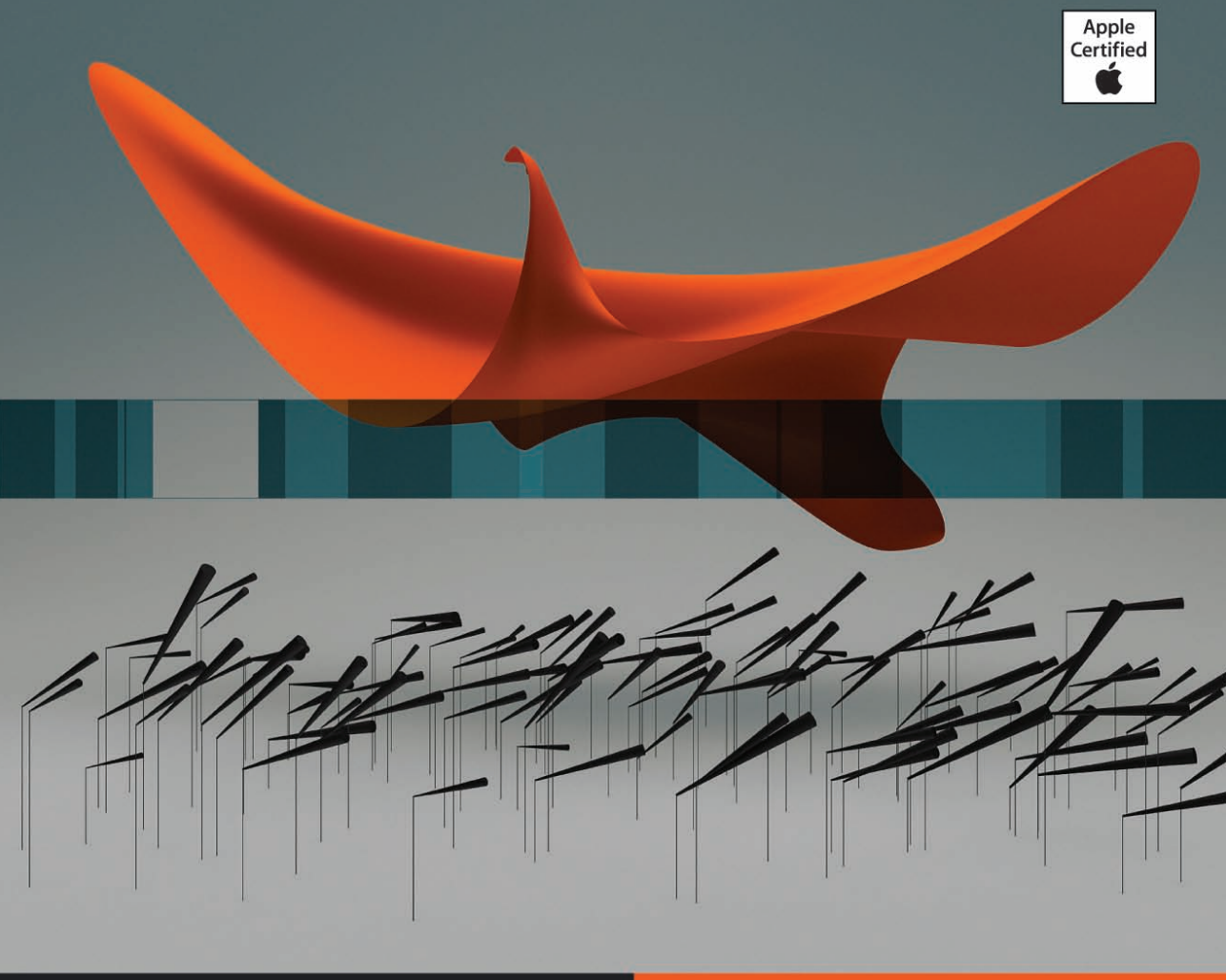


Apple Pro Training Series

OS X Lion Server Essentials

Das offizielle Handbuch zu OS X Lion Server für Administration, Help Desk und Support

Arek Dreyer mit Ben Greisler

ADDISON-WESLEY

Apple Pro Training Series

OS X Lion Server Essentials

Arek Dreyer mit Ben Greisler

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie;
detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de abrufbar.

Autorisierte Übersetzung der amerikanischen Originalausgabe: »Apple Pro Training Series: OS X Lion Server Essentials«.

Authorized translation from the English language edition, entitled »Apple Pro Training Series:
OS X Lion Server Essentials«, published by Peachpit Press, Berkeley, CA, Copyright © 2012.

10 9 8 7 6 5 4 3 2 1

14 13 12

ISBN 978-3-8273-3132-8

Lektorat: Boris Karnikowski, bkarnikowski@pearson.de
Fachlektorat: Oliver Jeckel, Allan Schmid, brainworks Training GmbH
Korrektorat: Friederike Daenecke, Zülpich
Übersetzung und Satz: G&U Language & Publishing Services GmbH (www.GundU.com)
Herstellung: Elisabeth Prümm, epruemm@pearson.de
Einbandgestaltung: Kent Oberheu
Druck und Verarbeitung: Drukarnia Dimograf, Bielsko-Biala

Printed in Poland

Apple Pro Training Series

OS X Lion Server Essentials

Das offizielle Handbuch zu OS X Lion Server für Administratoren, Help Desk und Support

Arek Dreyer mit Ben Greisler

Kapitel 3

Verwenden von Open Directory

In diesem Kapitel wird beschrieben, wie Sie mithilfe eines Verzeichnisdienstes Benutzer und Ressourcen in Ihrem Netzwerk verwalten können. Sie lernen die Funktionen der Open Directory-Dienste von Apple kennen und erfahren, wie diese Dienste mit anderen Verzeichnisdiensten in einer gemischten Umgebung integriert werden können. Sie erfahren auch, wie Sie Verzeichnisse und Benutzeraccounts mit der Server-App, dem Programm Server-Admin und dem Arbeitsgruppenmanager einrichten und verwalten können. Abschließend erfahren Sie Näheres über gelegentlich auftretende Probleme bei Open Directory-Diensten und lernen, wie Sie diese Probleme beheben.

Open Directory ist äußerst vielseitig, was die Integration mit verschiedenen anderen Verzeichnisdiensten wie Active Directory, eDirectory und NIS (*Network Information Service*) angeht. Szenarien hinsichtlich des gemischten Einsatzes mit Verzeichnisdiensten anderer Plattformen sind allerdings nicht Thema dieses Buchs.

Wenn Sie zwei zusätzliche Lion Server-Computer haben, können Sie in den Übungen einen davon als Open Directory-Replik und den anderen als den mit der Open Directory-Replik verbundenen Server verwenden. Haben Sie keine zusätzlichen Server, lesen Sie diese Übungen einfach durch.

Konzepte der Verzeichnisdienste

Erhält ein Benutzer mehrere Accounts auf verschiedenen Computern, kann das zu Problemen führen. Besitzt beispielsweise jeder Computer in einem Netzwerk eine eigene Datenbank für die Authentifizierung, muss sich der Benutzer unter Umständen für jeden Computer ein anderes Kennwort merken. Selbst wenn Sie dem Benutzer auf jedem Computer dasselbe Kennwort zuweisen, werden die Kennwörter im Laufe der Zeit möglicherweise inkonsistent, da der Benutzer das Kennwort auf einem Computer ändern, dies aber auf einem anderen Computer vergessen kann. Sie können dieses Problem lösen, indem Sie die Authentifizierungsdaten zentral auf einem einzelnen Computer speichern.

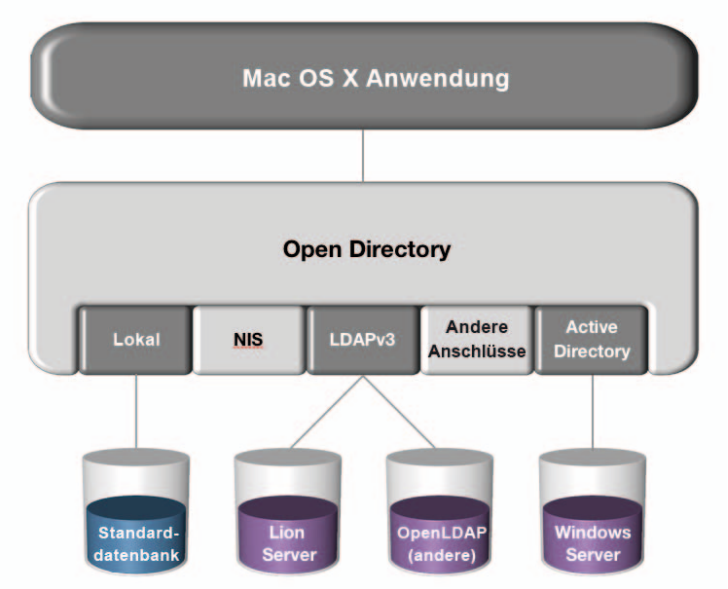
Verzeichnisdienste bieten einen solchen zentralen Speicherort für Informationen zu den Computern, Programmen und Benutzern einer Organisation. Mithilfe von Verzeichnisdiensten können Sie dafür sorgen, dass die Informationen zu allen Benutzern – etwa Namen, Kennwörter und Einstellungen – sowie zu Druckern und anderen Netzwerkressourcen konsistent bleiben. Sie können diese Informationen an einem einzelnen Speicherort anstatt auf einzelnen Computern verwalten. Dadurch können Sie Verzeichnisdienste für folgende Aufgaben nutzen:

- Bereitstellen einer einheitlichen Umgebung für Benutzer
- Erleichtern des Zugriffs auf Netzwerkressourcen wie Drucker und Server
- Ermöglichen der Anmeldung an mehreren Computern mit einem einzigen Account

Beispiel: Sobald Sie Lion-Computer an einen Open Directory-Dienst *binden* (d. h., einen Computer so konfigurieren, dass er die von einem anderen Computer bereitgestellten Verzeichnisdienste verwendet), können sich die Benutzer nach Belieben an jedem gebundenen Lion-Computer anmelden und ihre Sitzung unter Berücksichtigung ihrer Identität, Gruppenzugehörigkeit, des Computers, an dem sie angemeldet sind, und dessen Computergruppenzugehörigkeit verwalten lassen. Bei Verwendung eines gemeinsam genutzten Verzeichnisdienstes besteht außerdem die Möglichkeit, den Benutzerordner eines Benutzers auf einem anderen Server abzulegen und automatisch auf dem Computer zu aktivieren, an dem sich der Benutzer anmeldet. Voraussetzung ist lediglich, dass der Computer an das gemeinsam genutzte Verzeichnis gebunden ist.

Informationen zu Open Directory

Open Directory ist die erweiterbare Verzeichnisdienstarchitektur, die in OS X Lion und OS X Lion Server integriert ist. Open Directory funktioniert wie ein Mittler zwischen Verzeichnissen, die Informationen zu Benutzern und Ressourcen enthalten, und den Programmen und Systemsoftwareprozessen, die diese Informationen benötigen.



Der Open Directory-Dienst umfasst eine Reihe von Diensten auf Lion Server, die eine Identifizierung, Authentifizierung und Clientverwaltung bereitstellen.

Zahlreiche Dienste von OS X benötigen für eine korrekte Funktionsweise Informationen vom Open Directory-Dienst. Der Open Directory-Dienst kann die Kennwörter von Benutzern sicher speichern und überprüfen, die sich an Clientcomputern im Netzwerk anmelden oder weitere Netzwerkressourcen verwenden möchten, für die eine Authentifizierung erforderlich ist. Sie können den Open Directory-Dienst auch verwenden, um Richtlinien wie das Ablaufen und die Minimallänge von Kennwörtern umzusetzen und Benutzereinstellungen zu verwalten.

Mit dem Open Directory-Dienst können Sie für Windows-Benutzer Authentifizierungsmöglichkeiten für Datei- und Druckdienste sowie andere von Lion Server angebotene Dienste bereitstellen.

Überblick über die Komponenten des Open Directory-Dienstes

Open Directory ermöglicht eine zentrale Authentifizierung. Zur Identifizierung verwendet Open Directory *OpenLDAP*, eine Open-Source-Implementierung von LDAP (*Lightweight Directory Access Protocol*), bei dem es sich um ein Standardprotokoll für den Zugriff auf Verzeichnisdienstdaten handelt. Open Directory verwendet LDAPv3, um Lese- und Schreibzugriff auf die Verzeichnisdaten zu ermöglichen.

Dabei greift der Open Directory-Dienst auf weitere Open-Source-Technologien zurück, z. B. Kerberos, und kombiniert diese mit leistungsstarken Serververwaltungsprogrammen. So werden zuverlässige Verzeichnis- und Authentifizierungsdienste bereitgestellt, die sich einfach konfigurieren und verwalten lassen. Da keine auf der Anzahl der Arbeitsplätze oder Benutzer basierenden Lizenzgebühren anfallen, kann Open Directory an die Anforderungen einer Organisation angepasst werden, ohne hohe Kosten zu verursachen.

Nachdem ein OS X-Computer an einen bestimmten Open Directory-Server gebunden wurde, erhält der mit OS X oder Lion Server betriebene Computer automatisch Zugriff auf Netzwerkressourcen, einschließlich Diensten zur Benutzerauthentifizierung, Netzwerkbenutzerordnern, Netzwerkfreigaben und Einstellungen.

Grundlagen von Open Directory-Mastern

Ein Lion Server-Computer, der zur Verwaltung von Netzwerkaccounts eingerichtet ist und Verzeichnisdienste bereitstellt, wird als *Open Directory-Master* bezeichnet. In der Server-App wird dieser Begriff nicht angezeigt, aber in Server-Admin.

Neben der Rolle des Open Directory-Masters gibt es auch die Rolle der *Open Directory-Replik*. Beide Rollen stellen Verzeichnisdienste bereit, wobei jedoch die Replik eine replizierte Version der Verzeichnisinformationen anbietet, die regelmäßig mit den Daten des Open Directory-Masters synchronisiert wird. Um eine verwechslungsfreie Terminologie durchzusetzen, bezeichnen wir einen Lion Server-Computer, der als Open Directory-Server fungiert, entweder als Master oder als Replik (obwohl jede Replik technisch gesehen auch ein Master ist).

Berücksichtigen Sie bei der Planung der Verzeichnisdienste für Ihr Netzwerk, in welchem Umfang Sie Benutzer- und Ressourceninformationen für mehrere Lion-Computer freigeben müssen. Ist dieser Umfang gering, ist nur wenig Verzeichnisplanung erforderlich. Auf alle Informationen kann über ein lokales Serververzeichnis zugegriffen werden. Wenn Sie jedoch Daten auf mehreren Computern gemeinsam nutzen möchten, müssen Sie mindestens einen Open Directory-Server (einen Open Directory-Master) konfigurie-

ren. Wenn Sie eine hohe Verfügbarkeit von Verzeichnisdiensten gewährleisten möchten, sollten Sie mindestens einen zusätzlichen Lion Server-Computer als Open Directory-Replik konfigurieren.

