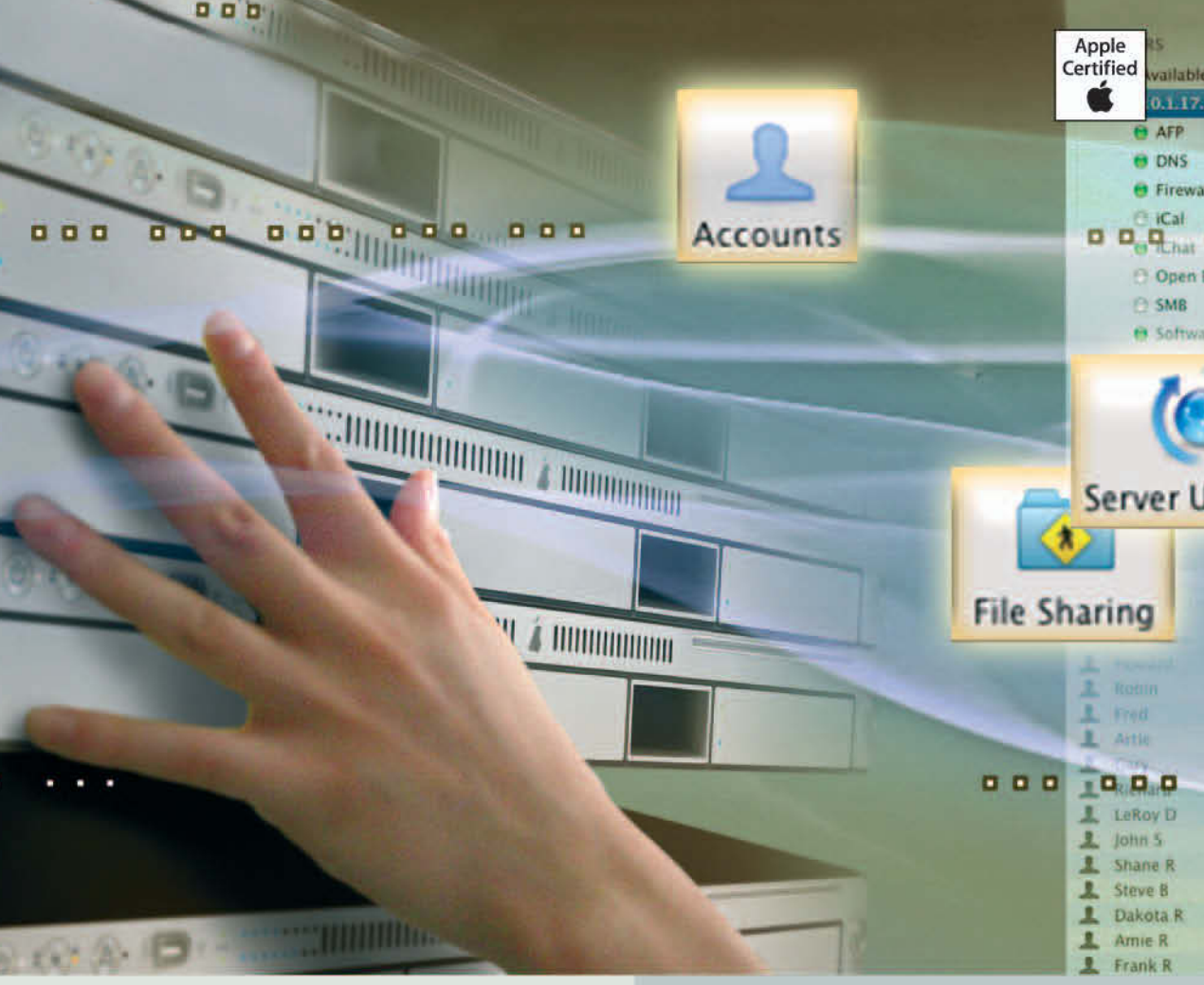


Apple Training Series

Mac OS X Server Essentials 2. Auflage

Der offizielle Leitfaden zu Einsatz und Support von Mac OS X Server v10.5

Schoun Regan mit David Pugh

ADDISON-WESLEY

Lektion **3**

Identifizieren und Autorisieren von Accounts

Bei der Identifizierung gibt ein Benutzer an, welchen Benutzeraccount er auf dem System verwenden wird. Dieser Prozess ähnelt zwar der Identitätsprüfung (Anmeldung) eines Benutzers auf einem System, sollte aber dennoch davon unterschieden werden. Diese Unterscheidung ist nützlich, da möglicherweise mehrere Benutzer denselben Benutzernamen und dasselbe Kennwort verwenden oder ein Benutzer mehrere Benutzeraccounts auf einem System besitzt. In beiden Fällen wird der gewünschte Benutzeraccount mittels Name und Kennwort identifiziert, sofern diese Daten korrekt eingegeben werden. Es gibt zwar noch weitere Methoden, sich bei einem Benutzeraccount zu identifizieren, etwa via Smart Cards oder Stimmerkennung, doch die Verwendung von Name und Kennwort ist die gängigste (und wird in dieser Lektion angenommen).

Bei der Autorisierung wird bestimmt, welche Aufgaben ein Benutzer mit einem identifizierten Benutzeraccount auf dem System erledigen kann. Bei der Autorisierung spielen Dateizugriffsrechte auf Basis von Benutzeraccounts eine wichtige Rolle. Diese werden über Mac OS X oder die Verwaltungsprogramme für den Dienstzugriff von Mac OS X Server festgelegt.

In dieser Lektion wird das Erstellen und Verwalten von Benutzer- und Gruppenaccounts auf Ihrem Server erläutert. Sie erfahren, wie Benutzer- und Gruppenaccounts konfiguriert werden und wie mit diesen Accounts der Zugriff auf Dateien und Dienste gesteuert wird. Da der Zugriff auf der Identifizierung (Anmeldung) basiert, sollten Sie unbedingt wissen, wie die Autorisierung (die Vergabe von Rechten) gehandhabt wird.

Verwalten des Serverzugriffs

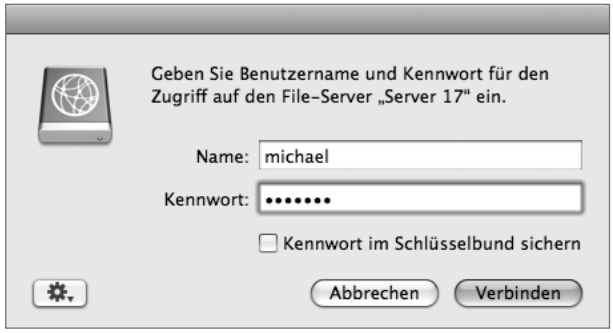
