings, enregistré par Apple	apple-mcxsettings 1.3.6.1.4.1.63.1000.1.1.1.16	schéma étendu Apple
RealName, enregistré par Apple	apple-group-realname 1.3.6.1.4.1.63.1000.1.1.1.14.5	schéma étendu Apple
Keywords, enregistré par Apple	apple-keyword 1.3.6.1.4.1.63.1000.1.1.1.19	schéma étendu Apple
RecordName, RFC 2256	cn 2.5.4.3	Standard RFC

Nom Open Directory, RFC/classe	OID de nom d'attribut LDAP	Module externe Active Directory
GroupMembership, RFC 2307	memberUid 1.3.6.1.1.1.1.12	Étendu à l'aide de RFC
PrimaryGroupID, RFC 2307	gidNumber 1.3.6.1.1.1.1.1	Étendu à l'aide de RFC

Mappages d'utilisateurs préréglés (PresetUsers)

Les tableaux suivants spécifient la manière dont le module LDAPv3 de Format de répertoire mappe le type d'enregistrements et les attributs d'utilisateurs préréglés (PresetUsers) Open Directory sur les classes d'objets LDAP. Les tableaux spécifient également la manière dont le module Active Directory de Format de répertoire mappe et génère des attributs et des catégories d'objets Active Directory à partir d'attributs et de types d'enregistrements Open Directory.

Mappages des types d'enregistrements d'utilisateurs préréglés (PresetUsers)

Nom Open Directory, RFC/classe	OID de nom de classe d'objets LDAP	Module externe Active Directory
PresetUsers, enregistré par Apple	apple-preset-user 1.3.6.1.4.1.63.1000.1.1.2.15	ObjectCategory = Person

Mappages des attributs d'utilisateurs préréglés (PresetUsers)

Nom Open Directory, RFC/classe	OID de nom d'attribut LDAP	Module externe Active Directory
HomeDirectory, enregistré par Apple	apple-user-homeurl 1.3.6.1.4.1.63.1000.1.1.1.6	n/d
HomeDirectoryQuota, enregistré par Apple	apple-user-homequota 1.3.6.1.4.1.63.1000.1.1.1.8	schéma étendu Apple
HomeDirectorySoftQuota, enregistré par Apple	apple-user-homesoftquota 1.3.6.1.4.1.63.1000.1.1.1.17	schéma étendu Apple
MailAttribute, enregistré par Apple	apple-user-mailattribute 1.3.6.1.4.1.63.1000.1.1.1.9	schéma étendu Apple
PrintServiceUserData, enregistré par Apple	apple-user-printattribute 1.3.6.1.4.1.63.1000.1.1.1.13	schéma étendu Apple
MCXFlags, enregistré par Apple	apple-mcxflags 1.3.6.1.4.1.63.1000.1.1.1.10	schéma étendu Apple
MCXSettings, enregistré par Apple	apple-mcxsettings 1.3.6.1.4.1.63.1000.1.1.1.16	schéma étendu Apple
AdminLimits, enregistré par Apple	apple-user-adminlimits 1.3.6.1.4.1.63.1000.1.1.1.14	schéma étendu Apple
Picture, enregistré par Apple	apple-user-picture 1.3.6.1.4.1.63.1000.1.1.1.12	schéma étendu Apple
AuthenticationAuthority, enregistré par Apple	authAuthority 1.3.6.1.4.1.63.1000.1.1.2.16.1	schéma étendu Apple

Nom Open Directory, RFC/classe	OID de nom d'attribut LDAP	Module externe Active Directory
PasswordPolicyOptions, enregistré par Apple	apple-user-passwordpolicy 1.3.6.1.4.1.63.1000.1.1.1.18	schéma étendu Apple
PresetUserIsAdmin, enregistré par Apple	apple-preset-user-is-admin 1.3.6.1.4.1.63.1000.1.1.1.15.1	schéma étendu Apple
Keywords, enregistré par Apple	apple-keyword 1.3.6.1.4.1.63.1000.1.1.1.1.19	schéma étendu Apple
RecordName, RFC 1274	cn 2.5.4.3	Standard RFC
RealName, RFC 2256	cn 2.5.4.3	Standard RFC
Password, RFC 2256	userPassword 2.5.4.35	n/d
GroupMembership, RFC 2307	memberUid 1.3.6.1.1.1.1.12	Étendu à l'aide de RFC
PrimaryGroupID, RFC 2307	gidNumber 1.3.6.1.1.1.1.1	Étendu à l'aide de RFC
NFSHomeDirectory, RFC 2307	homeDirectory 1.3.6.1.1.1.1.3	n/d
UserShell, RFC 2307	loginShell 1.3.6.1.1.1.1.4	Étendu à l'aide de RFC
Change, RFC 2307	shadowLastChange 1.3.6.1.1.1.1.5	n/d
Expire, RFC 2307	shadowExpire 1.3.6.1.1.1.1.10	n/d

Mappages d'imprimantes (Printers)

Les tableaux suivants spécifient la manière dont le module LDAPv3 de Format de répertoire mappe le type d'enregistrements et les attributs d'imprimantes (Printers) Open Directory sur les classes d'objets LDAP. Les tableaux spécifient également la manière dont le module Active Directory de Format de répertoire mappe et génère des attributs et des catégories d'objets Active Directory à partir d'attributs et de types d'enregistrements Open Directory.