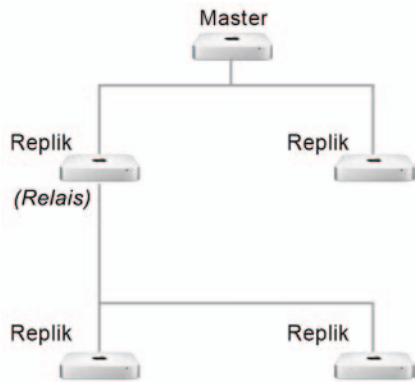
Grundlagen von Open Directory-Repliken

Wenn Sie bereits einen Open Directory-Masterserver konfiguriert haben, können Sie mindestens einen weiteren Lion Server-Computer als Verzeichnisreplik einrichten, die die gleichen Verzeichnis- und Authentifizierungsdaten bereitstellt wie der Master. Der Replikserver enthält eine Kopie des LDAP-Verzeichnisses, der Kennwortserver-Datenbank und des Kerberos-KDC des Masters. Wenn Authentifizierungsdaten vom Master auf eine Replik übertragen werden, werden diese Daten verschlüsselt.

Sie können Repliken verwenden, um Ihre Verzeichnisinfrastruktur zu skalieren und die Such- und Abrufzeit in verteilten Netzwerken zu verbessern sowie um eine hohe Verfügbarkeit von Open Directory-Diensten bereitzustellen. Die Replikation schützt außerdem vor Netzwerkausfällen, da Clientsysteme beliebige Repliken in Ihrem Unternehmen verwenden können.

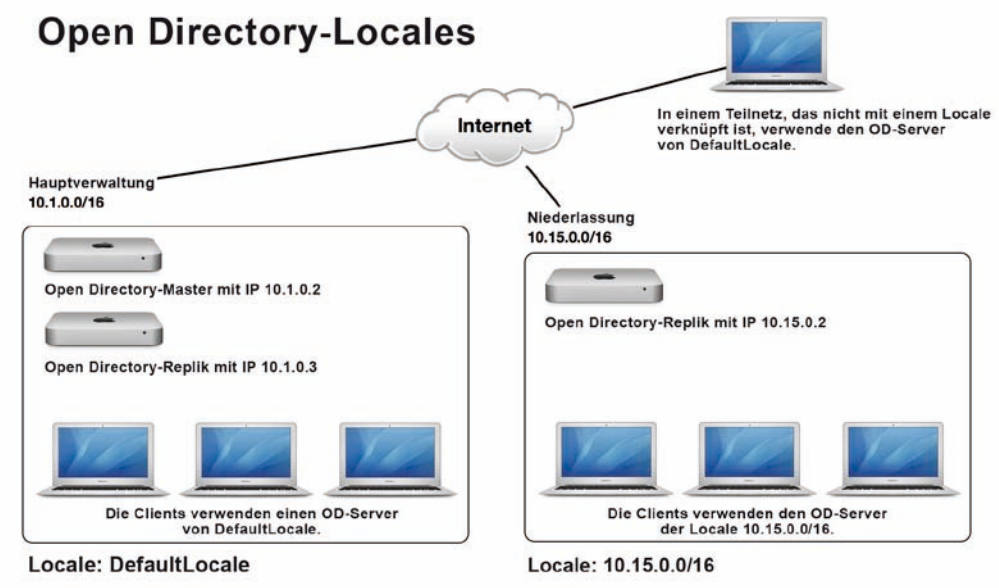
Sie können auch verschachtelte Repliken einrichten, also Repliken von Repliken. Von einem Master können bis zu 32 Repliken erstellt werden, von denen jeweils 32 Repliken erstellt werden können. Ein Master plus 32 Repliken plus 32 × 32 Repliken der Repliken ergibt 1057 Open Directory-Server für eine einzelne Open Directory-Domäne. Das Verschachteln von Repliken wird ermöglicht, indem Sie eine Replik zu Ihrem Open Directory-Master und dann weitere Repliken zur ersten Replik hinzufügen.

Die folgende Abbildung zeigt einen Open Directory-Master und eine Replik, die auch ein *Relais* darstellt, d. h. eine Replik, von der es wiederum mindestens eine Replik gibt. Die Abbildung zeigt drei Repliken ohne zugehörige weitere Repliken.



Grundlagen von Open Directory-Locales

Open Directory-Locales sind ein neues Merkmal von Lion Server, mit dem es für Sie einfacher wird, die Last auf geeignete Open Directory-Server zu verteilen. Ein Open Directory-Locale ist eine Gruppe von Open Directory-Servern, die für ein bestimmtes Teilnetz da sind. Mit Server-Admin können Sie ein Locale definieren und dann ein oder mehrere Open Directory-Server und ein oder mehr Teilnetze damit verknüpfen. Wenn ein Clientcomputer an einen Ihrer Open Directory-Server gebunden ist und sich in einem mit diesem Locale verknüpften Teilnetz befindet, bevorzugt er die Open Directory-Server im zugehörigen Locale. Dies ist eine Verbesserung gegenüber den früheren Versionen von OS X und OS X Server, bei denen ein manueller Eingriff, standortspezifische DNS-Einträge oder Änderungen am Ablauf der Bereitstellung erforderlich waren, um Clientcomputer in einer Organisation mit mehreren Standorten oder Netzwerken dazu zu bringen, einen geeigneten Open Directory-Server zu nutzen.



Die Konfiguration von Open Directory-Locales würde den Rahmen dieses Buches sprengen. Informationen darüber finden Sie unter *help.apple.com/advancedserveradmin*.

Verwenden eines anderen Open Directory-Servers

Wenn Sie beabsichtigen, mehrere Server einzurichten, wäre es äußerst unpraktisch, auf allen Servern dieselben Benutzeraccounts anzulegen. Stattdessen können Sie Ihren Lion Server-Computer an ein anderes Verzeichnissystem binden. In dieser Funktion ruft der

Server Authentifizierungs-, Benutzer- und weitere Verzeichnisinformationen vom Verzeichnisdienst eines anderen Servers ab. Auf diese Weise können sich Benutzer bei Ihrem Lion Server-Computer mit einem Account authentifizieren, der in dem lokalen Verzeichnis des Server-Computers definiert ist, oder mit einem Account von einem beliebigen Verzeichnis-Knoten, an den Ihr Server gebunden ist. Bei dem anderen Verzeichnis-Knoten kann es sich um ein Open Directory- oder ein Active Directory-System handeln.

Es gibt eine Reihe von Möglichkeiten, um Ihren Lion Server-Computer an den anderen Verzeichnisdienst zu binden. Unter anderem können Sie die Server-App verwenden. In diesem Fall kann es sein, dass Sie erst die Schritte durchlaufen müssen, um den Computer zu einem Open Directory-Master zu machen. Das ist vor allem für Benutzergruppen in größeren Organisationen nützlich. Wenn Sie der Administrator einer solchen Gruppe sind, können Sie mit Lion Server zusätzliche Dienste bereitstellen oder weitere Gruppen von Personen anlegen, ohne diejenigen um Hilfe bitten zu müssen, die Ressourcen für den Rest der Organisation verwalten. Sie können unabhängig von dem Verzeichnisdienst vorgehen, der von der Organisation als Ganzes verwendet wird.

Für manche Dienste, z. B. den Profil-Manager, ist es erforderlich, den Server zur Verwaltung von Netzwerkaccounts einzurichten, ihn also zu einem Open Directory-Master zu machen. Das ist in Ordnung, denn ihr Server kann sowohl als Open Directory-Master fungieren als auch an einen anderen Open Directory-Dienst gebunden sein.

Sie können Ihren Lion Server-Computer so einrichten, dass er die Verzeichnisdienste eines anderen Servers nutzt. Beachten Sie, dass die Konfiguration Einfluss darauf hat, ob alle Benutzer eines Verzeichnisdienstes Zugriff auf die Dienste Ihres Lion Server-Computers haben oder ob nur die Benutzer, die Sie »importieren«, dazu autorisiert sind (siehe den Abschnitt »Importieren von Benutzern mit der Server-App«).

Vorbereitungen auf die Einrichtung von Open Directory-Diensten

Es gibt verschiedene Methoden, um einen Lion Server-Computer zur Bereitstellung von Verzeichnisdiensten, zur Verwendung eines anderen Verzeichnisdienstes oder für beides einzurichten. Im Folgenden werden Sie lernen, welches Programm sich für Ihre Bedürfnisse eignet.

Um sämtliche Open Directory-Dienste bereitstellen zu können, muss Ihr Lion Server-Computer über DNS-Einträge zur Vorwärts- und Rückwärtsauflösung verfügen, bevor Sie ihn als Open Directory-Master erstellen können.

In den nächsten beiden Abschnitten erfahren Sie, welche Werkzeuge sich für diese Aufgaben eignen und wie Sie die DNS-Einträge untersuchen.

Auswählen eines Programms zur Einrichtung von Verzeichnisdiensten

Es gibt mehrere Methoden, um Lion Server für die Bereitstellung von Open Directory-Diensten zu konfigurieren. Wie wählen Sie die zu verwendende Methode aus? Dies hängt von Ihren Anforderungen ab. Sie sollten die Auswirkungen kennen, die die Verwendung der einzelnen Programme hat.

Auswählen eines Programms für die Einrichtung eines Open Directory-Masters

Um den Lion Server-Computer als Verzeichnisserver oder Open Directory-Master einzurichten, können Sie die folgenden Programme verwenden:

- Server-App
- Server-Admin

Beide Programme führen eine Reihe von Aufgaben durch, darunter:

- Einrichtung von OpenLDAP, Kerberos (falls der Server noch nicht zu einem Kerberos-Realm gehört) und Kennwortserver-Datenbanken
- Hinzufügen des neuen Verzeichnisdienstes zum Authentifizierungssuchpfad
- Erstellen der Netzwerkgruppe *Workgroup*
- Hinzufügen der lokalen Gruppe *Local Accounts* zur Netzwerkgruppe *Workgroup*
- Erstellen eines SSL-Zertifikats und Signierung durch eine neue Intermediate-Zertifizierungsinstanz, die wiederum von einer neuen Root-Zertifizierungsinstanz signiert ist
- Hinzufügen der Root- und der Intermediate-Zertifizierungsinstanz zum Systemschlüsselbund des Lion Server-Computers
- Hinzufügen eines Zugriffssteuerungseintrags (*Access Control Entry*, ACE) zur Freigabe *Public*, um der Netzwerkgruppe *Workgroup* den Lese- und Schreibzugriff zu gestatten

Die Server-App führt darüber hinaus die folgenden Aufgaben durch, die Server-Admin nicht erledigt:

- Einrichten des Lion Server-Computers, sodass er der Root- und der Intermediate-Zertifizierungsinstanz vertraut

- Erstellen von Zugriffssteuerungslisten für Dienste (*Service Access Control Lists, SACLs)*
- Hinzufügen aller vorhandenen lokalen Benutzer zu diesen SACLs, sodass sie autorisiert sind, auf alle betreffenden Dienste zuzugreifen, sofern diese ausgeführt werden

Die Dienste, für die die SACLs aufgestellt werden, können Sie in der Server-App einsehen, indem Sie einen Benutzer markieren und Zugriff auf Dienste bearbeiten wählen:

- Adressbuch
- Dateifreigabe (hierfür werden zwei SACLs aufgestellt: eine für AFP und eine für SMB)
- iCal-Server
- iChat-Server
- Mailserver
- Podcast
- Profil-Manager
- Time Machine
- VPN

Die Server-App richtet automatisch einen Kerberos-Realm ein, dessen Name auf den Hostnamen des Lion Server-Computers zurückgeht. Wenn Sie dagegen Server-Admin einsetzen, um Ihren Lion Server-Computer zum Open Directory-Master zu machen, können Sie einen anderen Namen für den Kerberos-Realm angeben, beispielsweise einen, der den Organisationsnamen widerspiegelt und nicht den Servernamen. Außerdem können Sie in Server-Admin leichter Protokolle einsehen und die SACLs untersuchen.

Auswahlmöglichkeiten für Verzeichnisdienste in Server-Admin

Wenn Sie mehr Optionen brauchen, als die Server-App bietet, können Sie den Lion Server-Computer mithilfe von Server-Admin zur Bereitstellung von Open Directory-Diensten einrichten. Mit Server-Admin können Sie die Open Directory-Dienste des Lion Server-Computers auf verschiedene Weise konfigurieren:

- *Als eigenständiger Server:* Entfernen Sie die vorhandene Verzeichniskonfiguration, sodass der Server keine Verzeichnisinformationen für andere Computer bereitstellt oder von vorhandenen Systemen abruft. Das lokale Verzeichnis kann nicht freigegeben werden.

- *Als mit einem Verzeichnissystem verbundener Server:* Sie können den Server so konfigurieren, dass er Dienste bereitstellt, für die Benutzeraccounts und eine Authentifizierung erforderlich sind, etwa Datei- und Mail-Dienste, jedoch Accounts verwendet, die auf einem anderen Server eingerichtet sind.
- *Als Open Directory-Replik:* Ein Server stellt eine replizierte Version eines Verzeichnisses bereit. Die Replik wird regelmäßig mit dem Master synchronisiert.
- *Als Open Directory-Master:* Ein Server kann anderen Systemen Verzeichnisinformationen und Authentifizierungsinformationen zur Verfügung stellen.

Wenn Ihr Lion Server-Computer noch nicht für irgendeine Verzeichnisdienstrolle eingerichtet ist, sehen Sie folgende Auswahlmöglichkeiten:

- Einen Open Directory-Master einrichten
- Mit einem anderen Verzeichnis verbinden
- Eine Open Directory-Replik einrichten

Ist der Lion Server-Computer bereits als Open Directory-Master eingerichtet, haben Sie folgende Optionen:

- Ein eigenständiges Verzeichnis einrichten
- Mit einem anderen Verzeichnis verbinden
- Eine Open Directory-Replik einrichten

Ist der Lion Server-Computer bereits als Open Directory-Replik eingerichtet, haben Sie folgende Optionen:

- Replik in Open Directory-Master umwandeln
- Replik ausser Dienst stellen und mit einem anderen Verzeichnis verbinden
- Replik ausser Dienst stellen und ein eigenständiges Verzeichnis einrichten

Ist der Lion Server-Computer zur Verwendung eines anderen Verzeichnisdienstes eingerichtet, sehen Sie folgende Optionen:

- Verbunden bleiben und einen Open Directory-Master einrichten
- Verbunden bleiben und eine Open Directory-Replik einrichten
- Trennen und ein eigenständiges Verzeichnis einrichten

Wie diese Liste zeigt, bietet Server-Admin je nach der aktuellen Verzeichnisdienstkonfiguration eine flexible und dynamische Auswahl von Konfigurationsmöglichkeiten an.

Auswählen eines Programms für die Einrichtung einer Open Directory-Replik

Mit der Server-App ist es nicht möglich, Ihren Server als Replik eines anderen Open Directory-Masters einzurichten. Verwenden Sie dazu Server-Admin (oder die Werkzeuge in der Befehlszeile, was aber in diesem Buch nicht beschrieben wird).

