

Apple Training Series

Mac OS X Server Essentials v10.6

Der offizielle Leitfaden zu Einsatz und Support von
Mac OS X Server v10.6

Arek Dreyer mit Ben Greisler



3

Dauer Übungsziele

Für dieses Lektion sollten Sie ungefähr 4 Stunden einplanen.

Kennenlernen der vier Open Directory-Serverfunktionen, die Sie unter Mac OS X Server konfigurieren können

Konfigurieren von Mac OS X Server als Open Directory-Server mithilfe des Serverassistenten, der Servereinstellungen und des Programms „Server-Admin“

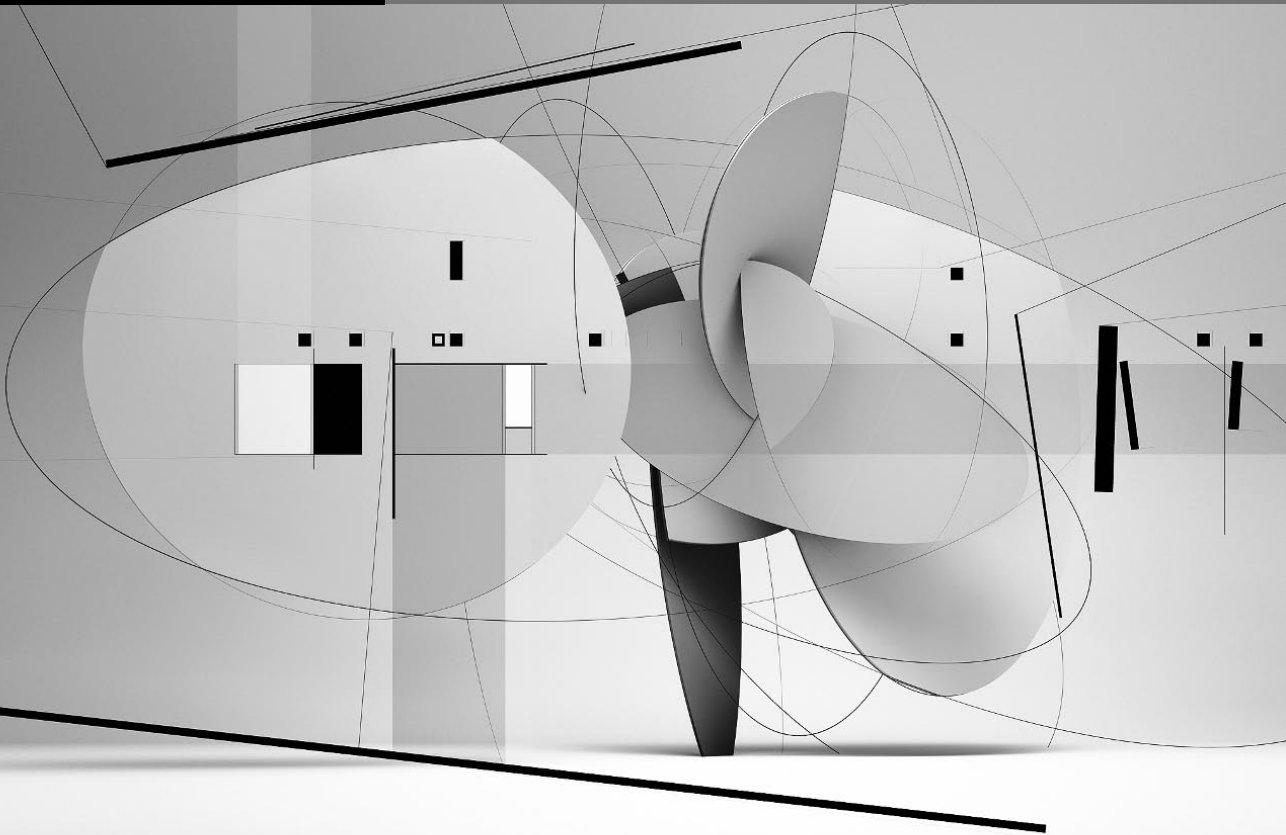
Verwenden der Systemeinstellung „Benutzer“, um einen Mac OS X-Computer an einen Open Directory-Server zu binden

Suchen und Identifizieren von Protokolldateien, die zu Open Directory gehören

Prüfen und Wiederherstellen des Inhalts eines Open Directory-Archivs

Beschreiben von Authentifizierungsarten

Verstehen der grundlegenden Kerberos-Infrastruktur



Lektion 3

Verwenden von Open Directory

In dieser Lektion wird beschrieben, wie Sie mithilfe eines Verzeichnisdiensts 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 dem Programm „Servereinstellungen“, mit dem Programm „Server-Admin“ und mit dem Arbeitsgruppenmanager einrichten und verwalten können. Abschließend erfahren Sie Näheres über gelegentlich auftretende Probleme bei Open Directory-Diensten und wie Sie diese beheben.

Open Directory ist im Bezug auf die Verwendung mit verschiedenen anderen Verzeichnisdiensten wie Active Directory, eDirectory und NIS (Network Information Service) äußerst vielseitig. In dieser Lektion wird ein VerzeichnisdienstszENARIO „Mac OS X Server-zu-Mac OS X“ erörtert. Das Buch *Mac OS X Directory Services v10.6* enthält weitere Informationen zu VerzeichnisdienstszENARIEN mit mehreren verschiedenen Plattformen.

Wenn Sie zwei zusätzliche Mac OS X Server-Computer haben, können Sie in den Übungen einen davon als Open Directory-Replik und den anderen als 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 u. U. 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.

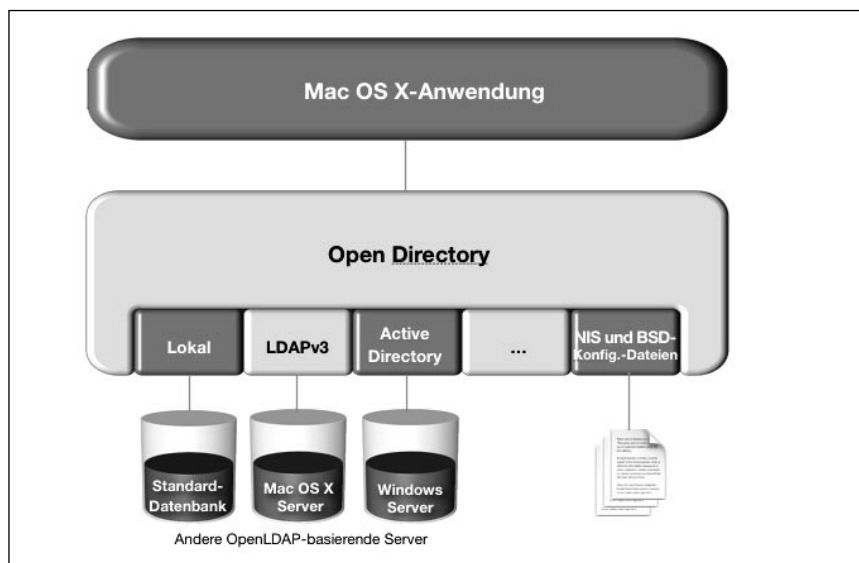
Verzeichnisdienste bieten einen solchen zentralen Speicherort für Informationen zu den Computern, Programmen und Benutzern einer Organisation. Mithilfe von Verzeichnisdiensten können Sie dafür sorgen, dass die Informationen zu allen Benutzern – etwa Namen, Kennwörter und Einstellungen – sowie zu Druckern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

Beispiel: Sobald Sie Mac OS X-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 Mac OS X-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 Verzeichnisdiensts 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 Mac OS X und Mac OS X 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 bei Mac OS X Server, die Identifizierung (Authentifizierung) und Clientverwaltung bereitstellen.