Mappages des types d'enregistrements d'imprimantes (Printers)

Nom Open Directory, RFC/classe	OID de nom de classe d'objets LDAP	Module externe Active Directory
Printers, enregistré par Apple	apple-printer 1.3.6.1.4.1.63.1000.1.1.2.9	ObjectCategory = Print-Queue
Printers, IETF-Draft-IPP-LDAP	printerIPP 1.3.18.0.2.6.256	

Mappages des attributs d'imprimantes (Printers)

Nom Open Directory, RFC/classe, emploi spécial	OID de nom d'attribut LDAP	Module externe Active Directory
RecordName, RFC 2256	cn 2.5.4.3	Standard RFC
RealName, RFC 2256	cn 2.5.4.3	1.2.840.113556.1.4.300 (Microsoft)
PrinterLPRHost, enregistré par Apple, gestion héritée	apple-printer-lprhost 1.3.6.1.4.1.63.1000.1.1.1.9.2	n/d
PrinterLPRQueue, enregistré par Apple, gestion héritée	apple-printer-lprqueue 1.3.6.1.4.1.63.1000.1.1.1.9.3	n/d
PrinterType, enregistré par Apple, gestion héritée	apple-printer-type 1.3.6.1.4.1.63.1000.1.1.1.9.4	n/d
PrinterNote, enregistré par Apple, gestion héritée	apple-printer-note 1.3.6.1.4.1.63.1000.1.1.1.9.5	n/d
Location, IETF-Draft-IPP-LDAP	printer-location 1.3.18.0.2.4.1136	1.2.840.113556.1.4.222 (Microsoft)
Comment, RFC 2256	description 2.5.4.13	Standard RFC
PrinterMakeAndModel, IETF-Draft-IPP-LDAP	printer-make-and-model 1.3.18.0.2.4.1138	1.2.840.113556.1.4.229 (Microsoft)
PrinterURI, IETF-Draft-IPP-LDAP	printer-uri 1.3.18.0.2.4.1140	Généré à partir de uNCName
PrinterXRISupported, IETF-Draft-IPP-LDAP	printer-xri-supported 1.3.18.0.2.4.1107	Généré à partir de portName/ uNCName
Printer1284DeviceID, enregistré par Apple	printer-1284-device-id 1.3.6.1.4.1.63.1000.1.1.1.9.6	schéma étendu Apple

Mappages de configurations automatiques de serveur (AutoServerSetup)

Les tableaux suivants spécifient la manière dont le module LDAPv3 de Format de répertoire mappe le type d'enregistrements et les attributs de configurations automatiques de serveur (AutoServerSetup) Open Directory sur les classes d'objets LDAP. Les tableaux spécifient également la manière dont le module Active Directory de Format de répertoire mappe et génère des attributs et des catégories d'objets Active Directory à partir d'attributs et de types d'enregistrements Open Directory.

Mappages des types d'enregistrements de configurations automatiques de serveur (AutoServerSetup)

Nom Open Directory, RFC/classe	OID de nom de classe d'objets LDAP	Module externe Active Directory
AutoServerSetup, enregistré par Apple	apple-serverassistant-config 1.3.6.1.4.1.63.1000.1.1.2.17	schéma étendu Apple

Mappages des attributs d'enregistrements de configurations automatiques de serveur (AutoServerSetup)

Nom Open Directory, RFC/classe	OID de nom d'attribut LDAP	Module externe Active Directory
RecordName, RFC 2256	cn 2.5.4.3	Standard RFC
XMLPlist, enregistré par Apple	apple-xmlplist 1.3.6.1.4.1.63.1000.1.1.1.17.1	schéma étendu Apple

Mappages d'emplacements (Locations)

Les tableaux suivants spécifient la manière dont le module LDAPv3 de Format de répertoire mappe le type d'enregistrements et les attributs d'emplacements (Locations) Open Directory sur les classes d'objets LDAP. Les tableaux spécifient également la manière dont le module Active Directory de Format de répertoire mappe et génère des attributs et des catégories d'objets Active Directory à partir d'attributs et de types d'enregistrements Open Directory.

Mappages des types d'enregistrements d'emplacements (Locations)

Nom Open Directory, RFC/classe	OID de nom de classe d'objets LDAP	Module externe Active Directory
Locations, enregistré par Apple	apple-locations 1.3.6.1.4.1.63.1000.1.1.2.18	schéma étendu Apple

Mappages des attributs d'emplacements (Locations)

Nom Open Directory, RFC/classe	OID de nom d'attribut LDAP	Module externe Active Directory
RecordName, RFC 2256	cn 2.5.4.3	Standard RFC
DNSDomain, enregistré par Apple	apple-dns-domain 1.3.6.1.4.1.63.1000.1.1.1.18.1	schéma étendu Apple
DNSNameServer, enregistré par Apple	apple-dns-nameserver 1.3.6.1.4.1.63.1000.1.1.1.18.2	schéma étendu Apple

Types d'enregistrements et attributs Open Directory standard

Pour plus d'informations sur les types d'enregistrements et les attributs standard dans les domaines Open Directory, consultez les sections suivantes :

- "Attributs standard dans les enregistrements d'utilisateurs" à la page 236.
- "Attributs standard dans les enregistrements de groupes" à la page 242.
- "Attributs standard dans les enregistrements d'ordinateurs" à la page 243.
- "Attributs standard dans les enregistrements de listes d'ordinateurs" à la page 244.
- "Attributs standard dans les enregistrements de montages" à la page 245.
- "Attributs standard dans les enregistrements de configurations" à la page 246.

Pour obtenir une liste complète des types d'enregistrements et des attributs standard, consultez le fichier suivant :

/System/Library/Frameworks/DirectoryService.framework/Headers/DirServicesConst.h

Attributs standard dans les enregistrements d'utilisateurs

Le tableau suivant décrit les attributs standard figurant dans les enregistrements d'utilisateurs Open Directory. Utilisez ces informations lorsque vous travaillez dans la sous-fenêtre Inspecteur de Gestionnaire de groupe de travail ou lorsque vous mappez des attributs d'enregistrements d'utilisateurs avec Format de répertoire.