Auswählen eines Programms zum Aufbau einer Verbindung zu einem anderen Verzeichnisdienst

Wenn Ihr Lion Server-Computer einfach nur einen zentralen Verzeichnisdienst nutzen und selbst keine Verzeichnisdienste anbieten soll, können Sie ihn an einen anderen Verzeichnisdienst binden, damit die Benutzer auf diesem zentralen Verzeichnisdienst untergebrachte Accountdaten nutzen können, um auf die Dienste des Lion Server-Computers zuzugreifen.

Die empfohlene Vorgehensweise zur Bindung eines Lion Server-Computers an einen anderen Verzeichnisdienst besteht darin, als Erstes die eigentliche Bindung in der Systemeinstellung Benutzer & Gruppen vorzunehmen und dann mithilfe von Server-Admin die Dienste darauf vorzubereiten, den Kerberos-Realm des anderen Verzeichnisdienstes zu verwenden.

Zur Bindung an einen anderen Verzeichnisdienst können Sie auch das Dienstprogramm *Verzeichnisdienste* verwenden. Handelt es sich bei dem anderen Dienst um einen Open Directory-Dienst, benötigen Sie die erweiterten Einstellungen des Programms *Verzeichnisdienste* nicht.

Zur Bindung an einen anderen Verzeichnisdienst können Sie in der Server-App Verwalten > Mit Verzeichnis verbinden wählen. Ist der Lion Server-Computer aber noch kein Open Directory-Master, öffnet die Server-App automatisch den Assistenten Netzwerkbenutzer und -gruppen konfigurieren. Wenn Sie diesen Assistenten abbrechen, können Sie nicht mit der Bindung an einen anderen Verzeichnisdienst fortfahren. Um die Bindung an einen anderen Verzeichnisdienst mit der Server-App vornehmen zu können, müssen Sie den Server erst als Open Directory-Master einrichten, wodurch die SACLs für eine Reihe von Diensten erstellt werden. Damit Benutzer aus anderen Verzeichnisdiensten die Dienste auf dem frisch gebundenen Lion Server-Computer nutzen können, müssen Sie diese Benutzer mit der Server-App »importieren«, wodurch sie zu den SACLs hinzufügt werden. Anderenfalls können diese Benutzer nur den Wiki-Dienst des Lion Server-Computers in Anspruch nehmen.

HINWEIS ► Dieses Problem tritt nicht auf, wenn Sie zur Einrichtung des Servers als Open Directory-Master Server-Admin verwenden, denn dadurch werden keine SACLs eingerichtet. Anschließend können Sie in der Server-App Verwalten > Mit Verzeichnis verbinden wählen.

Untersuchen der DNS-Einträge für Lion Server

Mit der Server-App können Sie Änderungen am Hostnamen und an der IP-Adresse Ihres Servers vornehmen und überprüfen, ob diese Angaben mit den verfügbaren DNS-Einträgen übereinstimmen.

Bevor Sie einen Server als Open Directory-Master oder -Replik definieren, sollten Sie sich mithilfe des Netzwerkdienstprogramms vergewissern, dass für seinen Hostnamen und seine primäre IP-Adresse geeignete DNS-Einträge verfügbar sind.

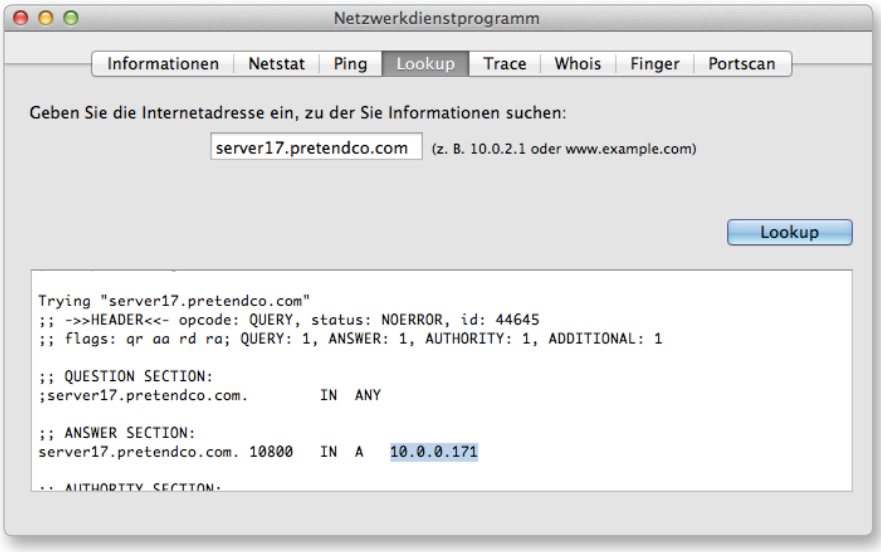
Wenn Sie Lion Server in einer Umgebung installiert oder konfiguriert haben, in der ein DNS-Eintrag für die dabei zugewiesene IP-Adresse verfügbar ist, wird der DNS-Dienst vom Serverassistenten nicht konfiguriert oder gestartet. Haben Sie Lion Server jedoch in einer Umgebung ohne einen solchen DNS-Eintrag installiert oder konfiguriert, erstellt die Server-App die erforderlichen DNS-Zonen und -Einträge für den Hostnamen und die IP-Adresse des Servers und startet dann den DNS-Dienst.

Für die Übungen in diesem Buch wird vorausgesetzt, dass Ihr Lion-Administratorcomputer Zugriff auf die DNS-Einträge Ihrer Lion Server-Computer hat. In den Übungsschritten werden Sie angewiesen, die vollständig qualifizierten Domänen-Namen (FQDNs) Ihrer Server (wie *server17.pretendco.com*) zu verwenden. Sie können die Bonjour-Namen Ihrer Server (zum Beispiel *server-17.local*) verwenden, es ist jedoch ratsam, in Verbindung mit den Serverwerkzeugen immer den Hostnamen zu nutzen. Wenn Probleme mit der Verfügbarkeit von DNS-Einträgen auftreten, stellen Sie diese bei Verwendung der Werkzeuge eher fest und haben dann Gelegenheit, die DNS-Probleme zu beheben, bevor Sie fortfahren.

WEITERE INFORMATIONEN ► Weitere Informationen zur Verwendung des Netzwerkdienstprogramms für die Untersuchung von DNS-Einträgen erhalten Sie in Kapitel 6, »Netzwerkkonfiguration«, des Buchs *Apple Pro Training Series: OS X Lion Support Essentials* im Abschnitt »Beheben von Fehlern der Netzwerkkonfiguration«.

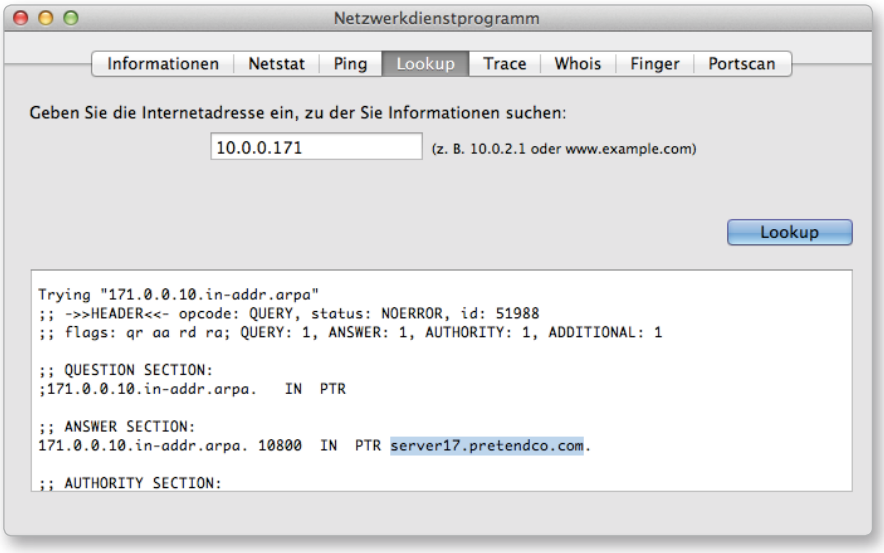
Überprüfen Sie mit dem Netzwerkdienstprogramm, ob Ihr Server über die geeigneten DNS-Einträge für den Lion Server-Computer verfügt:

1. Öffnen Sie auf dem Administratorcomputer die Server-App.
2. Wählen Sie im Menü Werkzeuge die Bildschirmfreigabe.
3. Geben Sie den Hostnamen des Servers ein (**server17.pretendco.com**).
4. Authentifizieren Sie sich als *ladmin*, um den Bildschirm Ihres Servers freizugeben (Kennwort *ladminpw*).
5. Melden Sie sich im Anmeldedialog des Servers als *ladmin* an (Kennwort *ladminpw*), falls Sie das noch nicht getan haben.
6. Öffnen Sie Launchpad, den Ordner *Dienstprogramme* und dann das Netzwerkdienstprogramm.
7. Klicken Sie auf den Titel Lookup.
8. Geben Sie den Hostnamen des Servers in das Textfeld ein (**server17.pretendco.com**).
9. Klicken Sie auf Lookup.
10. Vergewissern Sie sich, dass unter ANSWER SECTION die IP-Adresse des Servers aufgeführt wird.



11. Geben Sie in das Textfeld die IP-Adresse des Servers ein, und klicken Sie auf Lookup.

12. Vergewissern Sie sich, dass unter ANSWER SECTION der Hostname des Servers aufgeführt wird.



13. Beenden Sie das Netzwerkdienstprogramm.

14. Melden Sie sich auf dem Lion Server-Computer ab.

15. Beenden Sie die Bildschirmfreigabe auf dem Administratorcomputer.

Führen Sie dieses einfache Verfahren zur Bestätigung der Forward- und Reverse-DNS-Einträge mithilfe des Netzwerkdienstprogramms immer dann durch, wenn Sie einen Lion Server-Computer als Open Directory-Master, -Replik oder einfach als Mitgliedsserver einrichten.

Konfigurieren von Open Directory-Diensten

Nachdem Sie jetzt die verfügbaren Werkzeuge kennen und die DNS-Einträge bestätigt haben, können Sie den Lion Server-Computer so einrichten, dass er Verzeichnisdienste bereitstellt und nutzt.

Einrichten eines Lion Server-Computers als Open Directory-Master

Wenn der Lion Server-Computer noch nicht als Open Directory-Master eingerichtet oder mit einem anderen Verzeichnisdienst verbunden ist, können Sie die Verzeichnisdienste mit den beiden folgenden Optionen im Menü Verwalten der Server-App konfigurieren:

- Netzwerkaccounts verwalten
- Mit Verzeichnis verbinden

Als Lion Server-Administrator werden Sie am häufigsten diese beiden Optionen in der Server-App verwenden. In Server-Admin stehen noch weitere Optionen zur Verfügung. Wenn Sie Netzwerkaccounts verwalten wählen, führt die Server-App Sie durch die erforderlichen Schritte, um den Server zu einem Open Directory-Master zu machen. Bei Mit Verzeichnis verbinden arbeiten Sie in der Server-App den Vorgang durch, mit dem Sie den Server zur Verwendung eines anderen Verzeichnisdienstes einrichten. Allerdings fordert die Server-App Sie in diesem Fall zunächst auf, den Server zu einem Open Directory-Master zu machen.

Die Option »Netzwerkaccounts verwenden« der Server-App

Die Server-App ist das empfohlene Werkzeug, um einen Lion Server-Computer zur Verwaltung von Netzwerkaccounts einzurichten, ihn also mit anderen Worten zu einem Open Directory-Master zu machen.

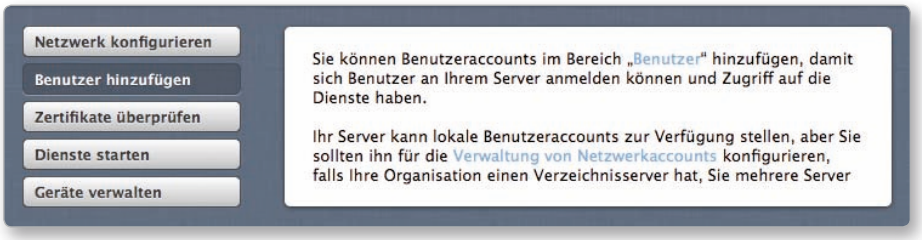
Diese Übung ist nur für Server sinnvoll, die noch keine Open Directory-Master oder -Repliken sind und nicht an deren Verzeichnisdienst gebunden sind. Verwenden Sie den Abschnitt Weitere Schritte, um den Lion Server-Computer als Open Directory-Master einzurichten.

> **HINWEIS ►** Der Standardaccountname für den Verzeichnisadministrator lautet *diradmin*. Bei der Bindung zweier Lion-Verzeichnisserver müssen die Verzeichnisadmistratoraccounts der beiden Computer jedoch jeweils einen eindeutigen Namen haben. Weitere Informationen finden Sie unter *help.apple.com/advancedserveradmin*.

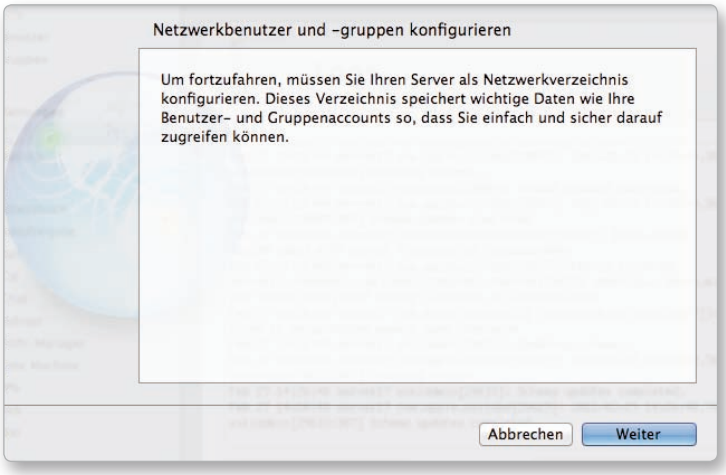
1. Öffnen Sie auf dem Administratorcomputer die Server-App, und stellen Sie als lokaler Administrator eine Verbindung zu Ihrem Server her (Administratorname *ladmin*, Kennwort *ladminpw*).

2. Klicken Sie falls erforderlich auf Weitere Schritte, um den entsprechenden Abschnitt einzublenden, und dann auf Benutzer hinzufügen.

3. Klicken Sie im Text auf der rechten Seite des Abschnitts Weitere Schritte auf »Verwaltung von Netzwerkaccounts« (oder wählen Sie Verwalten > Netzwerkaccounts verwalten).