Zahlreiche Dienste von Mac OS X benötigen für eine korrekte Funktionsweise Informationen von Open Directory-Diensten. Open Directory-Dienste können 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 Open Directory-Dienste auch verwenden, um Richtlinien wie das Ablufen und die Minimallänge von Kennwörtern umzusetzen und Benutzereinstellungen zu verwalten.

Außerdem können mit Open Directory-Diensten Windows-Benutzer für Anmeldung, Dateidienste, Druckdienste und weitere Windows-Dienste authentifiziert werden, die von Mac OS X Server bereitgestellt werden. Open Directory verwendet Samba 3, mit dessen Hilfe ein Open Directory-Server als Windows-PDC (Primary Domain Controller) oder -BDC (Backup Domain Controller) genutzt werden kann.

Überblick über die Komponenten des Open Directory-Diensts

Open Directory ermöglicht eine zentrale Authentifizierung und Identifizierung. Zur Authentifizierung 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.

WEITERE INFORMATIONEN ► Unter Mac OS X Server 10.3 und 10.4 wurde LDAP wegen seiner gemeinsam genutzten Datenbank verwendet. In älteren Versionen von Mac OS X und Mac OS X Server wurde der NetInfo-Systemkonfigurationsdatenbankdienst für lokale und gemeinsam genutzte Verzeichnisdienste genutzt. Ab Mac OS X 10.5 wurde NetInfo durch einfache oder strukturierte (Text-) Dateien ersetzt.

Dabei greift der Open Directory-Dienst auf weitere Open-Source-Technologien zurück, z. B. Kerberos und LDAP, 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 Mac OS X-Computer an einen bestimmten Open Directory-Server gebunden wurde, erhält der mit Mac OS X oder Mac OS X Server betriebene Computer automatisch Zugriff auf Netzwerkressourcen, einschließlich Diensten zur Benutzerauthentifizierung, Netzwerkbenutzerordnern, Netzwerkvolumen und Einstellungen.

Überprüfen von DNS-Einträgen

Ihr Mac OS X Server-Computer muss über DNS-Einträge zur Vorwärts- und Rückwärtsauflösung verfügen, bevor Sie einen Open Directory-Master erstellen, sodass sämtliche Open Directory-Dienste bereitgestellt werden können. Zusätzlich muss der Computer, den Sie mit Server-Admin verwenden, auch über einen DNS-Eintrag für seine IP-Adresse verfügen.

Überprüfen von DNS-Einträgen für Mac OS X Server

Mit dem Mac OS X Server-Befehl `changeip` können Sie Änderungen am Hostnamen oder an der IP-Adresse Ihres Servers vornehmen oder überprüfen, ob der Hostname und die primäre IP-Adresse Ihres Servers mit den verfügbaren DNS-Einträgen übereinstimmen. Bevor Sie einen Server als Open Directory-Master oder -Replik definieren, sollten Sie sich mithilfe des Befehls `changeip` vergewissern, dass für den Hostnamen und die primäre IP-Adresse Ihres Servers geeignete DNS-Einträge verfügbar sind.

Wenn Sie Mac OS X Server in einer Umgebung konfigurieren, in der ein DNS-Eintrag für die Ihrem Server bei der Konfiguration zugewiesene IP-Adresse *verfügbar* ist, wird der DNS-Dienst vom Serverassistenten nicht konfiguriert oder gestartet. Wenn Sie

Mac OS X Server jedoch in einer Umgebung *ohne* DNS-Eintrag für die dem Server bei der Konfiguration zugewiesene IP-Adresse konfigurieren, erstellt der Serverassistent die erforderlichen DNS-Zonen und -Einträge für Hostname und IP-Adresse des Servers und startet dann den DNS-Dienst.

HINWEIS ► Lesen Sie den Abschnitt „Definieren von DNS-Einträgen“ am Ende dieser Lektion, wenn Ihre Umgebung keine DNS-Einträge für die Computer umfasst, die Sie in den Übungen für diese Lektion verwenden, und Sie Ihren Server zur Bereitstellung der geeigneten DNS-Einträge konfigurieren möchten.

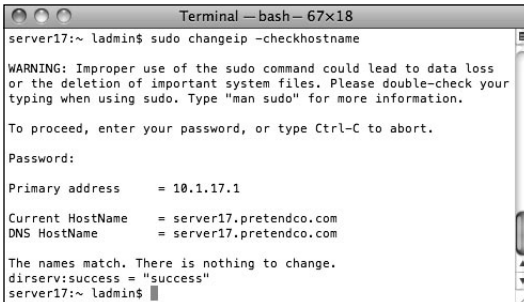
Bei den Übungen in diesem Buch wird davon ausgegangen, dass Ihr Mac OS X-Administratorcomputer Zugriff auf die DNS-Einträge Ihrer Mac OS X Server-Computer hat. In den Übungsschritten werden Sie angewiesen, die vollständig qualifizierten Domain-Namen (FQDNs) Ihrer Server (wie `server17.pretendco.com`) 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 FQDN zu verwenden. 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 ► In Lektion 7, „Netzwerkconfiguration“, im Handbuch *Apple Training Series: Mac OS X Support Essentials 10.6* finden Sie Informationen zur Verwendung des Netzwerkdienstprogramms zum Überprüfen von DNS-Einträgen.

Vergewissern Sie sich mithilfe von `changeip`, dass Ihrem Server die erforderlichen DNS-Einträge zur Verfügung stehen:

- 1 Öffnen Sie auf Ihrem Clientcomputer Server-Admin und stellen Sie als „ladmin“ eine Verbindung zu Ihrem Server (`server17.pretendco.com`) her. Wählen Sie Ihren Server in der Liste „Quelle“ aus und wählen Sie anschließend „Server“ > „Auf Serverbildschirm zugreifen“.
- 2 Authentifizieren Sie sich als „ladmin“, um den Bildschirm Ihres Servers freizugeben.
- 3 Melden Sie sich im Anmeldefenster des Servers als „ladmin“ an (Kennwort: `ladmin`).

- 4 Öffnen Sie das Programm „Terminal“ (in „/Programme/Dienstprogramme“).
- 5 Geben Sie den Befehl `sudo changeip -checkhostname` ein und drücken Sie den Zeilenschalter.
- 6 Geben Sie Ihr Kennwort (ladmin) ein, falls erforderlich.



```
Terminal — bash — 67x18
server17:~ ladmin$ sudo changeip -checkhostname
WARNING: Improper use of the sudo command could lead to data loss
or the deletion of important system files. Please double-check your
typing when using sudo. Type "man sudo" for more information.

To proceed, enter your password, or type Ctrl-C to abort.

Password:
Primary address      = 10.1.17.1
Current HostName     = server17.pretendco.com
DNS HostName         = server17.pretendco.com

The names match. There is nothing to change.
dirserv:success = "success"
server17:~ ladmin$
```

- 7 Vergewissern Sie sich, dass das Ergebnis des Befehls `changeip` „The names match. There is nothing to change.“ lautet. Falls Sie ein anderes Ergebnis erhalten, lesen Sie den Abschnitt „Definieren von DNS-Einträgen“ am Ende dieser Lektion.
- 8 Beenden Sie auf Ihrem Mac OS X-Server das Programm „Terminal“.
- 9 Beenden Sie auf Ihrem Mac OS X-Computer die Bildschirmfreigabe.