Wenn Sie einen Server für den Zugriff durch Benutzer konfigurieren, müssen Sie festlegen, welche Dienste der Server bereitstellen soll und welche Zugriffsrechte den einzelnen Benutzern zugewiesen werden sollen. Im vorliegenden Buch wurden bisher nur Netzwerkdienste beschrieben, für die keine speziellen Zugriffsrechte für den Server erforderlich sind, nachdem der Dienst aktiviert wurde. Für zahlreiche der anderen in diesem Buch genannten Dienste, etwa File-Sharing, müssen gezielt Benutzeraccounts auf dem Server erstellt werden.

Wenn Sie die Erstellung von Benutzeraccounts in Betracht ziehen, sollten Sie festlegen, wie Sie Ihre Benutzer am besten konfigurieren, wie Sie sie in Gruppen zusammenfassen, die den Anforderungen Ihrer Organisation entsprechen und wie Sie diese Informationen auch langfristig verwalten. Wie bei jedem Dienst bzw. jeder Aufgabe innerhalb der IT (Information Technology) empfiehlt es sich, die Anforderungen sorgfältig zu durchdenken und zu planen, bevor mit der Implementierung einer Lösung begonnen wird.

Erstellen und Verwalten von Serveraccounts für Benutzer und Administratoren

In den meisten Fällen erfolgt die Identifizierung unter Mac OS X und Mac OS X Server mithilfe des Anmeldefensters. Wenn Sie beispielsweise einen Mac OS X Computer starten, müssen Sie möglicherweise einen Benutzernamen und ein Kennwort in das erste Anmeldefenster eingeben, damit Sie das System überhaupt verwenden können. (Mac OS X ist standardmäßig so eingestellt, dass die Anmeldung automatisch über den ersten auf dem System konfigurierten Account erfolgt, ohne ein Kennnwort anzufordern. Sofern Sie diese Standardeinstellung nicht in der Systemeinstellung BENUTZER ändern, wird das erste Anmeldefenster beim Starten des Systems nicht angezeigt.) In diesem Anmeldebeispiel wird zwar nur Mac OS X genannt, es gilt jedoch auch, wenn Sie sich an einem Benutzeraccount im Netzwerk anmelden, der sich auf einem Mac OS X Server Computer befindet.