4. Klicken Sie im Fenster Netzwerkbenutzer und -gruppen konfigurieren auf Weiter.



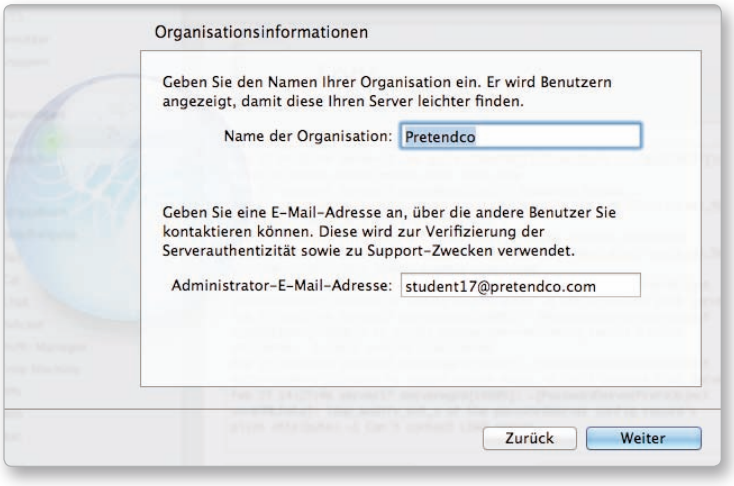
5. Geben Sie im Fenster Verzeichnisadministrator ein Kennwort für den Account *diradmin* ein.

   Verwenden Sie in diesem Beispiel das Kennwort *diradminpw*. In einer Produktionsumgebung sollten Sie selbstverständlich ein sicheres Kennwort verwenden. Außerdem können Sie für diesen Account einen anderen Namen als die Standardnamen *Directory Administrator* und *diradmin* festlegen.

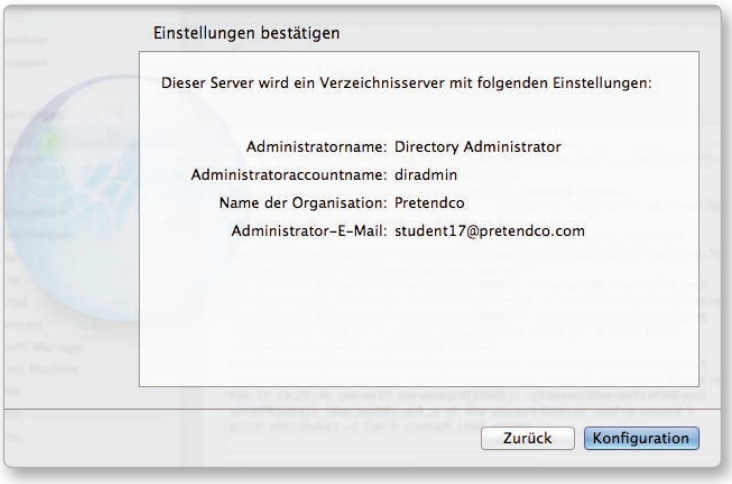
6. Klicken Sie auf Weiter.

7. Die Angaben im Fenster Organisationsinformationen sollten automatisch mit denen von der Erstkonfiguration von Lion Server ausgefüllt sein.

   Wenn Sie Lion Server auf Lion installiert haben, sind die Felder möglicherweise leer. Sie können die Informationen hier ändern. Lassen Sie sie für diese Übung jedoch unverändert, und klicken Sie auf Weiter.



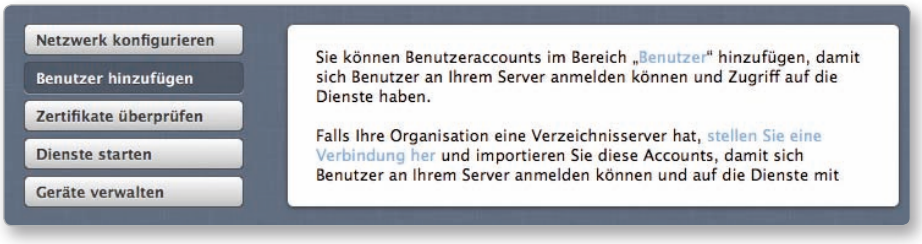
8. Klicken Sie im Fenster Einstellungen bestätigen auf Konfiguration.



9. Warten Sie einige Augenblicke, bis die Server-App den Lion Server-Computer als Netzwerkverzeichnisserver oder Open Directory-Master eingerichtet hat.

   Wenn die Server-App den Vorgang abgeschlossen hat, werden Sie wieder zu ihr zurückgeführt.

   Wie Sie sehen, ist der Text im Abschnitt Weitere Schritte der Server-App aktualisiert worden.

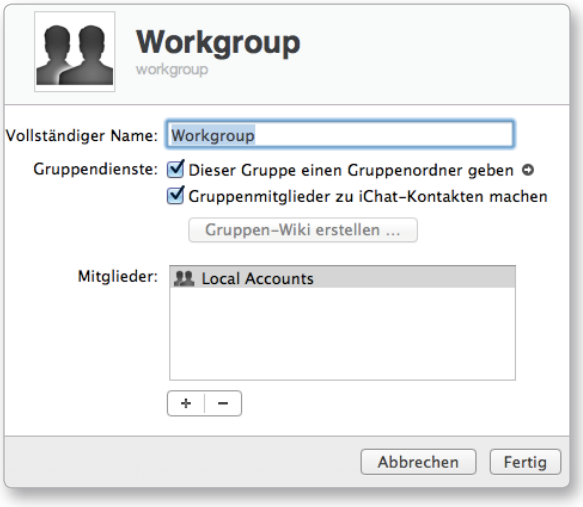


Untersuchen der Auswirkungen der Einrichtung als Open Directory-Master

1. Klicken Sie in der Seitenleiste der Server-App auf dem Administratorcomputer auf Gruppen.

Beachten Sie, dass neben den bereits vorhandenen lokalen Gruppen jetzt auch die neue Netzwerkgruppe *Workgroup* angezeigt wird, deren Symbol eine blaue Erdkugel enthält.

2. Doppelklicken Sie auf die Netzwerkgruppe *Workgroup*.



Das einzige Mitglied dieser Gruppe ist zurzeit die lokale Gruppe *Local Accounts*. Wenn Sie Darstellung > Systemaccounts anzeigen wählen, zeigt die Server-App in der Liste der Gruppenmitglieder ebenso nur die Gruppe *Local Accounts* an. Alle lokalen Accounts sind automatisch Mitglieder der lokalen Gruppe *Local Accounts*.

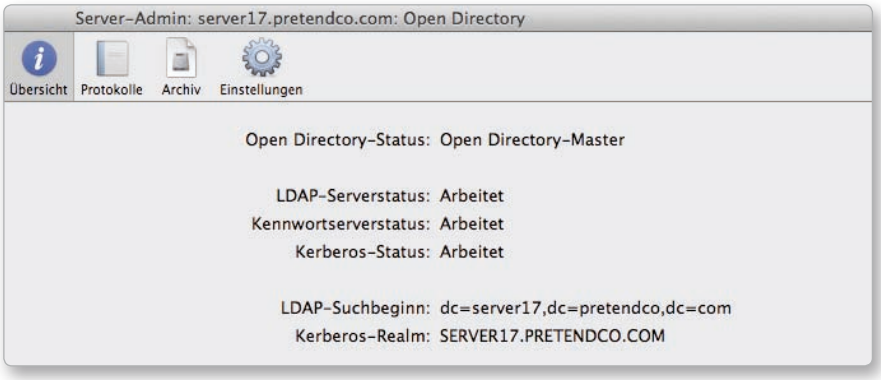
Öffnen Sie die Server-App auf dem Administratorcomputer, und stellen Sie eine Verbindung zu dem Open Directory-Master her (Hostname server17.pretendco.com, Benutzername *ladmin*, Kennwort *ladminpw*). Wenn Sie danach neue Benutzer mit der Server-App erstellen, werden die neuen Netzwerkbenutzer der Netzwerkgruppe *Workgroup* automatisch hinzugefügt.

3. Öffnen Sie auf dem Administratorcomputer Server-Admin, stellen Sie eine Verbindung mit dem Server her, und authentifizieren Sie sich als lokaler Administrator, falls Sie das noch nicht getan haben.

4. Klicken Sie in der Seitenleiste von Server-Admin falls nötig auf das Einblenddreieck für Ihren Server, um die zur Konfiguration bereitstehenden Dienste anzuzeigen.

5. Wählen Sie Open Directory aus.

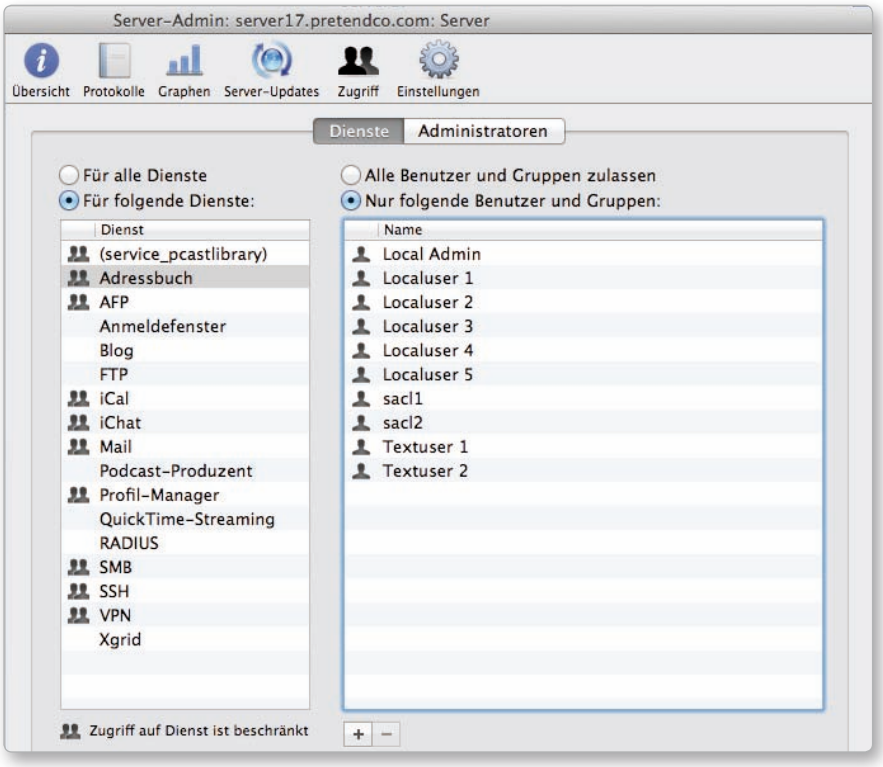
6. Klicken Sie auf Übersicht.



Wie Sie sehen, werden drei Dienste ausgeführt: LDAP-Server, Kennwortserver und Kerberos. Der LDAP-Suchbeginn und der Kerberos-Realm, deren Bezeichnungen standardmäßig auf den Hostnamen zurückgehen, werden angezeigt.

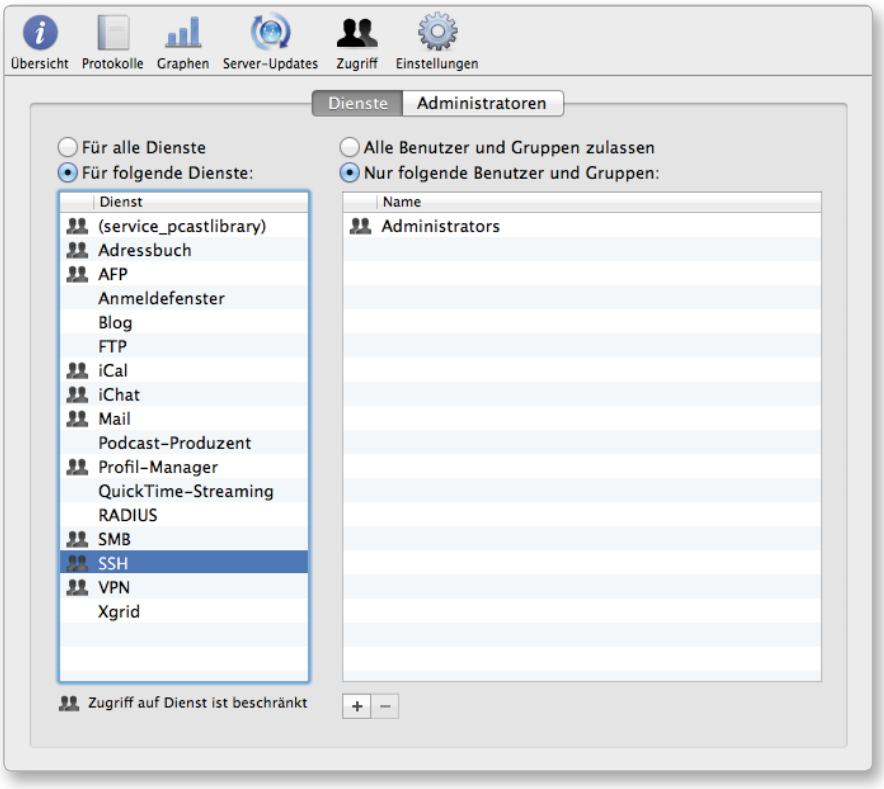
7. Klicken Sie in der Seitenleiste von Server-Admin auf Ihren Server, in der Symbolleiste auf Zugriff und dann auf Dienste. Beachten Sie die verschiedenen Dienste, neben denen Symbole angezeigt werden, was bedeutet, dass sie über SACLs verfügen.

8. Wählen Sie den Adressbuchdienst. Dies ist einer der Dienste mit einer SACL.



Wie Sie sehen, hat die Server-App all Ihre lokalen Benutzer automatisch in die die SACL für den Adressbuchdienst aufgenommen, sodass diese Benutzer Zugriff auf den Dienst haben. Wenn Sie einen neuen Benutzer mit der Server-App erstellen, fügt sie ihn automatisch zu den passenden SACLs hinzu.

9. Wählen Sie den Dienst SSH aus.



Die SSH-SACL erlaubt nur Mitgliedern der lokalen Administratorengruppe den Zugriff auf den SSH-Dienst. SSH gehört nicht zu den Diensten, die automatisch aktualisiert werden.

Sehen Sie sich als Nächstes den Systemschlüsselbund auf dem Lion Server-Computer an. Dazu müssen Sie sich an dem Server anmelden.

10. Wählen Sie Ihren Server in der Seitenleiste von Server-Admin aus.

11. Wählen Sie Darstellung > Auf Serverbildschirm zugreifen.

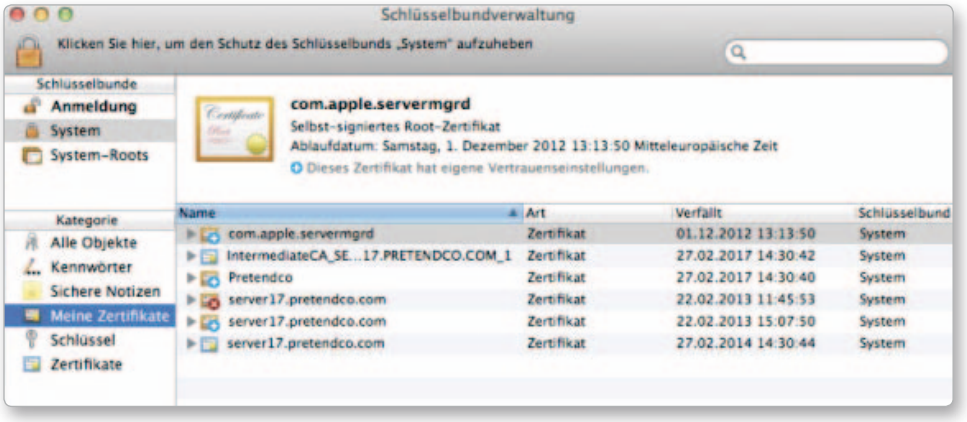
12. Geben Sie die Anmeldedaten des lokalen Administratoraccounts an (*ladmin* mit Kennwort *ladminpw*), und klicken Sie auf Verbinden.