Important : lors du mappage des attributs d'utilisateurs Mac OS X sur un domaine de répertoire LDAP en lecture/écriture (un domaine LDAP qui n'est pas en lecture seule), ne mappez pas l'attribut RealName et le premier attribut RecordName sur le même attribut LDAP. Par exemple, ne mappez pas à la fois RealName et RecordName sur l'attribut cn. Si RealName et RecordName sont mappés sur le même attribut LDAP, des problèmes se produiront lorsque vous essaierez de modifier le nom complet ou le premier nom abrégé dans Gestionnaire de groupe de travail.

Attribut d'utilisateur Mac OS X	Format	Exemples
Nom de l'entrée : Liste de noms associée à un utilisateur ; le premier est le nom abrégé de l'utilisateur, qui est également le nom de son répertoire de départ. *IMPORTANT* Tous les attributs utilisés pour l'authentification doivent être mappés sur RecordName.	Première valeur : caractères ASCII de A à Z, a à z, 0 à 9, _,- Deuxième valeur : texte romain UTF-8	Jean Jean D. J. Dupont Longueur non nulle, 1 à 16 valeurs. Maximum 255 octets (de 85 caractères triple octets à 255 caractères d'un octet) par instance. La première valeur doit comprendre entre 1 à 30 octets pour les clients utilisant Gestionnaire Macintosh, entre 1 à 8 octets pour les clients utilisant Mac OS X version 10.1 et antérieures.
Nom réel : Un nom, habituellement le nom complet de l'utilisateur ; non utilisé pour l'authentification.	Texte UTF-8	Jean Dupont. Longueur non nulle, maximum 255 octets (de 85 caractères triple octets à 255 caractères d'un octet).
Identifiant unique : Identifiant utilisateur unique, utilisé pour la gestion des autorisations d'accès.	Chaîne ASCII signée à 32 bits, composée de chiffres de 0 à 9	Les valeurs inférieures à 500 peuvent avoir une signification particulière. Les valeurs inférieures à 100 sont généralement attribuées aux comptes de système. Zéro est réservé au système. Normalement unique par rapport aux autres utilisateurs mais parfois en double. Avertissement : une valeur non entière est interprétée comme un 0, c'est-à-dire l'identificateur unique de l'utilisateur root.
Identifiant de groupe principal : Association de groupe principal d'utilisateur	Chaîne ASCII signée à 32 bits, composée de chiffres de 0 à 9	Plage de 1 à 2.147.483.648 Normalement unique par rapport aux autres entrées du groupe. Si vide, la valeur supposée est 20.

Attribut d'utilisateur Mac OS X	Format	Exemples
Répertoire d'accueil NFS : Chemin d'accès au répertoire de départ de l'utilisateur, dans le système de fichiers local	Texte UTF-8	/Network/Servers/example/Users/K-M/Tom King Longueur non nulle. Maximum 255 octets.
Répertoire d'accueil Emplacement d'un répertoire de départ AFP	Texte XML UTF-8	<home_dir> <url>afp://*server/sharept*</url> <path>*usershomedir*</path> </home_dir> Dans l'exemple ci-dessous, le répertoire d'accueil de Tom King est K-M/Tom King, qui réside en dessous du répertoire du point de partage, Utilisateurs : <home_dir> <url>afp://example.com/Users</url> <path>K-M/Tom King</path> </home_dir>
HomeDirectoryQuota : Quota de disque du répertoire de départ de l'utilisateur	Texte indiquant le nombre d'octets autorisés	Si le quota est de 10 Mo, la valeur sera la chaîne de texte "1048576".
Attribut de courrier : Configuration du service de courrier d'un utilisateur	Texte XML UTF-8	
PrintServiceUserData : Statistiques du quota d'impression d'un utilisateur	plist XML UTF-8, valeur unique	.
MCXFlags : S'il est présent, MCXSettings est chargé ; s'il est absent, MCXSettings n'est pas chargé ; requis pour un utilisateur géré.	plist XML UTF-8, valeur unique	
Réglages MCX : Préférences gérées d'un utilisateur	plist XML UTF-8, valeurs multiples	
AdminLimits : Autorisations accordées par Gestionnaire de groupe de travail à un utilisateur qui peut administrer le domaine de répertoire	plist XML UTF-8, valeur unique	
Mot de passe : Mot de passe de l'utilisateur	Cryptage UNIX	

Attribut d'utilisateur Mac OS X	Format	Exemples
Image : Chemin d'accès à un fichier d'image reconnu qui constituera l'image affichée pour l'utilisateur	Texte UTF-8	Maximum 255 octets.
Commentaires : Toute documentation que vous choisissez	Texte UTF-8	Jean est responsable du marketing Maximum 32 676 octets.
Shell utilisateur : L'emplacement du shell par défaut pour l'envoi de commandes au serveur	Chemin d'accès	/bin/tcsh /bin/sh Aucun (cette valeur empêche les utilisateurs possédant des comptes dans le domaine de répertoire d'accéder à distance au serveur via une ligne de commande) Longueur non nulle.
Change : Inutilisé par Mac OS X mais correspond à une partie du schéma LDAP standard	Nombre	
Expire : Inutilisé par Mac OS X mais correspond à une partie du schéma LDAP standard	Nombre	
Droit d'authentification : Décrit les méthodes d'authentification de l'utilisateur, comme, par exemple, Open Directory, Mot de passe shadow ou Mot de passe crypté. Pas obligatoire pour un utilisateur qui ne possède qu'un mot de passe crypté ; lorsque cet attribut est absent, c'est l'authentification héritée qui est utilisée (cryptée avec le Gestionnaire d'authentification, s'il est disponible).	Texte ASCII	Les valeurs décrivent les méthodes d'authentification d'utilisateur. Peut être multivalué (par exemple ;ApplePasswordServer; et ;Kerberosv5;). Chaque valeur a le format *vers*; *balise*; *données* (où *vers* et *données* peuvent être vides). **Mot de passe crypté :** ;basic; **Mot de passe Open Directory :** ;ApplePasswordServer; *HexID, clé publique du serveur IPaddress*:*port* ;Kerberosv5;*données Kerberos* **Mot de passe shadow** (domaine de répertoire local uniquement) : • ;ShadowHash; • ;ShadowHash;<*liste des méthodes d'authentification activées*>