Ein anderes Beispiel ist die Verbindung mit einem Netzwerkserver über AFP oder SMB. Benutzer müssen sich anmelden, bevor sie auf diese Dienste zugreifen. Dies gilt auch bei einer Anmeldung als Gastbenutzer. Werden Anmeldename und Kennwort nicht korrekt eingegeben, wird der Hinweis ANMELDUNG FEHLGESCHLAGEN angezeigt, was auf einen fehlgeschlagenen Identifizierungsversuch hinweist.



Damit ein Server anhand der Programme *Server-Admin* oder *Arbeitsgruppenmanager* verwaltet werden kann, muss sich der Administrator mithilfe dieser Programme identifizieren. Dies ist unabhängig davon erforderlich, ob der Server lokal oder per Fernzugriff verwaltet wird.

Verwenden des Programms »Servereinstellungen« für Benutzeraccounts

Wenn Sie Mac OS X Server als Standardserver oder Arbeitsgruppenserver konfiguriert haben, können Sie Benutzeraccounts mit dem Programm *Servereinstellungen* einrichten. In diesem Programm werden Benutzer und Gruppen mithilfe einer Oberfläche verwaltet, die stark den Systemeinstellungen unter Mac OS X ähnelt.

Das Programm SERVEREINSTELLUNGEN bietet Ihnen die grundlegenden Optionen für die Accountverwaltung, u. a. Accountdetails, Kontaktinformationen, Dienste, zu deren Verwendung der Benutzer berechtigt ist, und Gruppen, denen er angehört. Wie in Lektion 1 erwähnt, können Sie das Programm SERVEREINSTELLUNGEN nicht verwenden, wenn Sie Ihren Server im erweiterten Modus konfiguriert haben. Da die benutzerbezogenen Optionen in diesem Programm meist selbsterklärend sind, konzentrieren wir uns in dieser Lektion auf die Methoden für die Verwaltung einer erweiterten Konfiguration.

Verwenden des Arbeitsgruppenmanagers für die Konfiguration von Benutzeraccounts

Das Programm ARBEITSGRUPPENMANAGER spielt bei der Erstellung und Konfiguration von Benutzeraccounts unter Mac OS X Server eine wichtige Rolle. Da ein Benutzer bestimmte Rechte auf einem Mac OS X Server Computer erhält, müssen Sie einen Benutzeraccount für diesen Benutzer einrichten. Das Prinzip der Benutzeraccounts unter Mac OS X Server ist mit dem unter Mac OS X identisch, allerdings bieten die mit dem Arbeitsgruppenmanager erstellte Accounts komplexere Optionen und Einstellungen. Zudem haben Sie damit die Möglichkeit, im Netzwerk verfügbare Accounts zu erstellen, bei denen sich Benutzer per Fernzugriff anmelden können.