13. Melden Sie sich falls nötig als lokaler Administrator am Lion Server-Computer an.

14. Öffnen Sie auf dem Lion Server-Computer mithilfe von Launchpad die Schlüsselbundverwaltung im Ordner *Dienstprogramme*.

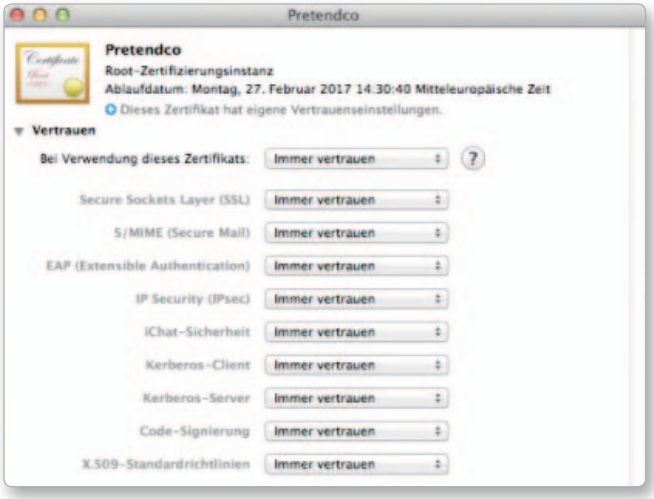
15. Klicken Sie unter Schlüsselbunde auf System.

16. Klicken Sie unter Kategorie auf Meine Zertifikate.

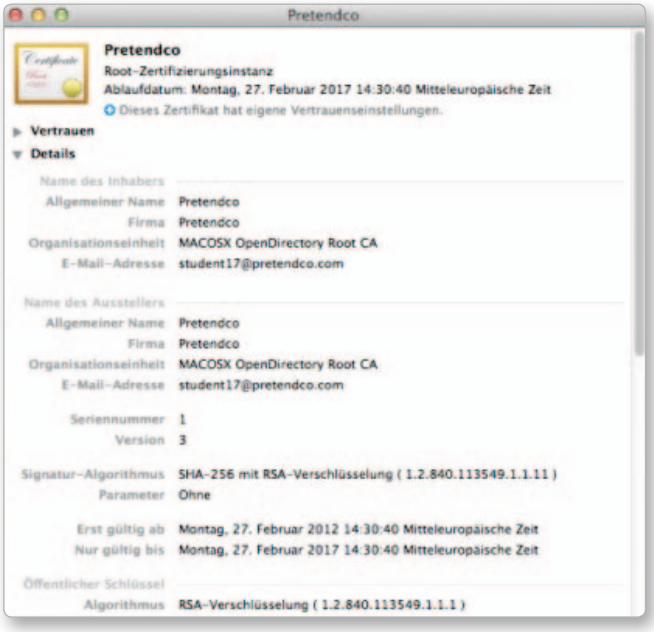


17. Doppelklicken Sie auf die Root-Zertifizierungsinstanz für Ihre Organisation, in diesem Beispiel also auf Pretendco.

18. Klicken Sie auf das Einblenddreieck für Vertrauen, und vergewissern Sie sich, dass Bei Verwendung dieses Zertifikats die Option Immer vertrauen eingestellt ist.



19. Klicken Sie erneut auf das Einblenddreieck für Vertrauen, um weniger Informationen über die Vertrauenseinstellungen anzuzeigen.



Vergewissern Sie sich unter Details, dass der Organisationsname (*Pretendco*) als Wert für Vollständiger Name und Organisation verwendet wird, dass die Organisationseinheit *MACOSX OpenDirectory Root CA* lautet und dass als E-Mail-Adresse diejenige angezeigt wird, die Sie zuvor angegeben haben.

Wie Sie sehen, sind die Informationen in den Abschnitten Aussteller und Name des Inhabers identisch. Die Root-Zertifizierungsstelle hat sich natürlich selbst-signiert.

20. Beenden Sie die Schlüsselbundverwaltung.

21. Beenden Sie die Bildschirmfreigabe.

Nachdem Sie Ihren Server als Open Directory-Master konfiguriert haben, können Sie andere Computer im Netzwerk für den Zugriff auf die Verzeichnisdienste des Servers konfigurieren.

HINWEIS ► Ändern Sie die Open Directory-Funktion nicht, nachdem Sie Accounts zur freigegebenen Open Directory-Domäne auf Ihrem Server hinzugefügt haben. Sie verlieren sonst unter Umständen alle Ihre Accountinformationen, und die Zuordnung der Daten Ihrer Benutzer kann verloren gehen.

Eine kurze Wiederholung: Sie haben mit einer lokalen Datenbank für Ihre lokalen Benutzer begonnen. Diese Datenbank ist weiterhin vorhanden. Der Administrator dieser Datenbank hat den Kurznamen *ladmin*. Sie haben eine zweite gemeinsam genutzte LDAP-Datenbank erstellt. Der Administrator dieser Datenbank hat den Kurznamen *diradmin*. Die Datenbanken sind eigenständig und erfordern unterschiedliche Anmeldedaten für die Verwaltung. Ferner haben Sie eine Kennwortserver-Datenbank erstellt, in der Benutzerkennwörter gespeichert werden, sowie ein Kerberos-KDC (*Key Distribution Center*). Zu diesen Punkten erfahren Sie in einem anderen Abschnitt mehr.

Einrichten eines Lion Server-Computers als Open Directory-Replik

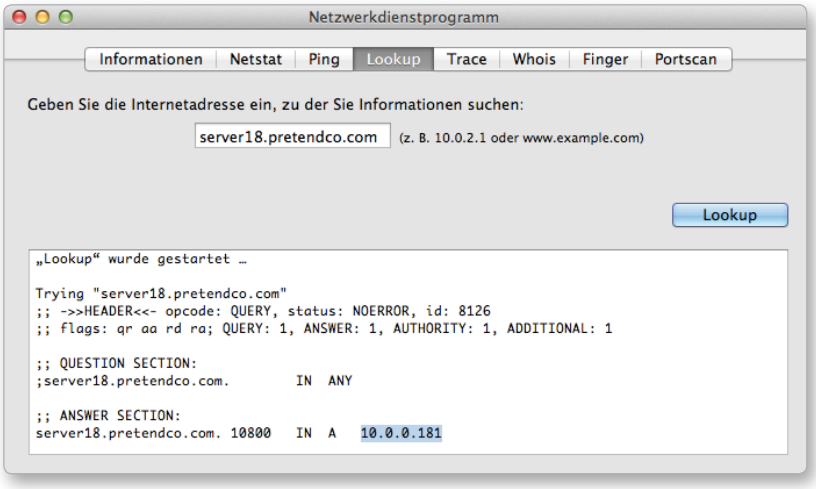
In diesem Abschnitt wird beschrieben, wie Sie eine Replik Ihres Open Directory-Masters mit Lion Server bereitstellen. Wenn Sie nur mit einem Lion Server-Computer und einem Lion-Client arbeiten, können Sie diese Übung lesen, aber die Schritte nicht ausführen. Für diese Übung wird vorausgesetzt, dass Sie einen weiteren Lion Server-Computer mit der Adresse 10.0.0.181 haben und diesen als Replik von 10.0.0.171 einrichten möchten. Außerdem müssen sowohl der Administratorcomputer als auch beide Server auf die Forward- und Reverse-DNS-Einträge für beide Server zugreifen können.

HINWEIS ► Sie können einen zweiten Server zur Verwendung als Open Directory-Replik einrichten, indem Sie wie in Kapitel 1, »Installieren und Konfigurieren von OS X Lion Server«, vorgehen, dabei aber 10.0.0.181 als IP-Adresse und server18 als Computername verwenden.

Informationen zum Konfigurieren von server17 zur Bereitstellung der DNS-Einträge für den Hostnamen server18.pretendco.com mit der IP-Adresse 10.0.0.181 finden Sie im Abschnitt »Konfigurieren des DNS-Dienstes zur Unterstützung mehrerer Open Directory-Server« am Ende dieses Kapitels.

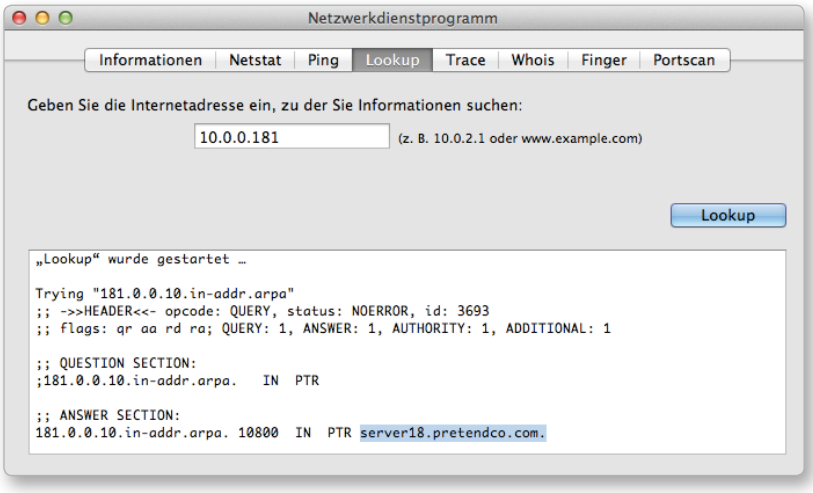
Führen Sie die folgenden Schritte aus, um die DNS-Einträge für den Server zu überprüfen, den Sie in eine Open Directory-Replik umwandeln möchten:

1. Öffnen Sie auf dem Administratorcomputer die Server-App.
2. Wählen Sie im Menü Werkzeuge die Bildschirmfreigabe.
3. Geben Sie den Hostnamen des Servers ein, den Sie als Open Directory-Replik einrichten möchten.
4. Authentifizieren Sie sich als *ladmin*, um den Bildschirm Ihres Servers freizugeben.
5. Melden Sie sich im Anmeldefenster des Servers als *ladmin* an (Kennwort *ladminpw*), falls Sie das noch nicht getan haben.
6. Öffnen Sie Launchpad, klicken Sie auf den Ordner *Dienstprogramme* und dann auf das Netzwerkdienstprogramm.
7. Klicken Sie auf den Titel Lookup.
8. Geben Sie den Hostnamen Ihres Servers in das Textfeld ein.
9. Klicken Sie auf Lookup.



10. Vergewissern Sie sich, dass unter ANSWER SECTION der Hostname und die IP-Adresse des Servers aufgeführt werden.

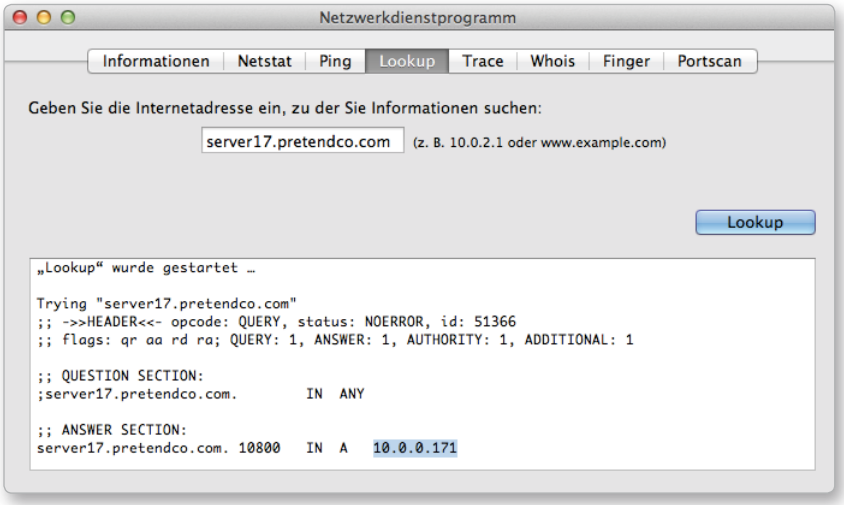
11. Geben Sie in das Textfeld die IP-Adresse des Servers ein, und klicken Sie auf Lookup.



12. Vergewissern Sie sich, dass unter ANSWER SECTION der Hostname des Servers aufgeführt wird.

Überprüfen Sie schließlich noch, dass der Lion Server-Computer die IP-Adresse des Open Directory-Masters über dessen Hostnamen herausfinden kann.

13. Geben Sie in das Textfeld den Hostnamen des Open Directoy-Masters ein, und klicken Sie auf Lookup.



Vergewissern Sie sich, dass unter ANSWER SECTION die IP-Adresse des Open Directoy-Masters aufgeführt wird. Die anderen Angaben unter ANSWER SECTION zu erläutern, würde den Rahmen dieses Buches sprengen.

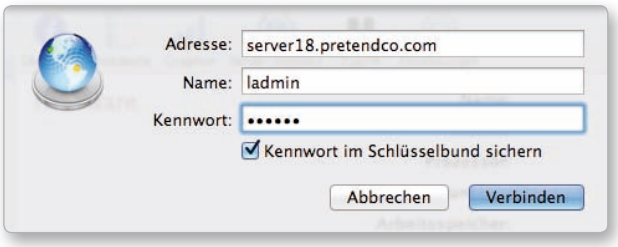
14. Schließen Sie auf dem Lion Server-Computer das Netzwerkdienstprogramm.

15. Melden Sie sich auf dem Lion Server-Computer ab.

16. Beenden Sie die Bildschirmfreigabe auf dem Administratorcomputer.

Gehen Sie wie folgt vor, um Ihren Lion Server-Computer in eine Open Directory-Replik umzuwandeln:

1. Öffnen Sie Server-Admin auf dem Administratorcomputer, und stellen Sie die Verbindung zu *server18.pretendco.com* her.



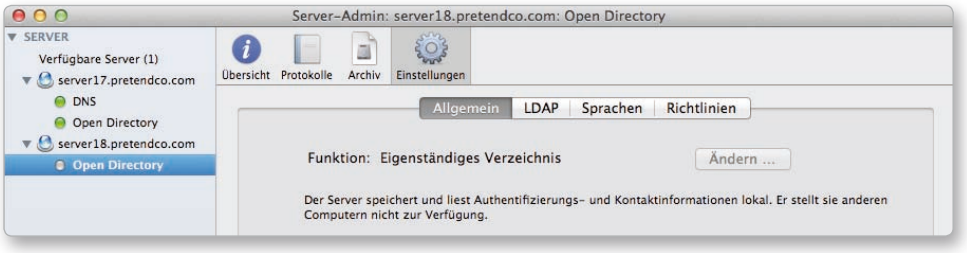
2. Wenn Sie die Meldung »Bei diesem Server sind keine Dienste als konfiguriert markiert« erhalten, klicken Sie auf Fortfahren.