Attribut d'utilisateur Mac OS X	Format	Exemples
Indice d'authentification : Texte défini par l'utilisateur pour être affiché à titre d'indice de mot de passe	Texte UTF-8	Vous avez vu juste. Maximum 255 octets.
FirstName : Utilisé par Carnet d'adresses et d'autres applications utilisant la politique de recherche de contacts		
LastName : Utilisé par Carnet d'adresses et d'autres applications utilisant la politique de recherche de contacts		
Adresse de courrier électronique : Adresse électronique vers laquelle le courrier est automatiquement transféré lorsque l'attribut MailAttribute d'un utilisateur n'est pas défini ; utilisé par Carnet d'adresses, Mail et d'autres applications utilisant la politique de recherche de contacts.	Toute adresse électronique légale selon RFC 822	utilisateur@exemple.com
PhoneNumber : Utilisé par Carnet d'adresses et d'autres applications utilisant la politique de recherche de contacts		
AddressLine1 : Utilisé par Carnet d'adresses et d'autres applications utilisant la politique de recherche de contacts		
PostalAddress : Utilisé par Carnet d'adresses et d'autres applications utilisant la politique de recherche de contacts		

Attribut d'utilisateur Mac OS X	Format	Exemples
PostalCode : Utilisé par Carnet d'adresses et d'autres applications utilisant la politique de recherche de contacts		
OrganizationName : Utilisé par Carnet d'adresses et d'autres applications utilisant la politique de recherche de contacts		

Données d'utilisateur utilisées par Mac OS X Server

Le tableau suivant décrit la manière dont votre serveur Mac OS X Server utilise les données des enregistrements d'utilisateurs des domaines de répertoire. Consultez ce tableau pour savoir quels sont les attributs (ou types de données) que les divers services de votre serveur s'attendent à trouver dans les enregistrements d'utilisateurs des domaines de répertoire. Notez que, dans la colonne de gauche, "Tous les services" incluent AFP, SMB/CIFS, FTP, HTTP, NFS, WebDAV, POP, IMAP, Gestionnaire de groupe de travail, Admin Serveur, la fenêtre d'ouverture de session Mac OS X et Gestionnaire Macintosh.

Composant du serveur	Attribut d'utilisateur Mac OS X	Dépendance
Tous les services	RecordName	Requis pour l'authentification
Tous les services	Nom réel	Requis pour l'authentification
Tous les services	AuthenticationAuthority	Utilisé pour l'authentification Kerberos, Serveur de mots de passe et mot de passe shadow
Tous les services	Password	Utilisé pour l'authentification élémentaire (mot de passe crypté) ou Liaison LDAP
Tous les services	Identifiant unique	Nécessaire pour l'autorisation (par exemple, permissions de fichier et comptes de courrier)
Tous les services	PrimaryGroupID	Nécessaire pour l'autorisation (par exemple, permissions de fichier et comptes de courrier)
Service FTP Service Web Service de fichiers Apple Service NFS Gestionnaire Macintosh Fenêtre d'ouverture de session de Mac OS X Préférences de l'application et préférences système	Répertoire d'accueil Répertoire d'accueil NFS	Facultatif

Composant du serveur	Attribut d'utilisateur Mac OS X	Dépendance
Service de courrier	Attribut de courrier	Requis pour la connexion au service de courrier de votre serveur
Service de courrier	Adresse électronique	Facultatif

Attributs standard dans les enregistrements de groupes

Le tableau suivant décrit les attributs standard figurant dans les enregistrements de groupes Open Directory. Utilisez ces informations lorsque vous travaillez dans la sous-fenêtre Inspecteur de Gestionnaire de groupe de travail ou lorsque vous mappez des attributs d'enregistrements de groupes avec Format de répertoire.

Attribut de groupe Mac OS X	Format	Exemples
RecordName : Nom associé à un groupe	caractères ASCII A à Z, a à z, 0 à 9, _	Sciences Dépt_Sciences Prof.Sciences Longueur non nulle, maximum 255 octets (de 85 caractères triple octets à 255 caractères d'un octet).
Nom réel : Habituellement le nom complet du groupe	Texte UTF-8	Professeurs du département de sciences Longueur non nulle, maximum 255 octets (de 85 caractères triple octets à 255 caractères d'un octet).
Identifiant de groupe principal : Un identifiant unique pour le groupe	Chaîne ASCII signée à 32 bits, composée de chiffres de 0 à 9	Normalement unique par rapport aux autres entrées du groupe.
Membres du groupe : Liste de noms abrégés d'enregistrements d'utilisateurs considérés comme faisant partie du groupe	Caractères ASCII A à Z, a à z, 0 à 9, _,-	bsmith, jdoe Peut être une liste vide (normalement pour le groupe principal des utilisateurs).
Répertoire d'accueil Emplacement d'un répertoire de départ AFP du groupe	Texte UTF-8 structuré	<home_dir> <url>afp://*server/sharept*</url> <path>*grouphomedir*</path> </home_dir> Dans l'exemple ci-dessous, le répertoire d'accueil du groupe Sciences est K-M/Science, qui réside en dessous du répertoire de point de partage Groupes : <home_dir> <url>afp://exemple.com/Groupes</url> <path>K-M/Science</path> </home_dir>