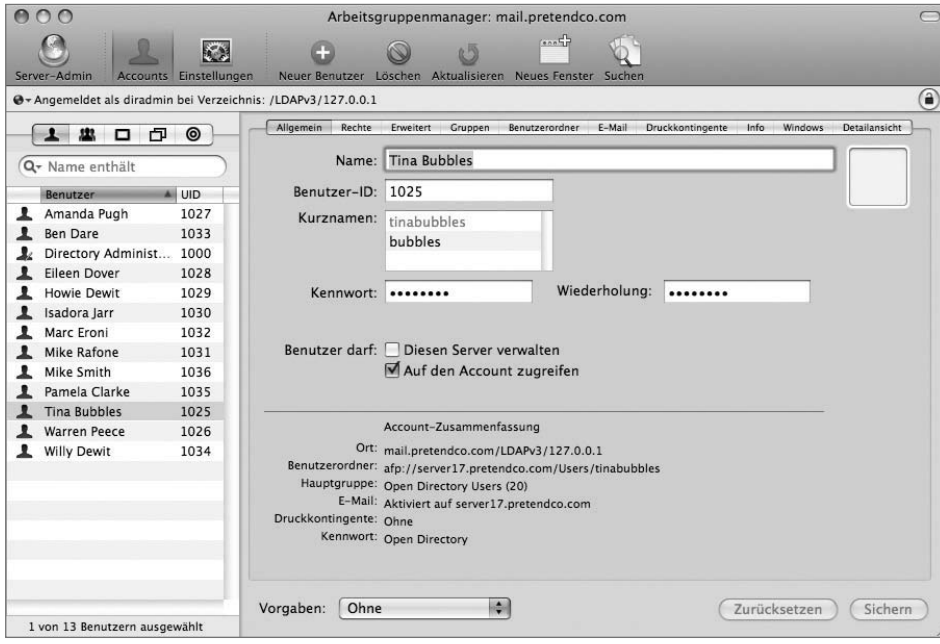
Unter Mac OS X Server können Sie mit lokalen Benutzeraccounts und Netzwerkaccounts arbeiten. Mit standardmäßigen Benutzeraccounts unter Mac OS X kann ein Benutzer auf Dateien und Programme zugreifen, die sich lokal auf diesem Computer befinden. Benutzeraccounts unter Mac OS X Server ermöglichen es Benutzern, die sich lokal anmelden, ebenfalls auf Dateien oder Dienste (wie Mail- und Druckdienste) zuzugreifen, die vom Server bereitgestellt werden. Gleichzeitig bieten sie jedoch auch entfernten Benutzern Zugriff auf Servervolumes und zugehörige Dateien, wenn die Benutzer in einem im Netzwerk verfügbaren Verzeichnisdienst erstellt werden. Lokale Benutzer können per Fernzugriff eine Verbindung zu Servern herstellen, sich jedoch nur lokal anmelden.

Nachfolgend finden Sie einige Beispiele von Benutzeraccount-Einstellungen unter Mac OS X Server:

- Name
- UNIX-Benutzer-ID (UID)
- Kurznamen
- Benutzerkennwort (Shadow, Crypt, Open Directory)
- Speicherort des Benutzerordners

- Adressinformationen des Benutzers
- Mail-Einstellungen
- Druckeinstellungen

Wenn Sie den Arbeitsgruppenmanager mit Mac OS X Server verwenden, können Sie einem einzelnen Benutzeraccount mehrere Kurznamen zuweisen. Der erste Kurzname darf nicht länger als 31 Zeichen sein, weitere Kurznamen können aber bis zu 255 Zeichen enthalten. Damit bietet sich einem Benutzer z. B. die Möglichkeit, einen anderen E-Mail-Namen zu verwenden, ohne den zuvor eingetragenen Kurznamen ändern zu müssen. Der Kurzname wird bei der Erstellung des Benutzerverzeichnisses des jeweiligen Benutzers verwendet.



Die Benutzer-ID im Bereich ALLGEMEIN ist ein numerischer Wert, mit dem das System die Benutzer voneinander unterscheidet. Obwohl Benutzer mittels eines Benutzernamens Zugriff auf das System erhalten, wird jedem Namen eine Benutzer-ID zugeordnet, die für den Computer in erster Linie maßgebend ist.

Beachten Sie, dass bei einer Anmeldung zweier Benutzer, die mit verschiedenen Namen und Kennwörtern, aber mit derselben Benutzer-ID auf Dokumente und Ordner zugreifen, das System diese Benutzer als ein und dieselbe Person ansieht. Wenn Sie versuchen, im Arbeitsgruppenmanager zwei Benutzer mit derselben ID anzulegen, müssen Sie bestätigen, dass Sie diesen Schritt wirklich ausführen möchten.

Neben der Verwaltung von Benutzeraccounts kann der Arbeitsgruppenmanager noch für weitere Zwecke eingesetzt werden. Er wird auch für die Verwaltung von Gruppenaccounts, womit mehrere Benutzer zusammengefasst werden können, genutzt. Außerdem dient er der Verwaltung von Computeraccounts, mit denen die für einen bestimmten Computer verfügbaren Funktionen gesteuert werden, sowie von Computergruppen, bei denen es sich einfach um eine Sammlung von Computeraccounts handelt. Der Arbeitsgruppenmanager wird auch zur Steuerung bestimmter Standardeinstellungen für Benutzer und Computer verwendet. Zu diesem Thema finden Sie in Lektion 10 »Verwalten von Accounts« nähere Informationen.