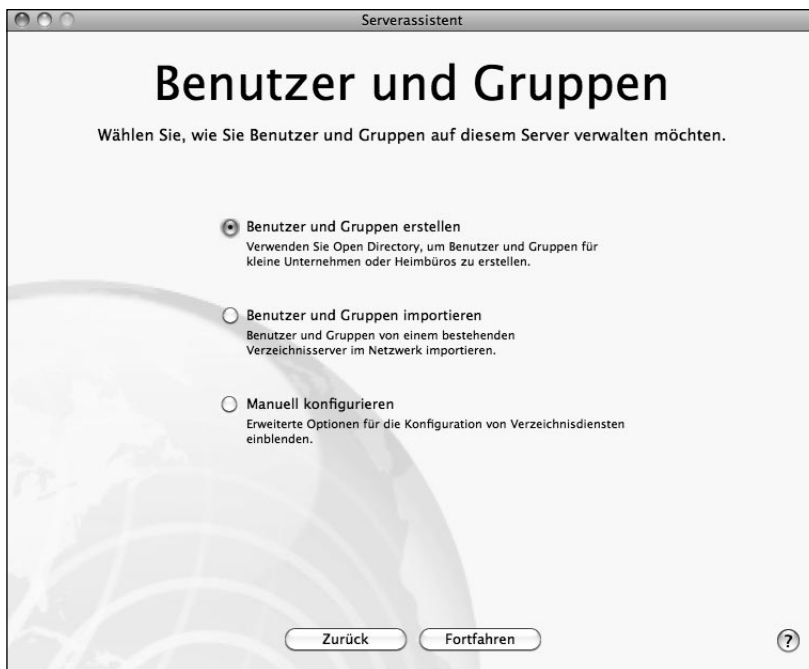
Konfigurieren von Open Directory-Diensten

Es gibt mehrere Methoden, Mac OS X Server für die Bereitstellung von Open Directory-Diensten zu konfigurieren. Wie wählen Sie die zu verwendende Methode aus? Dies hängt von Ihren Anforderungen ab. In den folgenden drei Abschnitten wird jedes Programm behandelt, das Sie verwenden können, um Ihren Mac OS X Server-Computer zur Bereitstellung von Open Directory-Diensten zu konfigurieren:

- ▶ Serverassistent
- ▶ Servereinstellungen
- ▶ Server-Admin

Konfigurieren von Open Directory-Diensten mit dem Serverassistenten

Wenn Mac OS X Server Verzeichnisdienste sowie einen Standardsatz von Diensten für Zusammenarbeit bereitstellen soll, können Sie Ihren Open Directory-Master bei der Erstkonfiguration von Mac OS X Server automatisch durch den Serverassistenten konfigurieren lassen. Wenn Sie „Benutzer und Gruppen erstellen“ oder „Benutzer und Gruppen importieren“ wählen, konfiguriert der Serverassistent Ihr freigegebenes Verzeichnis für Sie. Sie wählen weder den Kurznamen des Verzeichnisadministrators, die UID oder das Kennwort – der Serverassistent verwendet den Kurznamen „dir-admin“, die UID 1000 und das Kennwort, das Sie für Ihren ersten Account des lokalen Administrators angegeben haben.



Wenn Sie zusätzlich zum Konfigurieren Ihres Mac OS X Server-Computers als Open Directory-Master die Option „Benutzer und Gruppen importieren“ wählen, fordert der Serverassistent Sie auf, einen weiteren Verzeichnisdienst anzugeben, zu dem eine Bindung hergestellt werden kann.

Wenn Sie „Manuell konfigurieren“ wählen, können Sie vom Serverassistenten einen Open Directory-Master konfigurieren lassen. Sie können den Namen, Kurznamen und die UID des Verzeichnisadministrators angeben, aber als Kennwort für den

Benutzeraccount des Verzeichnisadministrators wird das Kennwort verwendet, das Sie dem ersten im Serverassistenten definierten Administratoraccount zugewiesen haben.

Konfigurieren von Open Directory-Diensten mit den Servereinstellungen

Wenn Sie den Serverassistenten bei der Erstkonfiguration von Mac OS X Server verwenden und „Manuell konfigurieren“ wählen, können Sie Ihren Mac OS X Server-Computer mithilfe der Servereinstellungen schnell als Open Directory-Master konfigurieren.

Wie bei den Optionen „Benutzer und Gruppen erstellen“ und „Benutzer und Gruppen importieren“ des Serverassistenten werden bei den Servereinstellungen folgende Optionen für den Benutzeraccount des Verzeichnisadministrators verwendet: der Kurzname „diradmin“, die UID 1000 und das Kennwort des Accounts des lokalen Administrators, das Sie zum Authentifizieren verwenden.

Diese Übung kann nur für einen Server ausgeführt werden, der noch kein Open Directory-Master ist.

HINWEIS ► Sie können diese Übung überspringen und Ihren Open Directory-Master mit Server-Admin statt mit den Servereinstellungen konfigurieren.

- 1 Öffnen Sie auf Ihrem Mac OS X-Computer das Programm „Servereinstellungen“.
- 2 Stellen Sie als lokaler Administrator (ladmin) eine Verbindung zu Ihrem Server her.



- 3 Klicken Sie auf „Benutzer“.

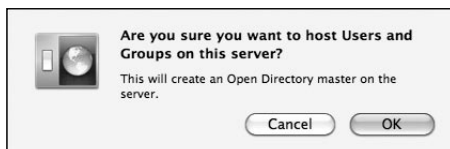
- 4 Weil die Servereinstellungen dazu gedacht sind, Netzwerkaccounts und nicht lokale Accounts zu verwalten, wird eine Meldung angezeigt, die angibt, dass dieser Server nicht zur Verwaltung von Benutzern und Gruppen konfiguriert ist.

Klicken Sie *nicht* auf „Konfigurieren“, wenn Sie Ihren Server mit Server-Admin als Open Directory-Master konfigurieren möchten. Server-Admin bietet Ihnen mehr Flexibilität. Sie können beispielsweise das Kennwort für den Benutzeraccount des Verzeichnisadministrators wählen.

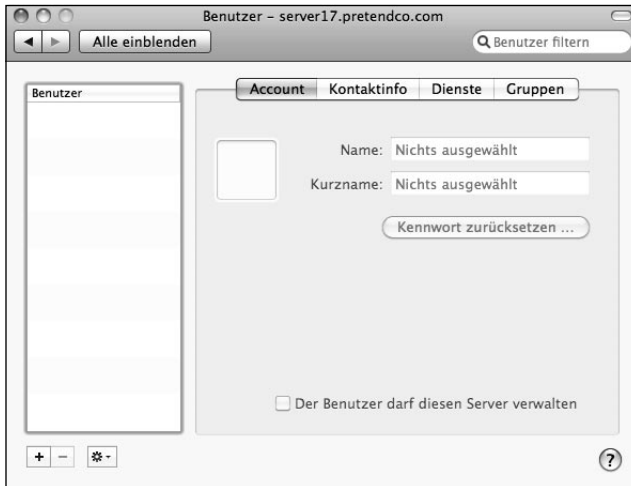
Wenn Sie wirklich die Servereinstellungen zum Konfigurieren eines Open Directory-Masters verwenden möchten, klicken Sie auf „Konfigurieren“. Sie können dann die Übung zum Konfigurieren eines Open Directory-Masters mit Server-Admin überspringen.