Attribut de groupe Mac OS X	Format	Exemples
Member : Même données que pour GroupMembership mais chacune étant utilisée par différents services de Mac OS X Server	Caractères ASCII A à Z, a à z, 0 à 9, _,-	bsmith, jdoe Peut être une liste vide (normalement pour le groupe principal des utilisateurs).
HomeLocOwner : Nom abrégé de l'utilisateur qui possède le répertoire de départ du groupe	Caractères ASCII A à Z, a à z, 0 à 9, _,-	
MCXFlags : S'il est présent, MCXSettings est chargé ; s'il est absent, MCXSettings n'est pas chargé ; requis pour un utilisateur géré.	plist XML UTF-8, valeur unique	
Réglages MCX : Préférences d'un groupe de travail (groupe géré)	plist XML UTF-8, valeurs multiples	

Attributs standard dans les enregistrements d'ordinateurs

Le tableau suivant décrit les attributs standard figurant dans les enregistrements d'ordinateurs Open Directory. Les enregistrements d'ordinateurs associent l'adresse matérielle de l'interface Ethernet principale d'un ordinateur à un nom attribué à cet ordinateur. Le nom fait partie d'un enregistrement de liste d'ordinateurs (similaire à la notion d'utilisateur dans un groupe). Utilisez ces informations lorsque vous travaillez dans la sous-fenêtre Inspecteur de Gestionnaire de groupe de travail ou lorsque vous mappez des attributs d'enregistrements d'ordinateurs avec Format de répertoire.

Attribut d'ordinateur Mac OS X	Format	Exemples
RecordName : Nom associé à un ordinateur	Texte UTF-8	iMac 1
Commentaires : Toute documentation que vous choisissez	Texte UTF-8	
EnetAddress : L'adresse MAC de l'interface Ethernet de l'ordinateur	Notation hexa, séparation par deux-points ; les zéros initiaux peuvent être ignorés	00:05:02:b7:b5:88

Attribut d'ordinateur Mac OS X	Format	Exemples
MCXFlags : Utilisé uniquement dans l'enregistrement d'ordinateur "guest" (invité) ; s'il est présent, MCXSettings est chargé ; s'il est absent, MCXSettings n'est pas chargé ; requis pour un ordinateur géré.	plist XML UTF-8, valeur unique	
Réglages MCX : Utilisé uniquement dans l'enregistrement d'ordinateur "guest" (invité) ; préférences d'un ordinateur géré	plist XML UTF-8, valeurs multiples	

Attributs standard dans les enregistrements de listes d'ordinateurs

Le tableau suivant décrit les attributs standard figurant dans les enregistrements de listes d'ordinateurs Open Directory. Un enregistrement de liste d'ordinateurs identifie un groupe d'ordinateurs (très similaire à la façon dont un enregistrement de groupe identifie un ensemble d'utilisateurs). Utilisez ces informations lorsque vous travaillez dans la sous-fenêtre Inspecteur de Gestionnaire de groupe de travail ou lorsque vous mappez des attributs d'enregistrements de listes d'ordinateurs avec Format de répertoire.

Attribut de liste d'ordinateurs Mac OS X	Format	Exemples
RecordName : Nom associé à une liste d'ordinateurs	Texte UTF-8	Ordinateurs de laboratoire Longueur non nulle, maximum 255 octets (de 85 caractères triple octets à 255 caractères d'un octet).
MCXFlags	plist XML UTF-8, valeur unique	
Réglages MCX : Stocke les préférences d'un ordinateur géré	plist XML UTF-8, valeurs multiples	
Computers	Liste à valeurs multiples de noms d'enregistrements d'ordinateurs	iMac 1, iMac 2
Groupe Une liste de groupes dont les membres peuvent ouvrir une session sur les ordinateurs de cette liste d'ordinateurs	Liste à valeurs multiples de noms abrégés de groupes	herbivores,omnivores

Attributs standard dans les enregistrements de montages

Le tableau suivant décrit les attributs standard figurant dans les enregistrements de montages Open Directory. Utilisez ces informations lorsque vous travaillez dans la sous-fenêtre Inspecteur de Gestionnaire de groupe de travail ou lorsque vous mappez des attributs d'enregistrements de montages avec Format de répertoire.

Attributs de montages Mac OS X	Format	Exemples
RecordName : Hôte et chemin d'accès au point de partage	Texte UTF-8	*hostname:/chemin d'accès sur le serveur* indigo:/Volumes/home2
VFSLinkDir Chemin d'accès pour le montage sur un client	Texte UTF-8	/Network/Servers
VFSType	Texte ASCII	Pour AFP : url Pour NFS : nfs
VFSOpts	Texte UTF-8	Pour AFP (deux valeurs) : net url==afp://;AUTH=NO%20USER%20AUTHENT@*serveur/point de partage/* Pour NFS : net
VFSDumpFreq		
VFSPassNo		

Attributs standard dans les enregistrements de configurations

Le tableau suivant décrit les attributs standard figurant dans les deux types d'enregistrements de configurations Open Directory suivants.

- L'enregistrement mcx_cache porte toujours le nom RecordName de mcx_cache. Il utilise aussi RealName et DataStamp pour déterminer si la mémoire cache doit être actualisée ou les réglages de serveur ignorés. Si vous voulez des clients gérés, vous devez avoir un enregistrement de configuration mcx_cache.
- L'enregistrement passwordserver possède l'attribut supplémentaire PasswordServerLocation.

Utilisez ces informations lorsque vous travaillez dans la sous-fenêtre Inspecteur de Gestionnaire de groupe de travail ou lorsque vous mappez des attributs d'enregistrements de configurations avec Format de répertoire.