Verwenden des Arbeitsgruppenmanagers für die Konfiguration von Administratoraccounts

Ein Administratoraccount ist ein spezieller Benutzeraccount unter Mac OS X Server, mit dem ein Server verwaltet werden kann. Ein Benutzer mit einem Administratoraccount kann Benutzeraccounts erstellen, bearbeiten und löschen. Zudem hat er die Möglichkeit, die Einstellungen verschiedener aktiver Dienste auf dem Mac OS X Server Computer zu ändern, auf dem der Administratoraccount eingerichtet ist. Der Administrator verwendet das Programm *Server-Admin*, um die meisten Diensteinstellungen zu konfigurieren, und das Programm *Arbeitsgruppenmanager*, um Benutzer, Gruppen und Accounteinstellungen zu bearbeiten.

Markieren Sie das Feld Benutzer darf diesen Server verwalten (vgl. vorherige Abbildung) im Bereich Allgemein des Arbeitsgruppenmanagers, um einen Benutzer- in einen Administratoraccount umzuwandeln.

Ist der Server als Open Directory-Master konfiguriert, wird eine zweite Administratoroption angeboten. Diese befindet sich im Bereich Rechte und heißt Verwaltungsrechte. Bei Auswahl der Option Benutzer darf diesen Server verwalten erhält der Benutzer die Möglichkeit, Zugriffsrechte auf dem Server zu ändern und den Server mit Server-Admin zu verwalten. Die Option Verwaltungsrechte gilt dagegen nur für Verzeichnisdaten darunter die Benutzer- und Gruppenverwaltung innerhalb von Open Directory. Sie könnten also einen Administrator erstellen, der ein Benutzerverzeichnis im Dateisystem hinzufügen darf, aber keinen Benutzeraccount im Verzeichnis anlegen kann.

Umgekehrt gilt das allerdings nicht. Ist ein Server als Open Directory-Server konfiguriert, muss ein Benutzer sowohl als Serveradministrator definiert sein als auch Zugriffsrechte für den Arbeitsgruppenmanager besitzen, um mit dem Arbeitsgruppenmanager Änderungen vorzunehmen und in der lokalen Verzeichnis-Domain arbeiten zu können. Mac OS X Server 10.5 bietet eine neue Funktion zum Erstellen eines Administrators mit eingeschränkten Rechten. Damit erhalten Sie die Möglichkeit, gezielt einen Administrator zum Ändern bestimmter Benutzer oder Gruppenmitglieder zu berechtigen. Ist der Open Directory-Server als eigenständiger Server konfiguriert, sind diese Optionen nicht verfügbar. Diese Server überprüfen lediglich, ob jemand Administratorrechte besitzt, bieten aber keine Möglichkeit, Accounts, wie bei einem Open Directory-Server, zu verwalten.

HINWEIS ► Open Directory und die Verwaltung von Verzeichnis-Domains wird in Lektion 4 »Verwenden von Open Directory« behandelt.

Konfigurieren lokaler Benutzeraccounts

Mac OS X Server erstellt eine Liste lokaler Accounts, um den Zugriff auf Ressourcen wie Dateien (bei Bereitstellung eines Dateiservers) zu verwalten. Mit dem Arbeitsgruppenmanager fügen Sie zwei lokale Demobenutzer zu Ihrem Servercomputer hinzu und importieren dann eine Datei mit weiteren Benutzern.

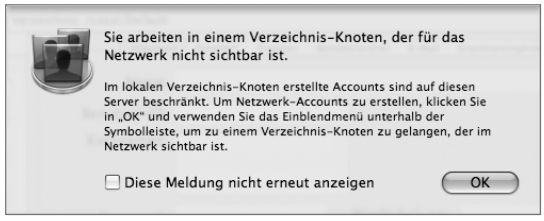
> **HINWEIS ►** In dieser Lektion verwenden Sie Ihren Mac OS X Computer für die Konfiguration des Mac OS X Server. Daran können Sie erkennen, dass Sie die Serverkonfiguration mit allen Mac OS X Computern ausführen können, die Netzwerkzugriff auf den Server besitzen. Außerdem melden Sie sich im Arbeitsgruppenmanager mit Ihrem lokalen Administratoraccount an.

Hinzufügen von Benutzern

Befolgen Sie diese Schritte, um zwei Benutzer zu Ihrem Mac OS X Server hinzuzufügen:

1 Öffnen Sie auf Ihrem Mac OS X Client-Computer den Arbeitsgruppenmanager und stellen Sie als lokaler Administrator eine Verbindung zum Mac OS X Server her.