- 5 Klicken Sie auf „OK“, wenn Sie dazu aufgefordert werden, um zu bestätigen, dass Sie diesen Server wirklich dazu verwenden möchten, Benutzer und Gruppen bereitzustellen.



Ihr Server dient nun als Open Directory-Master. In den Servereinstellungen wird die leere Liste der Benutzeraccounts im Netzwerk angezeigt.

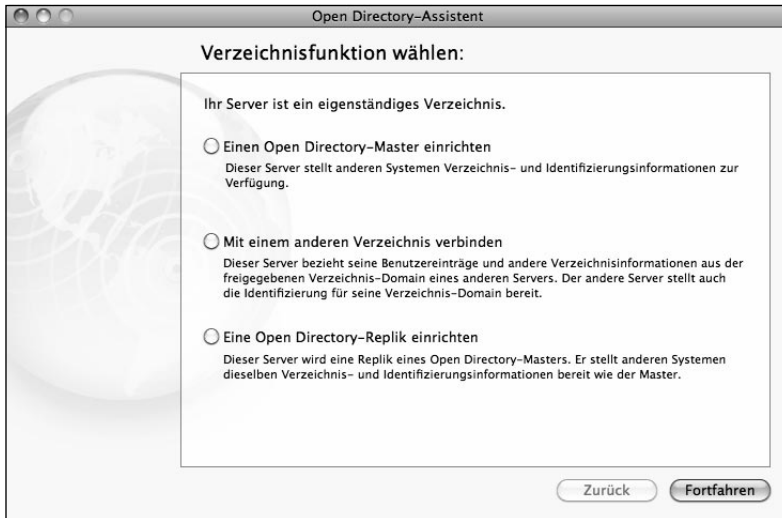


6 Beenden Sie die Servereinstellungen.

Konfigurieren von Open Directory-Diensten mit Server-Admin

Wenn Sie mehr Optionen benötigen, als der Serverassistent und die Servereinstellungen bieten, sollten Sie Server-Admin verwenden, um Mac OS X Server zur Bereitstellung von Open Directory-Diensten zu konfigurieren. Mit Server-Admin können die Open Directory-Dienste von Mac OS X Server auf folgende vier Arten konfiguriert werden:

- ▶ Als eigenständiger Server: Der Server stellt anderen Computern keine Verzeichnisinformationen zur Verfügung und erhält keine Verzeichnisinformationen von einem vorhandenen System. 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.



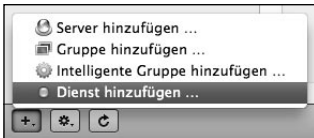
Berücksichtigen Sie bei der Planung der Verzeichnisdienste für Ihr Netzwerk, in welchem Umfang Sie Benutzer- und Ressourceninformationen für mehrere Mac OS X-Computer freigeben müssen. Ist dieser Umfang gering, ist nur wenig Verzeichnisplanung erforderlich. Auf alle Informationen kann über ein lokales Serververzeichnis zugegriffen werden. Wenn Sie jedoch Daten auf mehreren Computern gemeinsam nutzen möchten, müssen Sie mindestens einen Open Directory-Server (einen Open Directory-Master) konfigurieren. Wenn Sie hohe Verfügbarkeit von Verzeichnisdiensten gewährleisten möchten, sollten Sie mindestens einen zusätzlichen Mac OS X Server-Computer als Open Directory-Replik konfigurieren.

Konfigurieren eines Open Directory-Masters mit Server-Admin

Statt Mac OS X Server an einen anderen Server zu binden, um Verzeichnisdienste in Anspruch nehmen zu können, können Sie Ihren Server so konfigurieren, dass er ein gemeinsam genutztes LDAP-Verzeichnis, einen Kennwortserver und ein Kerberos Key Distribution Center (KDC) betreibt und so anderen Systemen Verzeichnisinformationen und Authentifizierungsdienste zur Verfügung stellt. Führen Sie die folgenden Schritte mit Server-Admin aus, um Ihren Server als Open Directory-Master zu konfigurieren. Wenn Sie bereits einen Open Directory-Master mit dem Serverassistenten oder mit den Servereinstellungen konfiguriert haben, lesen Sie einfach diese Schritte durch.

Damit Server-Admin bei der Konfiguration des Open Directory-Masters durchgängig Ihren DNS-Namen statt Ihrer IP-Adresse anzeigen kann, verwenden Sie in Server-Admin den DNS-Namen und nicht die IP-Adresse.

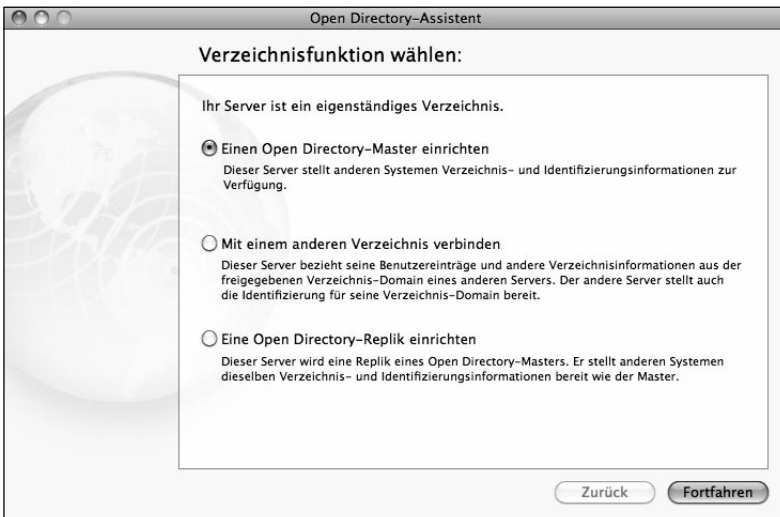
- 1 Öffnen Sie auf Ihrem Mac OS X-Computer das Programm „Server-Admin“ und stellen Sie als „ladmin“ eine Verbindung zu Ihrem Server (server18.pretendco.com) her (Kennwort: ladmin).
- 2 Wenn „Open Directory“ in der Liste der Dienste nicht angezeigt wird, klicken Sie auf die Taste „Hinzufügen“ (+) und wählen Sie „Dienst hinzufügen“ aus dem Einblendmenü aus.



- 3 Wählen Sie in der Liste der verfügbaren Dienste das Feld „Open Directory“ aus und klicken Sie auf „Sichern“.
- 4 Wählen Sie den Open Directory-Dienst aus und klicken Sie auf „Einstellungen“.



- 5 Klicken Sie auf „Ändern“, um den Open Directory-Assistenten zu öffnen.



- 6 Wählen Sie „Einen Open Directory-Master einrichten“ und klicken Sie auf „Fortfahren“.
- 7 Beim Einrichten des neuen Verzeichnisadministratoraccounts haben Sie die Möglichkeit, den Namen, den Kurznamen und die Benutzer-ID zu ändern. Behalten Sie für diese Übung die Standardwerte bei.