Attributs de configurations Mac OS X	Format	Exemples
RecordName : Nom associé à une configuration	Caractères ASCII A à Z, a à z, 0 à 9, _,-,.	mcx_cache passwordserver Longueur non nulle, maximum 255 octets (de 85 caractères triple octets à 255 caractères d'un octet).
PasswordServerLocation : Identifie l'hôte du serveur de mots de passe associé au domaine de répertoire	adresse IP ou nom d'hôte	192.168.1.90
Nom réel		Pour l'enregistrement de configuration mcx_cache, RealName est un GUID
DataStamp		Pour l'enregistrement de configuration mcx_cache, DataStamp est un GUID

Glossaire

Active Directory Le service de répertoire et d'authentification de Microsoft Windows 2000 Server et de Windows Server 2003.

administrateur Utilisateur disposant d'autorisations d'administration de serveur ou de domaine de répertoire. Les administrateurs sont toujours membres du groupe "admin" prédéfini.

adresse IP Adresse numérique unique qui identifie un ordinateur sur Internet.

AFP Apple Filing Protocol. Protocole client/serveur utilisé par le service de fichiers Apple sur les ordinateurs compatibles Macintosh pour partager des services de fichiers et de réseau. AFP utilise TCP/IP et d'autres protocoles pour les communications entre ordinateurs d'un réseau.

attribut Élément de données nommé contenant un type d'information spécifique et appartenant à une entrée (une fiche ou un objet) dans un domaine de répertoire. Les données qu'un attribut contient s'appellent la valeur de l'attribut.

attribut d'autorité d'authentification Valeur qui identifie le système de validation de mot de passe spécifié pour un utilisateur et fournit, si nécessaire, des informations supplémentaires.

authentification Processus de certification de l'identité d'un utilisateur, typiquement basé sur la validation d'un nom et d'un mot de passe utilisateur. L'authentification précède généralement le processus d'autorisation déterminant le niveau d'accès de l'utilisateur à une ressource. Par exemple, le service de fichiers autorise l'accès complet aux dossiers et fichiers dont l'utilisateur authentifié est le possesseur.

autorisation Processus par lequel un service détermine s'il doit permettre à un utilisateur l'accès à une ressource et quel degré d'accès il doit lui accorder. L'autorisation suit généralement le processus d'authentification prouvant l'identité de l'utilisateur. Par exemple, le service de fichiers autorise l'accès complet aux dossiers et fichiers dont l'utilisateur authentifié est le possesseur.

base de recherche Nom distinctif qui identifie l'endroit où il faut commencer la recherche d'informations dans la hiérarchie d'entrées d'un répertoire LDAP.

bidouilleur Personne qui aime la programmation et qui explore des façons de programmer de nouvelles fonctionnalités et d'étendre les possibilités d'un système informatique. Voir aussi **pirate**.

BSD Berkeley System Distribution. Version d'UNIX sur laquelle repose le logiciel Mac OS X.

chemin de recherche Voir **politique de recherche**.

CIFS Common Internet File System. Voir **SMB/CIFS**.

classe Voir **classe d'objets**.

classe d'objets Ensemble de règles qui définissent des objets semblables dans un domaine de répertoire en spécifiant les attributs que doit posséder chaque objet, ainsi que d'autres attributs possibles pour l'objet.

client géré Utilisateur, groupe ou ordinateur dont les autorisations d'accès et/ou les préférences sont sous le contrôle d'un administrateur.

compte d'ordinateur Voir **liste d'ordinateurs**.

DHCP Dynamic Host Configuration Protocol. Protocole utilisé pour la répartition dynamique d'adresses IP entre les ordinateurs clients. Chaque fois qu'un ordinateur client démarre, le protocole recherche un serveur DHCP et demande une adresse IP au serveur DHCP rencontré. Ce serveur cherche une adresse IP disponible et l'envoie à l'ordinateur client accompagnée d'un délai de bail—période pendant laquelle l'ordinateur client est autorisé à utiliser l'adresse.

DNS multidiffusion Protocole développé par Apple pour la détection automatique d'ordinateurs, de périphériques et de services sur les réseaux IP. Ce protocole standard Internet proposé est parfois aussi appelé "ZeroConf". Pour plus d'informations, visitez les sites www.apple.com ou www.zeroconf.org. Pour voir comment ce protocole est utilisé dans Mac OS X Server, voir **nom d'hôte local**.

domaine de répertoire Base de données spécialisée qui stocke des informations de référence sur les utilisateurs et les ressources réseau nécessaires au logiciel système et aux applications. La base de données est optimisée pour gérer de nombreuses requêtes d'informations et trouver et obtenir rapidement ces informations. Le domaine de répertoire peut également être appelé nœud de répertoire ou simplement répertoire.

domaine local domaine de répertoire accessible uniquement à partir de l'ordinateur sur lequel il réside.

dossier de groupes Répertoire servant à organiser les documents et les applications d'un intérêt particulier pour les membres d'un groupe et leur permettant d'échanger des informations.

enfant Ordinateur dont les informations de configuration proviennent du domaine de répertoire partagé d'un parent.

entrée Article, généralement court, posté dans un journal Web. Les lecteurs peuvent ajouter des commentaires à l'entrée, mais le contenu associé à celle-ci ne peut être modifié que par le propriétaire du journal Web. Dans un répertoire LDAP, une entrée est une collection d'attributs (d'éléments de données) qui porte un nom distinctif unique.