Da der lokale Verzeichnisknoten nur für die Identifizierung lokaler Accounts verwendet werden kann, werden Sie informiert, dass Ihr Verzeichnisknoten im Netzwerk nicht sichtbar ist. In Lektion 4 erfahren Sie Näheres über die Verzeichnisdienste.



2 Klicken Sie auf OK.

3 Vergewissern Sie sich, dass ACCOUNTS in der Symbolleiste ausgewählt ist, die Liste der Benutzer angezeigt wird und der aktuelle Administratoraccount ausgewählt und sichtbar ist.

4 Klicken Sie in der Symbolleiste auf NEUER BENUTZER.

Wird die Taste grau dargestellt, klicken Sie auf die Liste der Benutzer, um sie zu aktivieren.

5 Geben Sie im Bereich ALLGEMEIN die folgenden Informationen für den ersten neuen Benutzer ein:

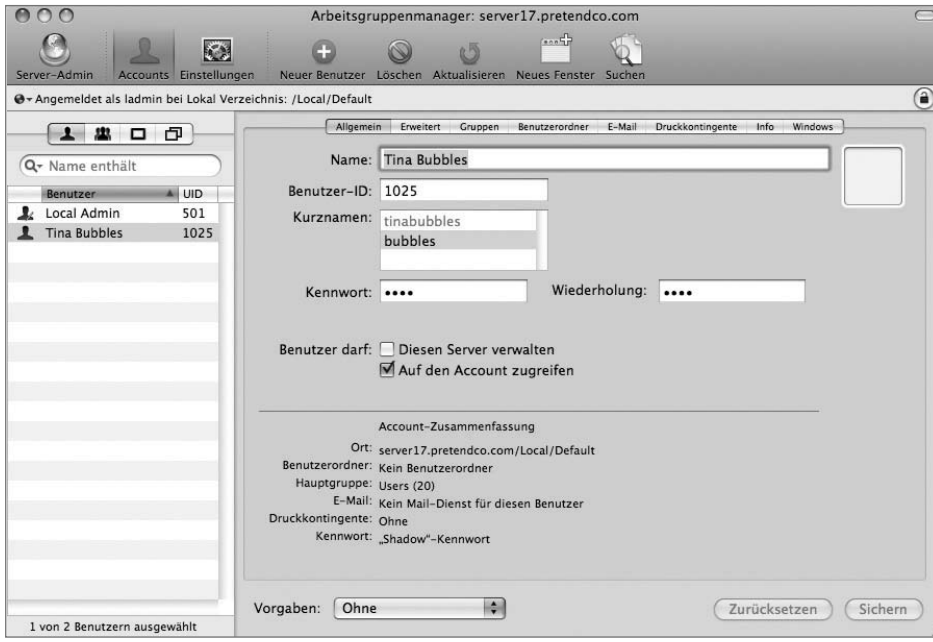
- Name: *Tina Bubbles*
- Kurznamen: *tinabubbles*
- Kennwort: *tina*
- Wiederholung: *tina*

6 Übernehmen Sie bei den anderen Einstellungen die Standardwerte und belassen Sie auch unten im Fenster die Einstellung OHNE im Einblendmenü VORGABEN. Vergewissern Sie sich, dass die Option BENUTZER DARF DIESEN SERVER VERWALTEN nicht ausgewählt ist.

7 Wählen Sie im Feld KURZNAMEN die zweite Zeile (die leere Zeile unter »tinabubbles«) durch Doppelklicken aus, um einen weiteren Kurznamen hinzuzufügen.

8 Geben Sie *bubbles* ein und klicken Sie dann auf SICHERN.

Der neue Benutzername wird in der Liste der Benutzer links im Fenster des Arbeitsgruppenmanagers angezeigt. Nun sollten Sie auch sehen, dass der erste Kurzname grau dargestellt wird, was bedeutet, dass er nicht geändert werden kann. Beachten Sie, dass der Name und die anderen Kurznamen auf diese Weise bearbeitet werden können.



9 Fügen Sie als zweiten Benutzer Warren Peece hinzu, indem Sie auf die Taste NEUER BENUTZER klicken und die folgenden Werte eingeben:

- Name: *Warren Peece*
- Kurznamen: *warren*
- Kennwort: *warren*
- Wiederholung: *warren*
- Übernehmen Sie für die anderen Einstellungen die Standardwerte.