Verwenden Sie für diese Übung das Kennwort `diradmin` und klicken Sie auf „Fortfahren“.

In einer Produktionsumgebung sollten Sie selbstverständlich ein sicheres Kennwort verwenden.

Open Directory-Assistent

Verzeichnisadministrator

Bitte geben Sie die Accountinformationen für den neuen Verzeichnisadministrator ein. Dieser Benutzeraccount erhält Administratorrechte für die Domain des Masters.

Name:

Kurzname: Benutzer-ID:

Kennwort:

Wiederholung:

- 8 Überprüfen Sie, ob die automatisch generierten Werte für die Felder „Kerberos-Realm“ und „LDAP-Suchbeginn“ mit den Werten in der folgenden Abbildung übereinstimmen.

Diese Werte sind etwas willkürlich, basieren jedoch auf dem Hostnamen Ihres Servers. Sie sollten die vorgeschlagenen Standardwerte beibehalten, sofern Sie keinen zwingenden Grund haben, sie zu ändern. Nehmen Sie für diese Übung keine Änderungen vor.

Wenn eines der Felder auf „local“ verweist, beenden Sie den Open Directory-Assistenten und überprüfen Sie Ihre DNS-Einträge erneut.

Der Open Directory-Assistent generiert anhand des DNS-Namens Ihres Servers ein Kerberos-Realm und einen LDAP-Suchbeginn. Sie dürfen diese Werte zwar ändern, die Beibehaltung der Standardwerte trägt jedoch zur Vereinheitlichung bei.

Klicken Sie auf „Fortfahren“, um diese Werte zu akzeptieren.



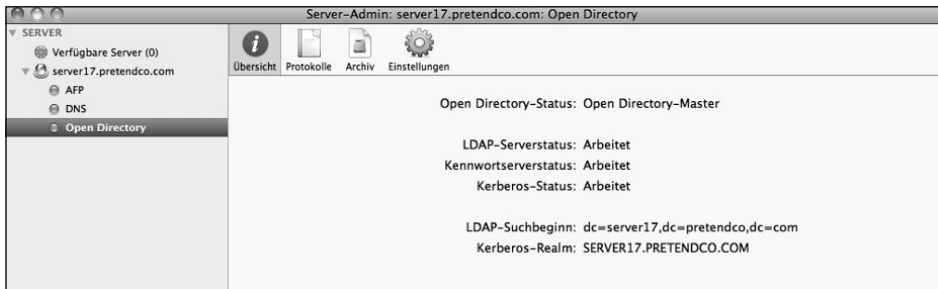
- 9 Klicken Sie im Fenster „Einstellungen bestätigen“ auf „Fortfahren“.



- 10 Klicken Sie auf „Fertig“, um den Open Directory-Assistenten zu beenden.



- 11 Klicken Sie in der Symbolleiste auf „Übersicht“. Es sollte angezeigt werden, dass die drei Dienste LDAP-Server, Kennwortserver und Kerberos aktiv sind.



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-Domain auf Ihrem Server hinzugefügt haben. Sie verlieren sonst u. U. 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 ist „admin“. Sie haben eine zweite gemeinsam genutzte LDAP-Datenbank erstellt. Als Administrator dieser Datenbank gilt (standardmäßig) „diradmin“. Die Datenbanken sind eigenständig und erfordern unterschiedliche Anmeldedaten für die Verwaltung. Ferner haben Sie eine Kennwortserver-Datenbank erstellt, in der LDAP-Benutzerkennwörter gespeichert werden, sowie ein Kerberos-KDC (Key Distribution Center). Zu diesen Punkten erfahren Sie in einem anderen Abschnitt mehr.

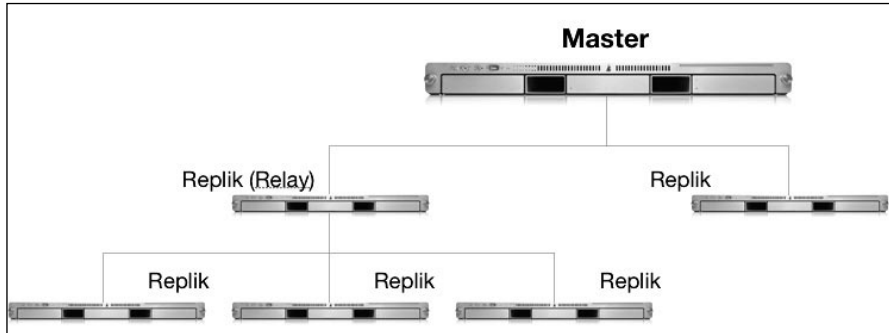
Konfigurieren einer Open Directory-Replik

Wenn Sie bereits einen Open Directory-Master-Server konfiguriert haben, können Sie mindestens einen weiteren Mac OS X Server-Computer als *Verzeichnisreplik* konfigurieren, die dieselben Verzeichnis- und Authentifizierungsdaten bereitstellt wie der Master. Der Replikserver enthält eine Kopie des LDAP-Verzeichnisses, der Kennwortserver-Authentifizierungsdatenbank und des Kerberos-KDC des Masters. Wenn Authentifizierungsdaten vom Master auf eine Replik übertragen werden, werden diese Daten beim Kopiervorgang verschlüsselt.

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

Wie bei Mac OS X Server 10.5 können Sie auch bei Mac OS X Server 10.6 verschachtelte Repliken erstellen, d. h. 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-Domain. 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.



Konfigurieren Ihres Servers für die Bereitstellung einer Replik eines Open Directory-Masters

In diesem Abschnitt wird beschrieben, wie Sie eine Replik Ihres Open Directory-Masters unter Mac OS X Server bereitstellen. Wenn Sie nur mit einem Mac OS X Server-Computer und einem Mac OS X-Client arbeiten, können Sie diese Übung lesen, aber die Schritte nicht ausführen. Bei dieser Übung wird vorausgesetzt, dass Sie einen weiteren Mac OS X Server-Computer mit der Adresse 10.1.18.1 haben, den Sie als Replik von 10.1.17.1 konfigurieren möchten, und dass DNS-Einträge zur Vorwärts- und Rückwärtsauflösung für beide Server verfügbar sind, die Ihrem Mac OS X-Computer und beiden Servern zur Verfügung stehen.

HINWEIS ► Sie können einen zweiten Server zur Verwendung als Open Directory-Replik konfigurieren. Gehen Sie hierfür so wie in Lektion 1 „Installieren und Konfigurieren von Mac OS X Server“ beschrieben vor, verwenden Sie jedoch 10.1.18.1 als IP-Adresse und „Server 18“ als Computername.

Informationen zum Konfigurieren von „Server 17“ als Host für DNS-Einträge für den Hostnamen „server18.pretendco.com“ und die IP-Adresse 10.1.18.1 finden Sie im Abschnitt „Definieren von DNS-Einträgen“ am Ende dieser Lektion.

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 Clientcomputer das Programm „Server-Admin“, stellen Sie als „admin“ eine Verbindung zu Ihrem Server (server18.pretendco.com) her, wählen Sie Ihren Server in der Liste „Quelle“ aus und wählen Sie anschließend „Server“ > „Auf Serverbildschirm zugreifen“.