FTP File Transfer Protocol. Protocole permettant aux ordinateurs de transférer des fichiers sur un réseau. Les clients FTP dont le système d'exploitation gère le protocole FTP peuvent se connecter à un serveur de fichiers et télécharger des fichiers, en fonction des autorisations d'accès dont ils bénéficient. La plupart des navigateurs Internet et bon nombre d'applications gratuites peuvent être utilisés pour accéder à un serveur FTP.

groupe Ensemble d'utilisateurs ayant les mêmes besoins. Les groupes simplifient l'administration des ressources partagées.

groupe principal Groupe par défaut d'un utilisateur. Le système de fichiers utilise l'identifiant du groupe principal lorsqu'un utilisateur accède à un fichier dont il n'est pas le possesseur.

hachage Forme brouillée, ou cryptée, d'un mot de passe ou d'un texte.

hiérarchie de domaine de répertoire Mode d'organisation des domaines de répertoire partagés et locaux. Une hiérarchie possède une structure arborescente inversée, le domaine racine (root) étant placé en haut et les domaines locaux en bas.

identifiant de groupe principal Numéro unique identifiant un groupe principal.

IP Internet Protocol. Également désigné par IPv4. Méthode utilisée conjointement avec le protocole TCP (Transmission Control Protocol) pour envoyer des données d'un ordinateur à un autre via un réseau local ou via Internet. Le protocole IP envoie les paquets de données, alors que le protocole TCP se charge de leur suivi.

KDC Kerberos Key Distribution Center. Serveur sécurisé qui émet des tickets Kerberos.

Kerberos Système d'authentification réseau sécurisé. Kerberos utilise des tickets, délivrés pour un utilisateur, un service et une période déterminés. Une fois l'utilisateur authentifié, celui-ci peut accéder à des services supplémentaires sans devoir saisir à nouveau de mot de passe (signature unique) pourvu que ces services aient été configurés pour accepter les tickets Kerberos. Mac OS X Server utilise Kerberos v5.

LDAP Lightweight Directory Access Protocol. Protocole client/serveur standard pour accéder à un domaine de répertoire.

liaison (n.) Connexion entre un ordinateur et un domaine de répertoire dans le but d'obtenir des données d'identification, d'autorisation et d'autres données administratives. (v.) Le processus d'établissement d'une telle connexion. Voir aussi **liaison sécurisée**.

liaison sécurisée Connexion authentifiée mutuellement entre un ordinateur et un domaine de répertoire. L'ordinateur fournit des références pour prouver son identité et le domaine de répertoire fournit des références pour prouver son authenticité.

liste d'ordinateurs Liste d'ordinateurs partageant les mêmes réglages de préférences et accessibles par les mêmes utilisateurs et groupes.

Mac OS X La dernière version du système d'exploitation d'Apple. Mac OS X allie la fiabilité d'UNIX à la facilité d'emploi de Macintosh.

Mac OS X Server Plate-forme de serveur puissante, capable de gérer immédiatement les clients Mac, Windows, UNIX et Linux et offrant un ensemble de services de réseau et de groupes de travail extensible, ainsi que des outils perfectionnés de gestion à distance.

maître Open Directory Serveur qui fournit un service de répertoire LDAP, un service d'authentification Kerberos et le serveur de mots de passe Open Directory.

mot de passe Chaîne alphanumérique utilisée pour authentifier l'identité d'un utilisateur ou autoriser l'accès à des fichiers ou à des services.

mot de passe crypté Type de mot de passe qui est stocké sous la forme d'un hachage (à l'aide de l'algorithme de cryptage UNIX standard) directement dans un enregistrement d'utilisateur.

mot de passe Open Directory Mot de passe stocké dans une base de données sécurisée sur le serveur et qui peut être authentifié à l'aide du serveur de mots de passe Open Directory ou de Kerberos (si Kerberos est disponible).

mot de passe shadow Mot de passe stocké dans un fichier sécurisé sur le serveur et qui peut être authentifié à l'aide de diverses méthodes d'authentification conventionnelles requises par les différents services de Mac OS X Server. Parmi les méthodes d'authentification, il y a APOP, CRAM-MD5, DHX, LAN Manager, NTLMv1, NTLMv2 et WebDAV-Digest.

NetInfo L'un des protocoles Apple d'accès à un domaine de répertoire.

nœud de répertoire Voir **domaine de répertoire**.

nom abrégé Abréviation du nom d'un utilisateur. Le nom abrégé est utilisé par Mac OS X pour les répertoires de départ, l'authentification et les adresses électroniques.

nom complet Forme longue d'un nom d'utilisateur ou de groupe. Voir aussi **nom d'utilisateur**.

nom d'hôte local Nom qui désigne un ordinateur sur un sous-réseau local. Il peut être utilisé sans système DNS global afin de résoudre les noms en adresses IP. Il est constitué de lettres minuscules, de chiffres ou de traits d'union (sauf en tant que derniers caractères) et se termine par ".local" (par exemple, factures-ordinateur.local). Bien que le nom soit défini par défaut à partir du nom d'ordinateur, l'utilisateur peut définir ce nom dans la sous-fenêtre Réseau des Préférences Système. Il peut être modifié facilement et utilisé partout où un nom DNS ou un nom de domaine complet est utilisé. Il peut uniquement être résolu sur le même sous-réseau que l'ordinateur qui l'utilise.

nom d'utilisateur Nom complet d'un utilisateur, parfois qualifié de réel. Voir aussi **nom abrégé**.

nom distinctif Il identifie une entrée (un objet) dans un répertoire LDAP. Il est représenté sous la forme d'une séquence d'entrées de répertoire séparées par des virgules, commençant par l'entrée elle-même et suivie par chaque entrée qui contient l'entrée précédente dans la séquence. Exemple : "cn=utilisateurs, dc=exemple, dc=com."