10 Klicken Sie auf SICHERN.

11 Wählen Sie den vorhandenen ACCOUNT LOCAL ADMINISTRATOR in der Liste der aktuellen Benutzer aus.

Beachten Sie, dass für den Administratoraccount das Feld BENUTZER DARF DIESEN SERVER VERWALTEN ausgewählt ist.

Vergleichen Sie nun die beiden neuen Accounts mit dem Administratoraccount. Inwiefern unterscheiden sich die drei Accounts? Die Option DIESEN SERVER VERWALTEN ist für den lokalen Administrator, aber nicht für die anderen Accounts ausgewählt. Wenn Sie neue Benutzer erstellen, werden diese nicht automatisch als Administratoren definiert. Sie müssen erst das entsprechende Feld markieren, damit Benutzer Administratorrechte erhalten.

Konfigurieren von Kommentaren und Schlüsselwörtern

Während der Accounteinrichtung können Sie weitere Informationen wie Kommentare und Schlüsselwörter in jedem Account hinterlegen. Diese Funktionen sind für die Verwaltung von Benutzern oder das Suchen nach bestimmten Benutzern anhand anderer Werte als Name oder Benutzer-ID nützlich. Dadurch erhalten Sie ein praxisorientiertes Verfahren, was die Verwendung individuell angepasster Suchmuster betrifft, ohne Benutzer tatsächlich zu einer bestimmten Gruppe hinzuzufügen.

1 Wählen Sie Tina Bubbles in der Liste der Benutzer aus.

2 Klicken Sie auf ERWEITERT.

3 Geben Sie *Employee# 408081* in das Feld KOMMENTAR ein.

4 Klicken Sie auf die Taste HINZUFÜGEN (+) neben dem Feld SCHLÜSSELWÖRTER.

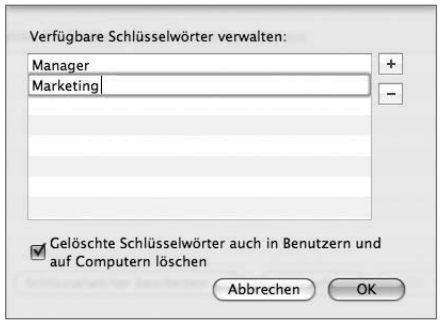
5 Klicken Sie im angezeigten Fenster auf die Taste SCHLÜSSELWÖRTER BEARBEITEN.

6 Klicken Sie im daraufhin angezeigten Fenster VERFÜGBARE SCHLÜSSELWÖRTER VERWALTEN auf die Taste HINZUFÜGEN (+).

7 Geben Sie *Manager* in das Textfeld ein.

8 Klicken Sie nochmals auf die Taste HINZUFÜGEN (+).

9 Geben Sie *Marketing* in die zweite Zeile ein.



10 Klicken Sie nochmals auf die Taste HINZUFÜGEN (+), um ein drittes Schlüsselwort hinzuzufügen: *Engineering*.

11 Klicken Sie auf OK, um die neuen Schlüsselwörter zu sichern und zum Fenster für die Schlüsselwortauswahl zurückzukehren.

12 Wählen Sie MANAGER und klicken Sie auf OK, um das Schlüsselwort *Manager* zu Tinas Benutzeraccount hinzuzufügen.

13 Klicken Sie auf SICHERN.

14 Klicken Sie nochmals auf HINZUFÜGEN (+) und fügen Sie das Schlüsselwort *Marketing* zu Tinas Account hinzu. Klicken Sie auf SICHERN.

15 Wählen Sie Warren aus der Benutzerliste aus, klicken Sie auf HINZUFÜGEN (+) und fügen Sie dann die Schlüsselwörter *Manager* und *Engineering* zum Benutzeraccount von Warren Peece hinzu.

16 Fügen Sie *Employee# 410103* zum Feld KOMMENTAR für Warrens Benutzeraccount hinzu und klicken Sie auf SICHERN.

17 Wählen Sie im Suchfeld über der Liste der Benutzer den Eintrag SCHLÜSSELWORT ENTHÄLT aus dem Einblendmenü neben dem Lupensymbol aus und geben Sie *Manager* ein.

Nur die Accounts von Tina Bubbles und Warren Peece sollten in der Benutzerliste zu sehen sein.