- 2 Authentifizieren Sie sich als „ladmin“, um den Bildschirm Ihres Servers freizugeben.
- 3 Melden Sie sich im Anmeldefenster des Servers als „ladmin“ an (Kennwort: ladmin).
- 4 Öffnen Sie das Programm „Terminal“ (in „/Programme/Dienstprogramme“).
- 5 Geben Sie den Befehl `sudo changeip -checkhostname` ein und drücken Sie den Zeilenschalter.
- 6 Geben Sie Ihr Kennwort (ladmin) ein, falls erforderlich.
- 7 Vergewissern Sie sich, dass das Ergebnis des Befehls `changeip` „The names match. There is nothing to change.“ lautet. Falls Sie ein anderes Ergebnis erhalten, lesen Sie den Abschnitt „Definieren von DNS-Einträgen“ am Ende dieser Lektion.
- 8 Beenden Sie auf Ihrem Mac OS X-Server das Programm „Terminal“.
- 9 Beenden Sie auf Ihrem Mac OS X-Computer die Bildschirmfreigabe.

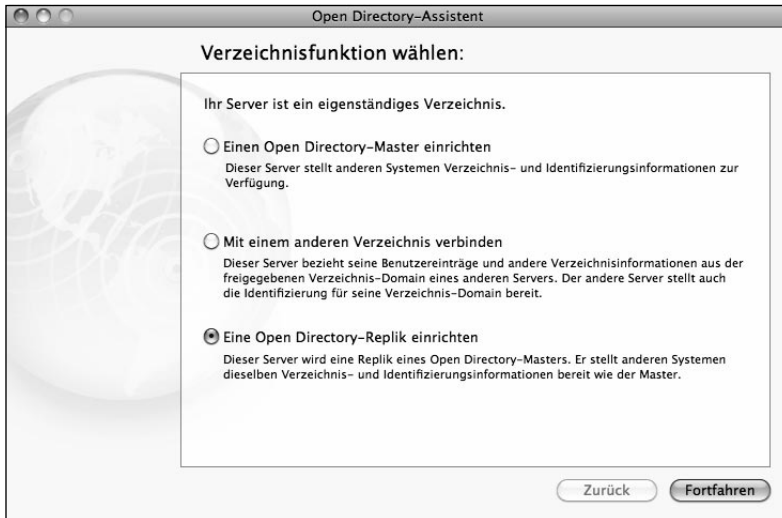
Gehen Sie wie folgt vor, um Ihren Mac OS X Server-Computer in eine Open Directory-Replik umzuwandeln:

- 1 Öffnen Sie auf Ihrem Mac OS X-Computer das Programm „Server-Admin“ und stellen Sie als „ladmin“ eine Verbindung zu `server18.pretendco.com` her (Kennwort: ladmin).
- 2 Fügen Sie den Open Directory-Dienst zur Liste der Dienste hinzu. Wählen Sie „Open Directory“ aus.
- 3 Klicken Sie in der Symbolleiste auf „Einstellungen“, klicken Sie auf „Allgemein“ und klicken Sie danach auf die Taste „Ändern“, um den Open Directory-Assistenten zu öffnen, so wie beim Erstellen eines Open Directory-Masters.

HINWEIS ► Sie können keine Replik erstellen, wenn in Ihrem Netzwerk kein Open Directory-Master vorhanden ist.

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

- 4 Nachdem der Open Directory-Assistent geöffnet wurde, wählen Sie „Eine Open Directory-Replik einrichten“ in der Liste aus und klicken Sie auf „Fortfahren“.



5 Konfigurieren Sie die Replik mit den folgenden Parametern: Achten Sie darauf, dass Sie den DNS-Namen (und nicht die IP-Adresse oder den Bonjour-Namen) des Open Directory-Masters verwenden.

- ▶ IP-Adresse oder vollständig qualifizierter Domain-Name des Open Directory-Masters: `server17.pretendco.com`
- ▶ root-Kennwort des Open Directory-Masters: `ladmin`
- ▶ Kurzname des Domain-Administrators: `diradmin`
- ▶ Kennwort des Domain-Administrators: `diradmin`

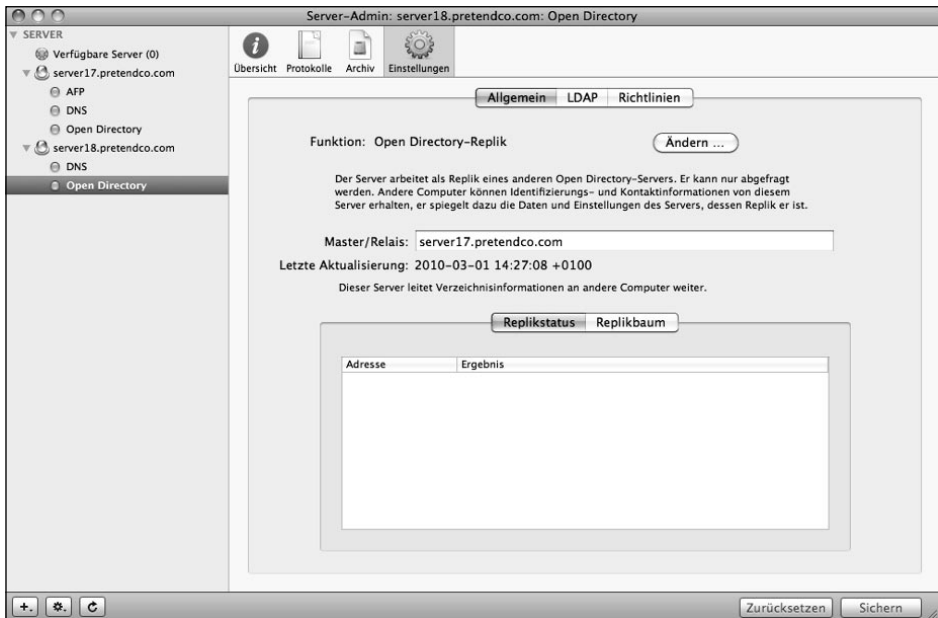
HINWEIS ▶ Sie müssen das root-Kennwort des Open Directory-Masters kennen, da die anfänglichen Informationen über diesen Account übertragen werden.



- 6 Klicken Sie auf „Fortfahren“.
- 7 Klicken Sie im Fenster „Einstellungen bestätigen“ auf „Fortfahren“.
- 8 Klicken Sie im Fenster „Zusammenfassung“ auf „Fertig“.



- 9 Beachten Sie, dass der Bereich „Replikstatus“ in Server-Admin leer ist. Dies deshalb, weil darin Server, die Repliken dieses Servers sind, aufgelistet werden.



- 10 Klicken Sie auf „Replikbaum“. Beachten Sie, dass darin berücksichtigt wird, dass „server17.pretendco.com“ ein Open Directory-Master und „server18.pretendco.com“ eine Open Directory-Replik von „server17.pretendco.com“ ist.



- 11 Klicken Sie in Server-Admin auf „Übersicht“.

Beachten Sie, dass Ihr Server jetzt eine Open Directory-Replik ist und alle drei Dienste bereitstellt: LDAP-Server, Kennwortserver und Kerberos.



HINWEIS ► Wenn Sie das freigegebene Verzeichnis mit dem Arbeitsgruppenmanager bearbeiten, wird es als „/LDAPv3/127.0.0.1“ angezeigt, unabhängig von der Adresse des Servers, zu dem Sie mit dem Arbeitsgruppenmanager eine Verbindung herstellen.