Open Directory Architecture des services de répertoires Apple qui peut accéder à des informations de référence sur les utilisateurs et les ressources réseau à partir de domaines de répertoire utilisant les protocoles LDAP, NetInfo, ou Active Directory, les fichiers de configuration BSD et les services de réseau.

open-source Terme désignant le développement coopératif de logiciels par la communauté Internet. Le principe de base consiste à impliquer le maximum de personnes dans l'écriture et la mise au point du code en publiant le code source et en encourageant la formation d'une large communauté de développeurs qui feront part de leurs modifications et améliorations.

ordinateur administrateur Ordinateur Mac OS X sur lequel vous avez installé les applications d'administration de serveur à partir du CD de Mac OS X Server Admin.

parent Ordinateur dont le domaine de répertoire partagé fournit des informations de configuration à un autre ordinateur.

pirate Utilisateur malveillant qui tente d'accéder à un système informatique sans y être autorisé dans le but de saboter des ordinateurs et des réseaux ou de voler des informations. Comparer à bidouilleur.

point de partage Dossier, disque dur (ou partition de disque dur) ou CD accessible via le réseau. Un point de partage constitue le point d'accès situé au premier niveau d'un groupe d'éléments partagés. Les points de partage peuvent être partagés à l'aide des protocoles AFP, Windows SMB, NFS (exportation) ou FTP .

politique de recherche Liste des domaines de répertoire parmi lesquels un ordinateur Mac OS X effectue ses recherches lorsqu'il a besoin d'informations de configuration. Désigne également l'ordre dans lequel les domaines sont pris en compte lors de la recherche. Parfois appelé "chemin de recherche".

possesseur Le propriétaire d'un élément peut modifier les autorisations d'accès à l'élément. Le propriétaire peut également remplacer l'entrée par n'importe quel groupe dont le propriétaire est membre. Par défaut, le propriétaire dispose d'autorisations Lecture et écriture.

préférences gérées Préférences Système ou d'applications sous le contrôle d'un administrateur. Gestionnaire de groupe de travail permet aux administrateurs de contrôler les réglages de certaines préférences système pour les clients gérés Mac OS X.

principal, Kerberos Nom et autres informations d'identification d'un client ou service que Kerberos peut authentifier. Le principal d'un utilisateur est généralement constitué du nom de l'utilisateur ou bien du nom de l'utilisateur et du royaume Kerberos. Le principal d'un service est généralement constitué du nom du service, du nom DNS complet du serveur et du royaume Kerberos.

protocole Ensemble de règles qui déterminent la manière dont les données sont échangées entre deux applications.

répertoire de départ Dossier destiné à l'usage personnel d'un utilisateur. Entre autres, Mac OS X utilise également le répertoire de départ pour stocker des Préférences Système et des réglages d'utilisateur gérés pour les utilisateurs Mac OS X.

royaume Kerberos Domaine d'authentification comprenant les utilisateurs et les services enregistrés auprès du même serveur Kerberos. Les services et utilisateurs enregistrés font confiance au serveur Kerberos pour vérifier l'identité de chacun.

royaume WebDAV Région d'un site Web, généralement un dossier ou un répertoire, réservé aux utilisateurs et groupes WebDAV.

schéma Ensemble d'attributs et de types (ou classes) d'enregistrements qui fournissent un modèle pour les informations contenues dans un domaine de répertoire.

serveur autonome Serveur qui fournit des services sur un réseau, mais qui ne bénéficie pas de services de répertoire de la part d'un autre serveur, et ne fournit pas de services de répertoire à d'autres ordinateurs.

Serveur de mots de passe Voir **Serveur de mots de passe Open Directory**.

serveur de mots de passe Open Directory Service d'authentification qui valide des mots de passe à l'aide de diverses méthodes d'authentification conventionnelles requises par les différents services de Mac OS X Server. Parmi les méthodes d'authentification, il y a APOP, CRAM-MD5, DHX, LAN Manager, NTLMv1, NTLMv2 et WebDAV-Digest.

services de répertoire Services fournissant au logiciel système et aux applications un accès uniforme aux domaines de répertoire et autres sources d'informations sur les utilisateurs et les ressources.

signature unique Stratégie d'authentification qui évite aux utilisateurs de devoir saisir un nom et un mot de passe pour chaque service de réseau. Mac OS X Server utilise Kerberos pour permettre la signature unique.

SLP DA Service Location Protocol Directory Agent. Protocole utilisé pour répertorier les services disponibles sur un réseau, afin de permettre aux utilisateurs d'y accéder facilement. Lorsqu'un service est ajouté au réseau, il utilise le protocole SLP pour s'enregistrer sur le réseau. SLP/DA conserve les services réseau enregistrés dans un référentiel centralisé.

SMB/CIFS Server Message Block/Common Internet File System. Protocole permettant à des ordinateurs clients d'accéder à des fichiers et à des services de réseau. Il peut être utilisé via TCP/IP, Internet ou d'autres protocoles. Les services Windows utilisent le protocole SMB/CIFS pour fournir l'accès aux serveurs, imprimantes et autres ressources réseau.

SSL Secure Sockets Layer. Protocole permettant d'envoyer sur Internet des informations cryptées et authentifiées. Les versions plus récentes de SSL sont appelées TLS (Transport Level Security).

ticket d'octroi de tickets Ticket Kerberos spécial qui permet à un client d'obtenir des tickets pour des services au sein du même royaume. Un client reçoit un ticket d'octroi de tickets en prouvant son identité, par exemple en saisissant un nom et un mot de passe valide lors de la connexion.

ticket, Kerberos Référence temporaire qui prouve l'identité d'un client Kerberos à un service.

utilisateur invité Utilisateur pouvant se connecter à votre serveur sans fournir de nom ni de mot de passe.

WebDAV Web-based Distributed Authoring and Versioning. Environnement de création en direct permettant aux utilisateurs clients d'extraire des pages Web d'un site, de les modifier, puis de les replacer sur le site sans que ce dernier ne cesse de fonctionner.

Index

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

W