3. Wenn Sie nicht automatisch zum Abschnitt Dienste mit dem hervorgehobenen Eintrag server18.pretendco.com in der Seitenleiste von Server-Admin weitergeleitet werden, klicken Sie in der Symbolleiste auf Einstellungen und dann auf Dienste.

4. Aktivieren Sie das Markierungsfeld, um Open Directory zur Liste der Dienste hinzuzufügen, und klicken Sie auf Sichern.

5. Klicken Sie falls notwendig auf das Einblenddreieck, um die Dienste für *server18.pretendco.com* in der Seitenleiste von Server-Admin anzuzeigen.

6. Klicken Sie unter server18.pretendco.com auf Open Directory.



Vergewissern Sie sich, dass Eigenständiges Verzeichnis als Rolle von *server18* angezeigt wird.

7. Klicken Sie wie beim Erstellen eines Open Directory-Masters in der Symbolleiste auf Einstellungen, auf Allgemein und danach auf Ändern, um den Open Directory-Assistenten zu öffnen.

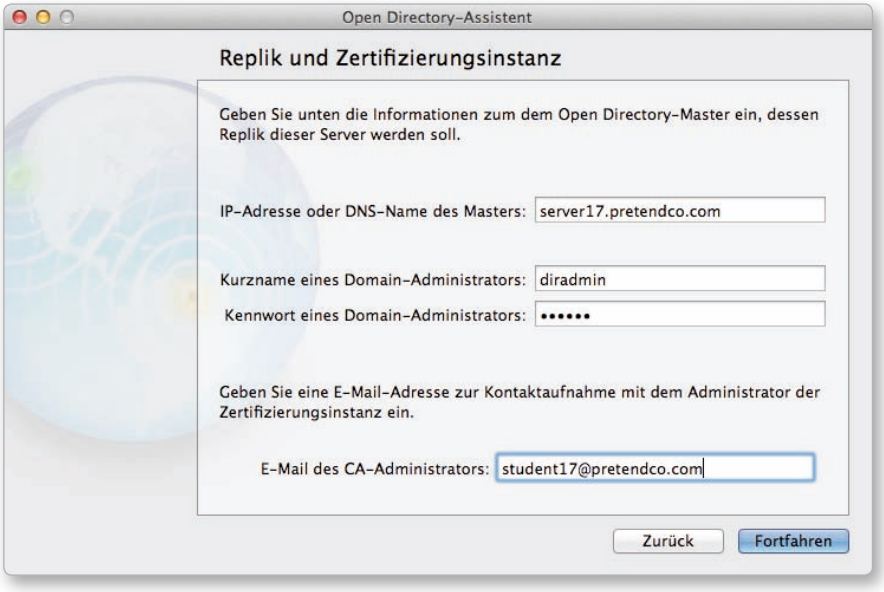
   HINWEIS ▸ Wenn Sie keinen Open Directory-Master haben, können Sie keine Replik erstellen.

   Ist dieser Server bereits ein Open Directory-Master, wird der gesamte Inhalt der aktuellen LDAP-Datenbank gelöscht.

8. Nachdem der Open Directory-Assistent geöffnet wurde, wählen Sie Eine Open Directory-Replik einrichten aus und klicken auf Fortfahren.

9. Richten Sie die Replik mit den folgenden Parametern ein (achten Sie darauf, dass Sie den DNS-Namen des Open Directory-Masters verwenden und nicht die IP-Adresse oder den Bonjour-Namen).

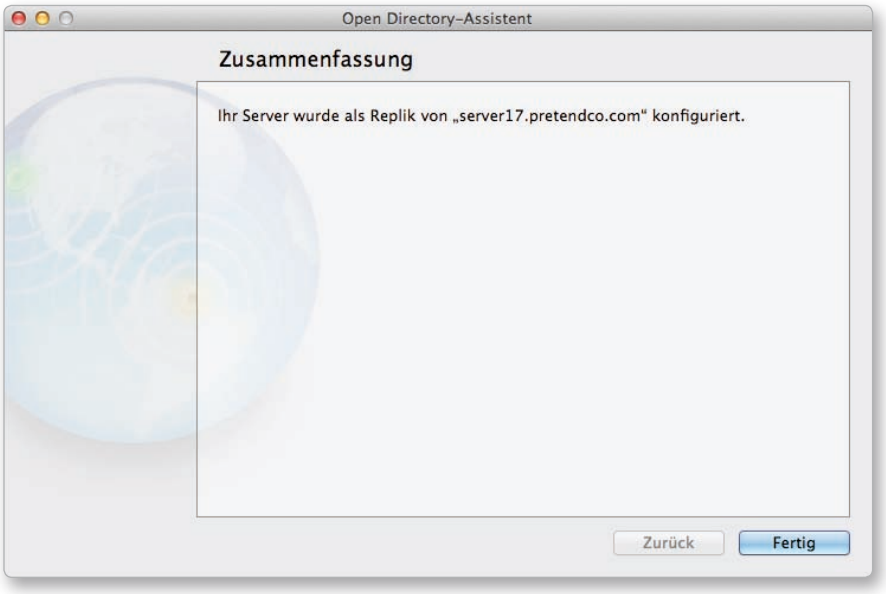
   - IP-Adresse oder DNS-Name des Masters: **server17.pretendco.com**
   - Kurzname des Domain-Administrators: **diradmin**
   - Kennwort des Domain-Administrators: **diradminpw**
   - E-Mail-Adresse des Administrators der Zertifizierungsinstanz: **student17@pretendco.com**



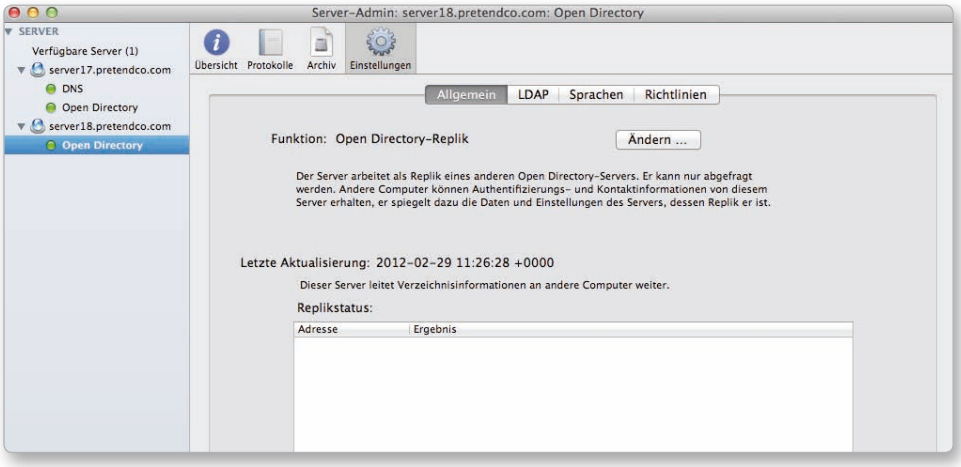
10. Klicken Sie auf Fortfahren.

11. Klicken Sie im Fenster Einstellungen bestätigen auf Fortfahren.

12. Klicken Sie im Fenster Zusammenfassung auf Fertig.

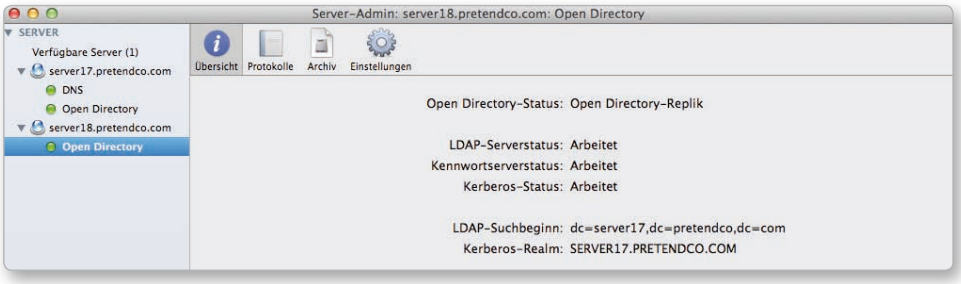


Die Rolle von *server18* wird als Open Directory-Replik aufgeführt. Beachten Sie, dass der Bereich Replikstatus leer ist. Das liegt daran, dass darin Server aufgeführt werden, die Repliken dieses Servers sind.

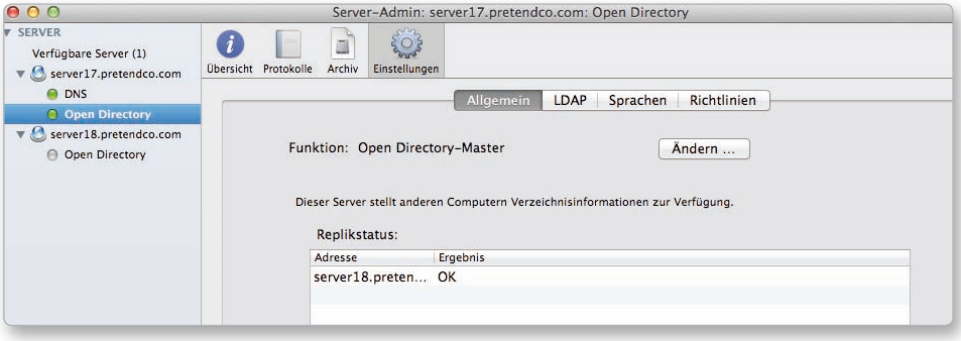


13. Klicken Sie in der Symbolleiste auf Übersicht.

Beachten Sie, dass *server18* jetzt eine Open Directory-Replik ist und alle drei Dienste bereitstellt: LDAP-Server, Kennwortserver und Kerberos. Der Kerberos-Realm hat den Hostnamen des Open Directory-Masters als Grundlage.



14. Wählen Sie in der Seitenleiste von Server-Admin Open Directory unter server17.pretendco.com aus, klicken Sie auf Einstellungen und dann auf Allgemein.



Sie sehen, dass *server17* die Rolle des Open Directory-Masters hat, während *server18.pretendco.com* als Replik aufgeführt wird.

Nachdem Sie Ihren Server als Open Directory-Replik konfiguriert haben, können andere Computer bei Bedarf eine Verbindung dazu herstellen. Der Open Directory-Master aktualisiert die Repliken automatisch, wenn sich die Verzeichnisinformationen ändern.

Nachdem eine einzelne Replik erstellt wurde, können andere Lion Server-Computer als Repliken der Replik konfiguriert werden. Damit wird die Redundanz erhöht und die Leistung der gesamten Open Directory-Struktur potenziell verbessert.

TIPP Da bei der Replikation und bei Kerberos Zeitstempel zum Einsatz kommen, empfiehlt es sich, die Uhren aller Open Directory-Master, -Repliken und -Server mithilfe von NTP mit vorhandenen Mastern zu synchronisieren. Die NTP-Dienste werden in Server-Admin aktiviert. Sie geben darin auch den gewünschten NTP-Server an.

Einrichten von Lion Server zur Verwendung eines anderen Open Directory-Servers

Da die Systemeinstellung Benutzer & Gruppen Ihnen automatisch anbietet, Ihren Client oder Server so einzurichten, dass er der Zertifizierungsinstanz des Open Directory-Masters und der Intermediate-Instanz vertraut, sollten Sie diese Systemeinstellung zur Bindung an einen Open Directory-Server verwenden. Um die Dienste Ihres Servers dazu zu bringen, den neuen Verzeichnisdienst zur Authentifizierung zu nutzen, setzen Sie außerdem Server-Admin ein.

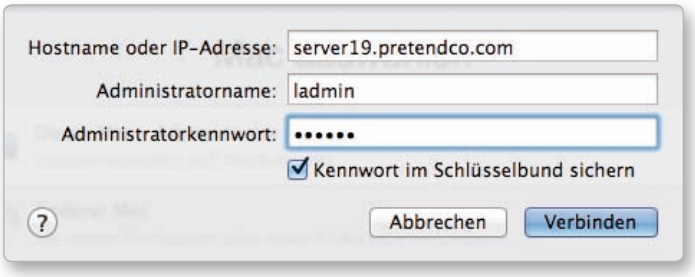
HINWEIS ▶ Sie könnten zwar auch in der Server-App Verwalten > Mit Verzeichnis verbinden wählen, aber dabei werden Sie zuerst dazu aufgefordert, Ihren OS X Lion Server-Computer als einen weiteren Open Directory-Master einzurichten. Erst danach erhalten Sie die Möglichkeit, ihn an einen anderen Verzeichnisdienst zu binden. Da bei dieser Methode automatisch SACLs erstellt werden, können nur die Benutzer, die Sie »importieren«, andere Dienste als den Wiki-Dienst des Lion Server-Computers nutzen.

In dieser Übung wird Folgendes vorausgesetzt:

- Sie verfügen aus der vorherigen Übung über eine Replik, die mit der Adresse 10.0.0.181 konfiguriert ist.
- Sie haben einen dritten Server so eingerichtet, wie es in Kapitel 1, »Installieren und Konfigurieren von OS X Lion Server«, beschrieben wurde, dabei aber 10.0.0.191 als IP-Adresse und *server19* als Computernamen verwendet.
- Sie konfigurieren einen eigenständigen Lion Server-Computer mit der Adresse 10.0.0.191, der an die Replik mit der Adresse 10.0.0.181 gebunden wird.
- Für diese Server sind DNS-Einträge zur Vorwärts- und Rückwärtsauflösung verfügbar.

Falls diese Voraussetzungen nicht erfüllt sind, können Sie diese Übung lesen, aber nicht durchführen.

1. Öffnen Sie auf dem Administratorcomputer die Server-App, wählen Sie Verwalten > Mit Server verbinden, wählen Sie den Server aus, an den die Bindung erfolgen soll (*server19.pretendco.com*), und authentifizieren Sie sich als *ladmin* (Kennwort *ladminpw*).



2. Wenn Sie das Dialogfeld Server kann die Identität nicht überprüfen sehen, klicken Sie auf Zertifikat einblenden, aktivieren das Markierungsfeld Immer vertrauen, klicken auf Fortfahren, authentifizieren sich, um die Änderungen an den Zertifikatvertrauenseinstellungen umzusetzen, und klicken auf Fortfahren.

3. Wählen Sie im Menü Werkzeuge die Bildschirmfreigabe.

4. Geben Sie im Fenster Mit freigegebenem Computer verbinden den Hostnamen des Servers ein (**server19.pretendco.com**), und klicken Sie auf Verbinden.

5. Geben Sie im Authentifizierungsfenster für die Bildschirmfreigabe falls nötig Anmeldedaten für *server19* ein (Name *ladmin*, Kennwort *ladminpw*).