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

Nachdem eine einzelne Replik erstellt wurde, können andere Mac OS X 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 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.

Verbinden von Mac OS X Server mit einem vorhandenen Verzeichnisdienst

Wenn Sie beabsichtigen, mehrere Server einzurichten, wäre es äußerst unpraktisch, auf allen Servern dieselben Benutzeraccounts anzulegen. Stattdessen können Sie Ihren Mac OS X-Server an ein weiteres 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 Mac OS X Server-Computer mit einem im lokalen Verzeichnis Ihres Servers definierten Account oder mit einem Account authentifizieren, der in einem beliebigen Verzeichnisknoten, an den Ihr Server gebunden ist, definiert ist. Bei dem anderen Verzeichnisknoten kann es sich um einen Open Directory- oder einen Active Directory-Verzeichnisdienst handeln.

Sie können Ihren Mac OS X Server-Computer mithilfe der Systemeinstellungen oder des Programms „Verzeichnisdienste“ an einen weiteren Verzeichnisdienst binden. Möchten Sie die Systemeinstellungen verwenden, müssen Sie sich im Anmeldefenster des Servers anmelden können, während Sie das Programm „Verzeichnisdienste“ entfernt von einem anderen Mac OS X- oder Mac OS X Server-Computer aus verwenden können.

Definieren von Bindungen mit den Systemeinstellungen

Sie können Ihren Server wie jeden beliebigen Mac OS X-Computer so konfigurieren, dass er Verzeichnisdienste von einem vorhandenen Open Directory-Server in Anspruch nimmt: Verwenden Sie dazu die Systemeinstellungen. In dieser Übung wird Folgendes vorausgesetzt:

- ▶ Sie verfügen aus der vorherigen Übung über eine mit der Adresse 10.1.18.1 konfigurierte Replik.
- ▶ Sie verfügen über einen dritten Server, den Sie wie in Lektion 1 „Installieren und Konfigurieren von Mac OS X Server“ beschrieben konfiguriert haben, außer dass Sie 10.1.19.1 als IP-Adresse und „Server 19“ als Computernamen verwendet haben.
- ▶ Sie konfigurieren einen eigenständigen Mac OS X-Server mit der Adresse 10.1.19.1, der an die Replik mit der Adresse 10.1.18.1 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.

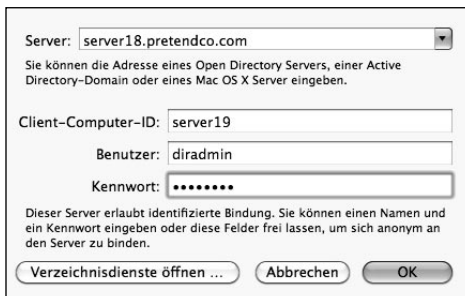
- 1 Öffnen Sie auf Ihrem Mac OS X-Computer das Programm „Server-Admin“ und stellen Sie eine Verbindung zu dem Server her, an den die Bindung erfolgen soll (verwenden Sie dazu den Benutzernamen „ladmin“ und das Kennwort ladmin).
- 2 Wählen Sie in der Serverliste den Server aus, an den eine Bindung erfolgen soll.
- 3 Wählen Sie „Server“ > „Auf Serverbildschirm zugreifen“.
- 4 Authentifizieren Sie sich für den Zugriff auf den Serverbildschirm als „ladmin“.
- 5 Öffnen Sie auf Ihrem Mac OS X-Server die Systemeinstellung „Benutzer“.
- 6 Klicken Sie auf „Anmeldeoptionen“.
- 7 Klicken Sie auf „Verbinden“.



- 8 Geben Sie den DNS-Namen oder die IP-Adresse eines Open Directory-Servers (server18.pretendco.com) ein und klicken Sie auf „OK“.



- 9 Authentifizieren Sie sich bei Aufforderung als lokaler Administrator.
- 10 Geben Sie die Anmeldeinformationen eines Netzwerkbenutzers ein, um einen Computeraccount zu erstellen und eine Verbindung zum Kerberos-Realm herzustellen. Der derzeit einzige Netzwerkbenutzer ist „Verzeichnisadministrator“, geben Sie daher diradmin als Benutzernamen und diradmin als Kennwort ein.



- 11 Beachten Sie, dass das Feld „Netzwerk-Account-Server“ jetzt den DNS-Namen des Open Directory-Servers enthält, zu dem Sie gerade eine Bindung hergestellt haben.



- 12 Schließen Sie die Systemeinstellung „Benutzer“.
- 13 Melden Sie sich als „ladmin“ bei „Server 19“ ab.
- 14 Beenden Sie auf Ihrem Mac OS X-Computer die Bildschirmfreigabe.

Überprüfen der Bindung mit dem Programm „Verzeichnisdienste“

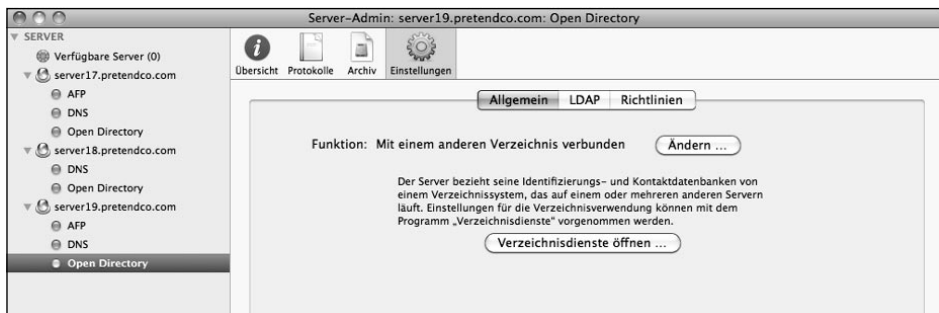
Sie können weiterhin das Programm „Verzeichnisdienste“ anstelle der Systemeinstellungen verwenden. Die Systemeinstellung „Benutzer“ bietet sogar einen Kurzbefehl für das Programm „Verzeichnisdienste“, das sich jetzt in „/System/Library/CoreServices“ befindet. Das Programm „Verzeichnisdienste“ bietet etwas mehr Kontrolle als die Taste „Verbinden“ der Systemeinstellung „Benutzer“. Es ermöglicht Ihnen, einen entfernten Computer von Mac OS X oder Mac OS X Server aus zu steuern, sodass die Bildschirmfreigabe nicht zwingend erforderlich ist.

In der folgenden Übung öffnen Sie das Programm „Verzeichnisdienste“ unter Mac OS X, stellen jedoch eine Verbindung zu Mac OS X Server her und überprüfen die Einstellungen für die Verzeichnisnutzung.

Für diese Übung wird vorausgesetzt, dass Sie über eine Replik mit der Adresse 10.1.18.1 verfügen, dass Sie einen eigenständigen Mac OS X Server-Computer mit der Adresse 10.1.19.1 konfigurieren, der an die Replik mit der Adresse 10.1.18.1 gebunden wird, und dass Sie für diese Server über DNS-Einträge zur Vorwärts- und Rückwärtsauflösung verfügen. Wenn Sie nur mit einem Mac OS X Server-Computer und einem Mac OS X-Clientcomputer arbeiten, können Sie diese Übung lesen, aber nicht durchführen.

- 1 Öffnen Sie auf Ihrem Mac OS X-Computer das Programm „Server-Admin“ und stellen Sie als „ladmin“ eine Verbindung zu server18.pretendco.com her (Kennwort: ladmin).
- 2 Wählen Sie in der Serverliste „server19.pretendco.com“ aus und klicken Sie auf das Dreiecksymbol, um die Liste der bereitgestellten Dienste anzuzeigen.
- 3 Wenn „Open Directory“ in der Liste der Dienste nicht angezeigt wird, klicken Sie auf die Taste „Hinzufügen“ (+) und wählen Sie „Dienst hinzufügen“ aus dem Einblendmenü aus. Wählen Sie in der Liste der verfügbaren Dienste das Feld „Open Directory“ aus und klicken Sie auf „Sichern“.
- 4 Wählen Sie den Dienst „Open Directory“ für server19.pretendco.com aus.
- 5 Klicken Sie auf „Einstellungen“ und dann auf „Allgemein“.

In Server-Admin wird angezeigt, dass die Funktion „Mit einem anderen Verzeichnis verbunden“ ist.



- 6 Zum Überprüfen der Bindungseinstellungen verwenden Sie das Programm „Verzeichnisdienste“.

Klicken Sie auf „Verzeichnisdienste öffnen“.

- 7 Sie müssen das Programm „Verzeichnisdienste“ verwenden, um eine Verbindung zu Ihrem Server herzustellen und die Verzeichnisdienste zu konfigurieren, die Ihr Server verwendet.

Wählen Sie „Ablage“ > „Verbinden“.

- 8 Geben Sie die folgenden Informationen ein, um sich beim entfernten Server zu identifizieren:

Adresse: server19.pretendco.com

Benutzername: ladmin

Kennwort: ladmin

Identifizieren

Adresse: server19.pretendco.com

Benutzername: ladmin

Kennwort:

Abbrechen Verbinden

- 9 Klicken Sie in der Symbolleiste auf „Dienste“.
- 10 Wählen Sie „LDAPv3“ aus.

Verzeichniszugriff: server19.pretendco.com

Dienste Suchpfad

Wählen Sie einen Dienst und klicken Sie auf das Stiftsymbol, um die Einstellungen zu bearbeiten.

Aktiv	Name	Version
<input type="checkbox"/>	Active Directory	6.0
<input checked="" type="checkbox"/>	LDAPv3	6.0
<input checked="" type="checkbox"/>	Local	6.0
<input checked="" type="checkbox"/>	Lokale BSD-Konfigurationsdateien und NIS	6.0

?

Anwenden

- 11 Klicken Sie auf die Taste „Bearbeiten“ (Stiftsymbol), um die Einstellungen zu prüfen.
- 12 Beachten Sie, dass der Konfigurationsname auf dem DNS-Namen des Servers basiert. Der DNS-Name des Servers, zu dem Sie eine Bindung hergestellt haben, wird in der mittleren Spalte aufgeführt.



- 13 Klicken Sie auf „OK“, um die LDAP-Serverliste zu schließen.

- 14 Klicken Sie in der Symbolleiste auf „Suchpfad“.



- 15 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.
- 16 Schließen Sie das Programm „Verzeichnisdienste“. Sichern Sie keine Änderungen, falls Sie dazu aufgefordert werden, da Sie das Programm „Verzeichnisdienste“ nur zum Prüfen der Einstellungen verwenden.
- 17 Beenden Sie Server-Admin.

Sie haben jetzt mit dem Programm „Verzeichnisdienste“ unter Mac OS X eine Verbindung zu einem entfernten Server hergestellt und Einstellungen entfernt geprüft.

Wenn Sie die Übungen mangels zusätzlicher Server nur gelesen haben, sollten Sie die Durchführung der Übungen jetzt fortsetzen.

Verbinden von Mac OS X Server mit einem Open Directory-Dienst

Nachdem Sie einen Open Directory-Master (und vielleicht eine oder mehr Repliken) konfiguriert haben, müssen Sie auch die *Client*computer so konfigurieren, dass eine Bindung an den Verzeichnisdienst erfolgt. Geben Sie auf jedem Clientcomputer mithilfe der Systemeinstellungen einen Server an, der einen Open Directory-Dienst enthält, oder erstellen Sie mit dem Programm „Verzeichnisdienste“ eine LDAP-Konfiguration, die die Adresse und den Suchpfad für einen Open Directory-Server umfasst.

Anschließend konfigurieren Sie Ihren Mac OS X-Computer für die Verwendung von Authentifizierungsdiensten vom Mac OS X Server-Computer. Sie haben bereits ein freigegebenes Verzeichnis eingerichtet, das den Mac OS X-Computern angezeigt werden sollte, damit diese sich dort anmelden können. Alle mit dem Open Directory-Dienst verbundenen Clients können Benutzer mit den Daten im freigegebenen Verzeichnis authentifizieren.

Binden von Mac OS X an Ihren Open Directory-Dienst

Damit Ihr Mac OS X-Computer die Open Directory-Dienste Ihres Servers nutzen kann, müssen Sie ihn an einen Open Directory-Server binden. In einer Umgebung mit vielen Open Directory-Repliken können Sie Mac OS X auch an eine Replik binden, sodass der Open Directory-Master vorrangig mit den Repliken kommunizieren kann.

Sie können die Systemeinstellung „Benutzer“ oder das Programm „Verzeichnisdienste“ verwenden, wenn Sie anspruchsvollere Bindungsoptionen benötigen.

Definieren von Bindungen mit der Systemeinstellung „Benutzer“

In den folgenden Schritten verwenden Sie die Systemeinstellungen, um Ihren Mac OS X-Computer an Ihren Open Directory-Master zu binden. Mac OS X wird auf ähnliche Weise gebunden wie Mac OS X Server: mit der Systemeinstellung „Benutzer“. Weil Ihr Mac OS X-Computer keine Dienste bereitstellt, die Benutzern die Verwendung von Kerberos zur Identifizierung ermöglichen, werden Sie möglicherweise nicht zur Anmeldung aufgefordert, um eine vertrauenswürdige Bindung zu konfigurieren.

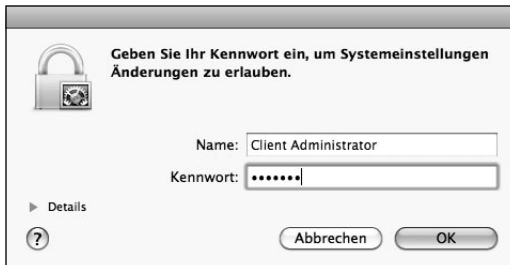
- 1 Öffnen Sie auf Ihrem Mac OS X-Computer die Systemeinstellung „Benutzer“.
- 2 Klicken Sie auf „Anmeldeoptionen“.
- 3 Klicken Sie auf „Verbinden“.



- 4 Geben Sie den FQDN Ihrer Open Directory-Replik, `server18.pretendco.com`, ein (wenn Sie nur einen Open Directory-Master haben, verwenden Sie stattdessen `server17.pretendco.com`). Klicken Sie dann auf „OK“.



- 5 Melden Sie sich nach Aufforderung als lokaler Administrator an (Benutzername „Client Administrator“ und Kennwort cadmin).



- 6 Vergewissern Sie sich, dass im Bereich „Anmeldeoptionen“ Ihr Open Directory-Server angezeigt wird.



- 7 Schließen Sie die Systemeinstellung „Benutzer“.