6. Melden Sie sich an *server19* an, falls das noch nicht geschehen ist (Name *ladmin*, Kennwort *ladminpw*).

7. Bestätigen Sie mithilfe des Netzwerkdienstprogramms, dass die Forward- und Reverse-DNS-Einträge für *server19.pretendco.com* sowie die Forward-Einträge für die Open Directory-Replik und den Open Directory-Master (*server18.pretendco.com* bzw. *server17.pretendco.com*) vorhanden sind (eine genaue Anleitung dazu erhalten Sie im Abschnitt »Untersuchen der DNS-Einträge für Lion Server«).

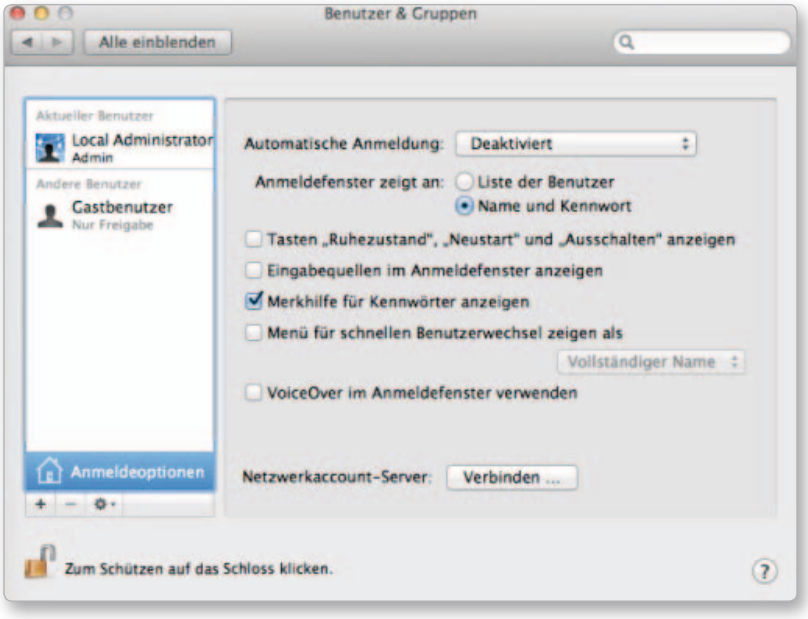
8. Öffnen Sie die Systemeinstellungen über das Apple-Menü.

9. Wählen Sie Benutzer & Gruppen.

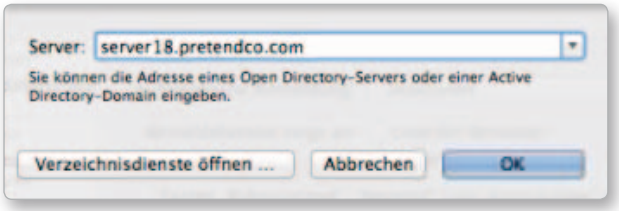
10. Wählen Sie Anmeldeoptionen.

11. Klicken Sie ggf. auf das Schlosssymbol in der unteren linken Ecke, und geben Sie die Anmeldedaten des lokalen Administrators ein.

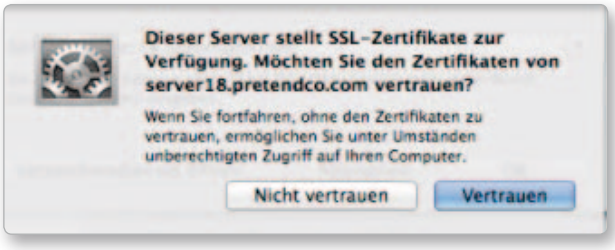
12. Klicken Sie auf Verbinden.



13. Geben Sie den Hostnamen Ihrer Open Directory-Replik ein (*server18.pretendco.com*; wenn Sie nur einen Open Directory-Master haben, verwenden Sie stattdessen *server17.pretendco.com*), und klicken Sie auf OK.

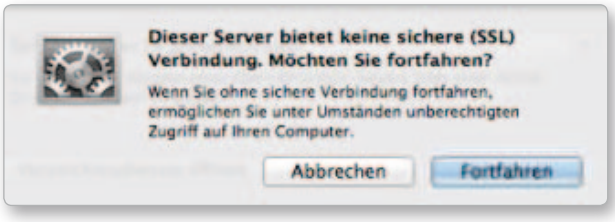


14. Klicken Sie im Dialogfeld Dieser Server stellt SSL-Zertifikate zur Verfügung auf Vertrauen.



15. Klicken Sie im Fenster Dieser Server bietet keine sichere (SSL) Verbindung auf Fortfahren.

Standardmäßig bietet ein Open Directory-Master keine LDAP-Dienste über SSL an. Da die im LDAP-Verzeichnis abgelegten Informationen nicht als vertraulich angesehen werden, ist das für die meisten Organisationen kein Problem.

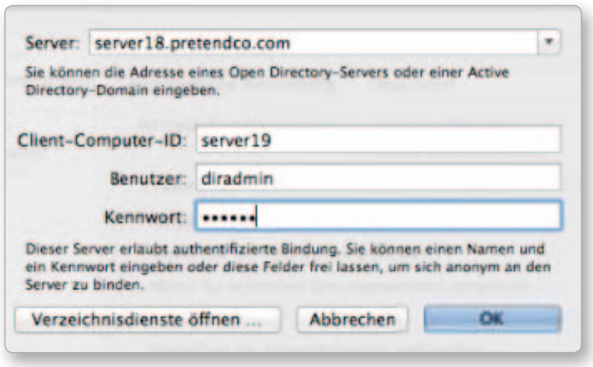


16. Lassen Sie im Fenster Client-Computer-ID die automatisch aus dem Hostnamen erstellte ID unverändert.

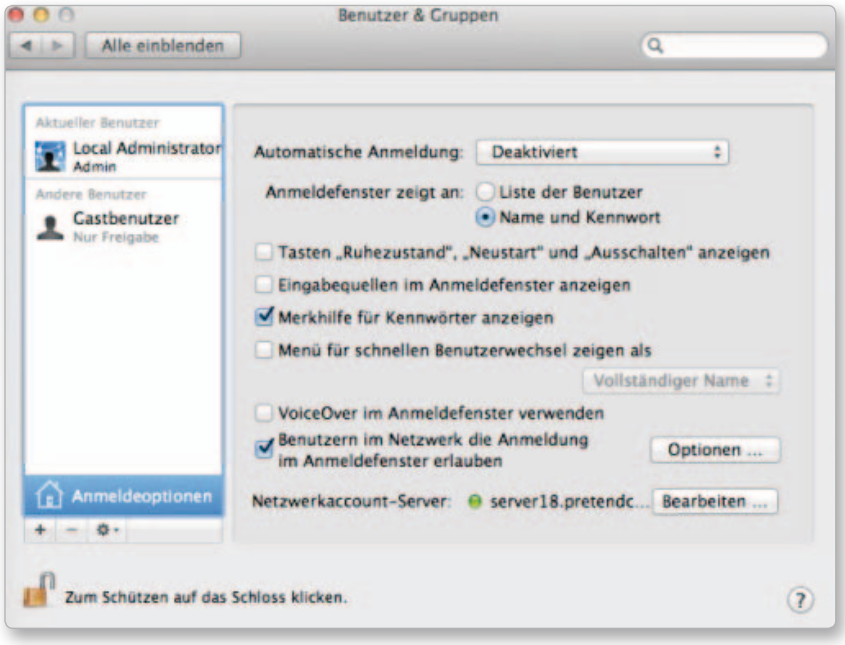
Sie haben hier die Wahl zwischen einer anonymen und einer authentifizierten Bindung.

Die anonyme Variante eignet sich für die Bindung von Lion-Clients, aber wenn Sie einen Lion Server-Computer an einen Open Directory-Master binden, sollten Sie die authentifizierte Bindung nutzen, bei der sich der Client und der Open Directory-Dienst gegenseitig authentifizieren. Bei der authentifizierten Bindung wird im Open Directory-Dienst ein Computereintrag erstellt, der zur gegenseitigen Authentifizierung dient.

Für die authentifizierte Bindung müssen Sie die Anmeldedaten des Verzeichnisadministrators angeben. Verwenden Sie die bereits bekannten Anmeldedaten mit dem Benutzernamen *diradmin* und dem Kennwort *diradminpw,* und klicken Sie auf OK.



17. In der Systemeinstellung Benutzer & Gruppen wird der Server jetzt als Netzwerk-Account-Server aufgeführt.



Schließen Sie die Systemeinstellungen.

18. Melden Sie sich als *ladmin* von *server19* ab.

19. Beenden Sie die Bildschirmfreigabe auf dem Administratorcomputer.

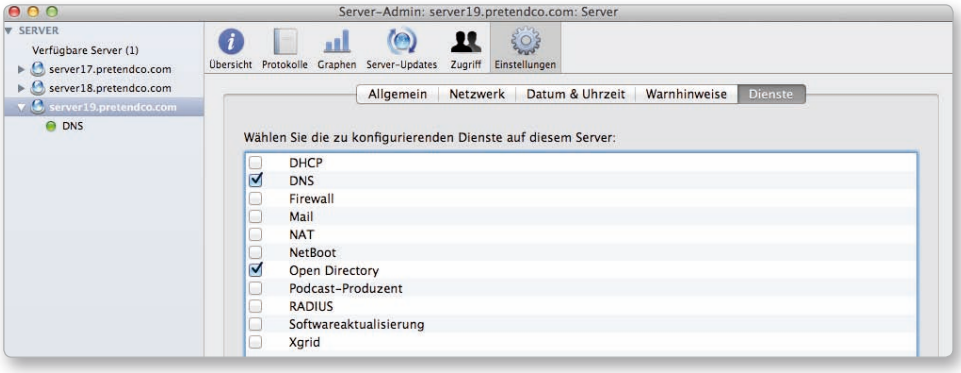
Als Nächstes bereiten Sie die Dienste des Mitgliedservers mit Server-Admin vor, um sie den Netzwerkbenutzern anzubieten.

20. Öffnen Sie auf dem Administratorcomputer das Programm *Server-Admin*.

21. Wenn *server19* in der Seitenleiste von Server-Admin noch nicht aufgeführt wird, klicken Sie im Programm unten links auf das Einblendmenü zum Hinzufügen (+), wählen Server hinzufügen, geben *server19.pretendco.com* und Ihre Anmeldedaten als lokaler Administrator ein und klicken auf Verbinden.

22. Wählen Sie *server19.pretendco.com* in der Seitenleiste von Server-Admin aus, klicken Sie auf Einstellungen und dann auf Dienste.

23. Aktivieren Sie das Markierungsfeld für Open Directory, und klicken Sie auf Sichern.

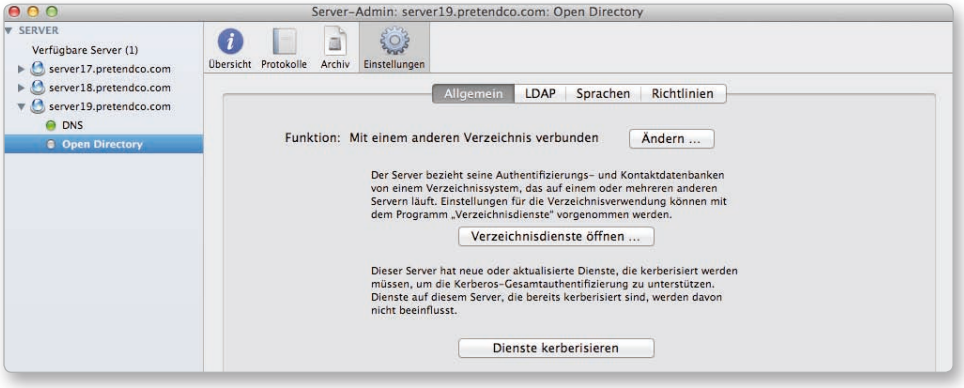


24. Klicken Sie falls nötig auf das Einblenddreieck für *server19.pretendco.com*, um die verfügbaren Dienste anzuzeigen.

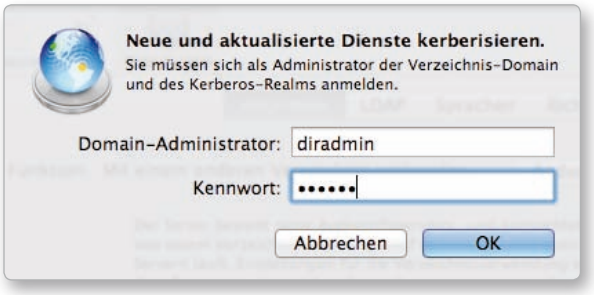
25. Wählen Sie in der Seitenleiste von Server-Admin Open Directory unter server19.pretendco.com aus.

26. Klicken Sie falls nötig auf Einstellungen und dann auf Allgemein.

27. Unter Rolle ist Mit einem anderen Verzeichnis verbunden angegeben. Klicken Sie auf Dienste kerberisieren.



28. Geben Sie die Anmeldedaten von *diradmin* ein, und klicken Sie auf OK.

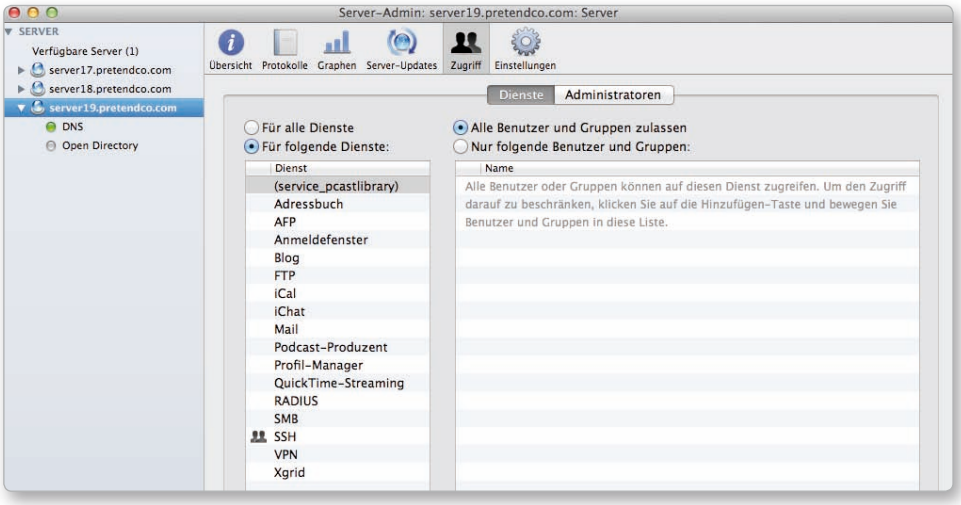


server19 ist jetzt so eingerichtet, dass er Kerberos-Anmeldedaten zur Authentifizierung aller Benutzer in dem Open Directory-Dienst akzeptiert, an den er gebunden ist.

HINWEIS ► Machen Sie sich keine Sorgen, wenn die Schaltfläche Dienste kerberisieren immer noch sichtbar ist. Sie müssen nicht noch einmal darauf klicken.

29. Untersuchen Sie die SACLs für die von *server19* angebotenen Dienste.

Wählen Sie in der Seitenleiste von Server-Admin *server19.pretendco.com* aus, und klicken Sie auf Zugriff.



Wie Sie sehen, hat *server19* keine SACLs bis auf die für den SSH-Dienst. Hätten Sie zur Bindung die Server-App verwendet (statt der Systemeinstellung Benutzer & Gruppen), gäbe es SACLs für verschiedene Dienste.

Verwenden des Programms Verzeichnisdienste über das Netzwerk

Sie können weiterhin das Programm *Verzeichnisdienste* anstelle der Systemeinstellungen verwenden. Die Systemeinstellung Benutzer & Gruppen enthält sogar einen Kurzbefehl für das Programm Verzeichnisdienste, das sich in */System/Library/CoreServices* befindet. Das Programm Verzeichnisdienste bietet etwas mehr Kontrolle als die Schaltfläche Verbinden der Systemeinstellung Benutzer & Gruppen. Es ermöglicht Ihnen, einen entfernten Computer von Lion oder Lion Server aus zu steuern, sodass die Bildschirmfreigabe nicht zwingend erforderlich ist.

In der folgenden Übung verwenden Sie das Programm Verzeichnisdienste auf Lion, um eine Verbindung mit dem Lion Server-Computer herzustellen und die Einstellungen für die Nutzung des Verzeichnisses zu überprüfen.

Für diese Übung wird vorausgesetzt, dass Sie über eine Replik mit der Adresse 10.0.0.181 verfügen, dass Sie einen eigenständigen Lion Server-Computer mit der Adresse 10.0.0.191 an die Replik mit der Adresse 10.0.0.181 gebunden haben, und dass Sie für diese Server über DNS-Einträge zur Vorwärts- und Rückwärtsauflösung verfügen.

1. Öffnen Sie auf dem Administratorcomputer falls nötig die Server-App.

2. Wählen Sie im Menü Werkzeuge das Programm *Verzeichnisdienste*.

3. Sie müssen das Programm Verzeichnisdienste verwenden, um eine Verbindung zu Ihrem Server herzustellen und die Verzeichnisdienste zu untersuchen, die Ihr Server verwendet.

   Wählen Sie Ablage > Verbinden.

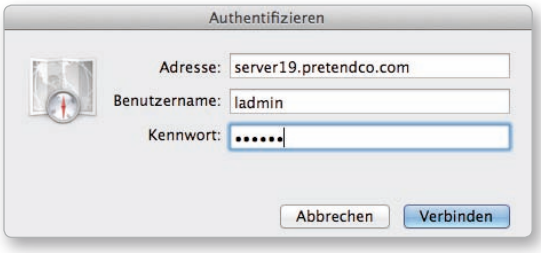
4. Geben Sie die folgenden Informationen ein, um sich beim entfernten Server zu authentifizieren:

   Adresse: **server19.pretendco.com**

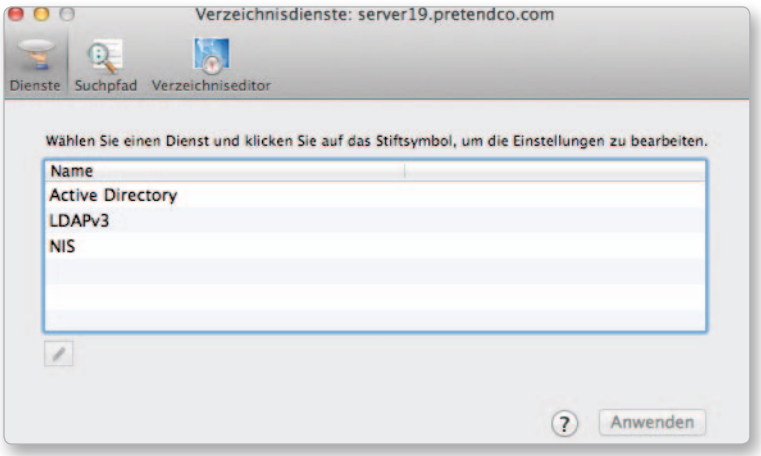
   Benutzername: **ladmin**

   Kennwort: **ladminpw**

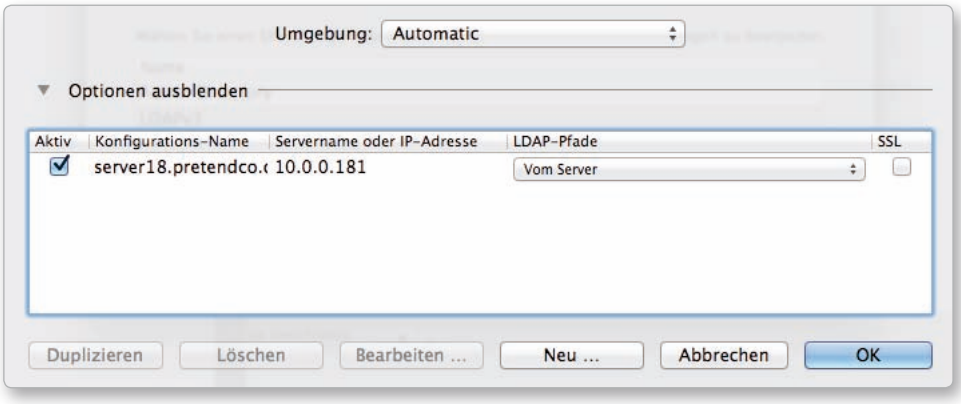
   Klicken Sie auf Verbinden.



5. Klicken Sie in der Symbolleiste ggf. auf Dienste.



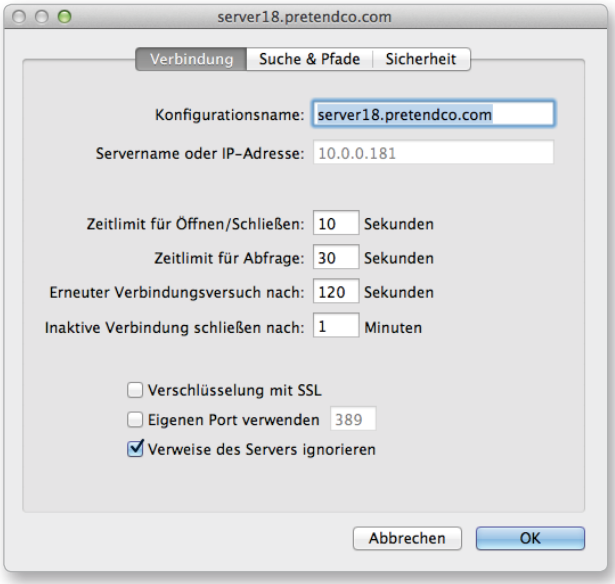
6. Doppelklicken Sie auf LDAPv3.



Der Konfigurationsname basiert auf dem DNS-Namen des Servers, aber unter Servername ist die IP-Adresse des Open Directory-Masters eingetragen.

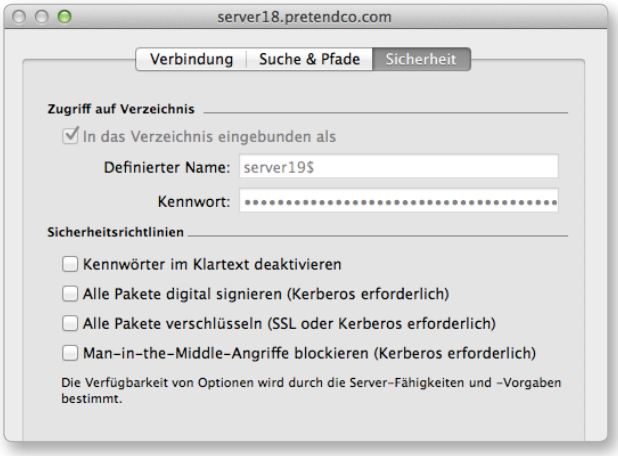
7. Wählen Sie die Konfiguration *server18.pretendco.com* aus, und klicken Sie auf Bearbeiten.

Dadurch wird das Fenster Verbindung geöffnet, das ausführliche Informationen über die Verbindung zum Open Directory-Server enthält.



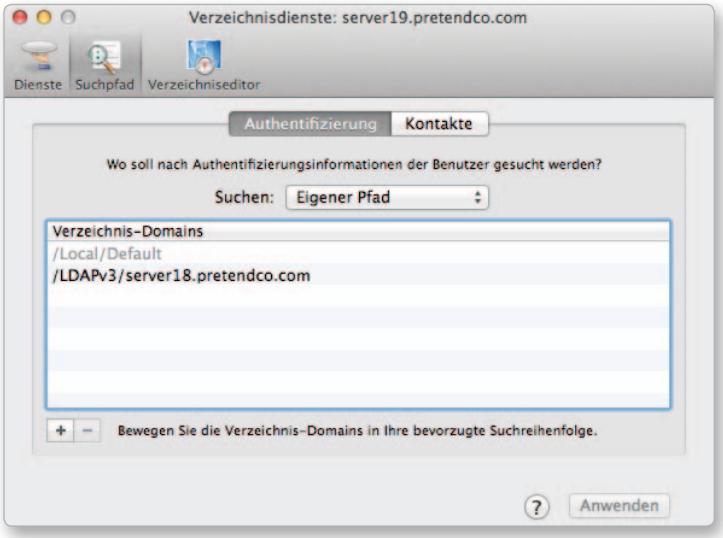
8. Klicken Sie auf den Titel Sicherheit.

   Sie sehen, dass *server19* den Computereintrag *server19$* verwendet. Machen Sie sich keine Sorgen darüber, dass das Markierungsfeld Kennwörter im Klartext deaktivieren nicht aktiviert ist. Diese Einstellung gilt nur für die Verbindung mit anderen LDAP-Diensten, nicht für Open Directory-Server.



9. Klicken Sie auf OK, um die LDAP-Serverliste zu schließen.

10. Klicken Sie in der Symbolleiste auf Suchpfad.



Vergewissern Sie sich, dass der Open Directory-Server aufgeführt wird. Der Name beginnt in der Liste mit */LDAPv3/*, gefolgt von der IP-Adresse bzw. dem DNS-Namen.

11. Klicken Sie auf Abbrechen, um das Fenster zu schließen.

12. Klicken Sie erneut auf Abbrechen, um die Liste der LDAP-Server zu schließen.

13. Beenden Sie das Programm Verzeichnisdienste. Sichern Sie keine Änderungen, falls Sie dazu aufgefordert werden, da Sie das Programm Verzeichnisdienste nur zum Prüfen der Einstellungen verwendet haben.

Sie haben jetzt mit dem Programm Verzeichnisdienste unter Lion eine Verbindung zu einem entfernten Server hergestellt und Einstellungen geprüft.

Binden von Lion an den Open Directory-Dienst

Nachdem Sie einen Open Directory-Master (und vielleicht auch eine oder mehr Repliken) eingerichtet haben, müssen Sie auch die Clientcomputer an den Verzeichnisdienst binden, damit diese ihn nutzen können. Geben Sie auf jedem Clientcomputer in der Systemeinstellung Benutzer & Gruppen einen Server an, der einen Open Directory-Dienst bereitstellt. Wenn Sie anspruchsvolle Bindungsmöglichkeiten brauchen, erstellen Sie mit dem Programm Verzeichnisdienste eine LDAP-Konfiguration, die die Adresse und den Suchpfad für einen Open Directory-Server enthält.

Als Nächstes konfigurieren Sie den Administratorcomputer so, dass er die Authentifizierungsdienste des Lion Server-Computers nutzt. Sie haben bereits ein freigegebenes Verzeichnis eingerichtet. Die Lion-Computer müssen dieses Verzeichnis finden können, damit sie sich dort anmelden können. Alle mit dem Open Directory-Dienst verbundenen Clients können Benutzer mit den Daten im freigegebenen Verzeichnis authentifizieren.

In einer Umgebung mit vielen Open Directory-Repliken können Sie Lion auch an eine Replik binden, sodass der Open Directory-Master vorrangig mit den Repliken kommunizieren kann.

Verwenden der Systemeinstellung »Benutzer & Gruppen« für die Bindung

In den folgenden Schritten verwenden Sie die Systemeinstellungen, um Ihren Lion-Computer an den Open Directory-Master zu binden. Der Vorgang ähnelt der Bindung eines Servers an einen Open Directory-Server, den Sie im vorhergehenden Abschnitt durchgeführt haben.

1. Öffnen Sie auf dem Lion-Computer die Systemeinstellung Benutzer & Gruppen.

2. Klicken Sie ggf. auf das Schlosssymbol in der unteren linken Ecke, und geben Sie die Anmeldedaten des lokalen Administrators ein.

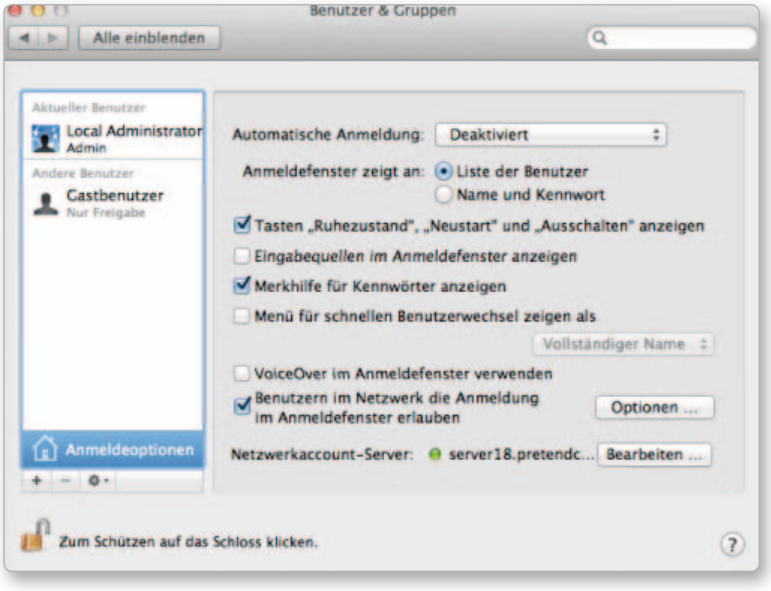
3. Klicken Sie auf Verbinden.

4. Geben Sie den Hostnamen Ihrer Open Directory-Replik ein (*server18.pretendco.com*; wenn Sie nur einen Open Directory-Master haben, verwenden Sie stattdessen *server17.pretendco.com*), und klicken Sie auf OK.

5. Klicken Sie im Dialogfeld Dieser Server stellt SSL-Zertifikate zur Verfügung auf Vertrauen.

6. Klicken Sie im Fenster Dieser Server bietet keine sichere (SSL) Verbindung auf Fortfahren.

   Damit kehren Sie zum Fenster Anmeldeoptionen zurück, wo der Eintrag Netzwerk-Account-Server jetzt aktualisiert worden ist.



7. Schließen Sie die Systemeinstellungen.

Copyright