18 Wählen Sie im Suchfeld über der Liste der Benutzer den Eintrag SCHLÜSSELWORT ENTHÄLT aus und geben Sie *Eng* ein.

Nun wird als einziger Benutzer Warren Peece aufgelistet, da Sie das Schlüsselwort *Engineering* nur zu Warrens Account hinzugefügt haben.

19 Wählen Sie im Suchfeld KOMMENTAR ENTHÄLT aus und geben Sie *41* ein.

In der Benutzerliste sollte nur Warren Peece aufgeführt werden, da der Kommentar zu seinem Account die Ziffern 41 als Teil der Personalnummer enthält.

Exportieren und Importieren von Benutzern und Gruppen

Benutzeraccounts können einzeln erstellt oder aus einer korrekt formatierten Datei importiert werden. Diese Datei kann selbst oder mit einem Drittanbieterprogramm erstellt, von von einem anderen Server oder einer Sicherungskopie des aktuellen Servers wiederhergestellt werden. Möchten Sie eine Datensicherung von Benutzer- und Gruppenaccounts anlegen und diese von einem Mac OS X Server Computer wiederherstellen (Näheres hierzu im nächsten Abschnitt), verwenden Sie die Befehle EXPORTIEREN und IMPORTIEREN im Arbeitsgruppenmanager.

Wenn Sie Sicherungskopien von Benutzer- und Gruppenaccounts erstellen wollen, die im Arbeitsgruppenmanager definiert sind, wählen Sie zuerst die zu exportierenden Accounts aus. Wählen Sie dann Server > Exportieren und geben Sie einen Namen und einen Speicherort für die erzeugte Datei an.

HINWEIS ► Sie müssen Benutzer, Benutzergruppen, Computer und Computergruppen separat exportieren, wenn Sie alle Ihre Accounts exportieren möchten. Bei Verwendung der Exportfunktion werden nur die in der aktuellen Ansicht des Arbeitsgruppenmanagers ausgewählten Accounts gesichert. Beachten Sie auch, dass die Kennwörter von Benutzern nie exportiert werden. Wenn Sie also Benutzer aus einer Datei importieren, müssen diese immer neue Kennwörter festlegen.

Wählen Sie Server > Importieren, um Benutzer- oder Gruppenaccounts mit dem Arbeitsgruppenmanager wiederherzustellen. Wählen Sie im Importfenster Neuen Datensatz ignorieren aus dem Einblendmenü Bei Duplikaten aus. Mit dieser Einstellung werden alle Datensätze übergangen, die bereits mit identischen Benutzer-IDs auf Ihrem Server vorhanden sind.

TIPP Mit dem Befehl Importieren können Sie Dateien mit Benutzer- und Gruppenaccounts importieren.

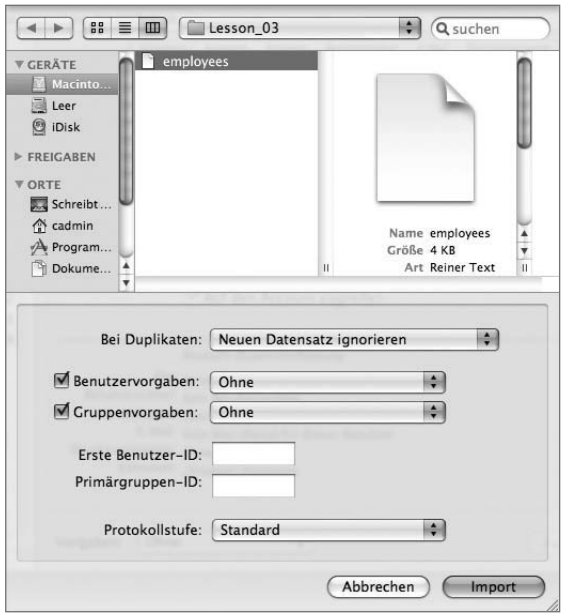
Wenn Sie einen neuen Server einrichten und zahlreiche Benutzer anlegen möchten, importieren Sie die Benutzer wahrscheinlich aus einer vorbereiteten Textdatei, anstatt sie alle einzeln hinzuzufügen. In diesem Abschnitt hat Ihnen ein anderer Systemadministrator eine Datei mit formatierten Benutzereinträgen für die Verwendung mit Ihrem Server zur Verfügung gestellt.

TIPP Versuchen Sie beim Importieren von Benutzer- und Gruppenaccounts mit dem Befehl Importieren die Anzahl der Accounts in jeder Datei auf 10.000 Benutzer zu beschränken. Der Import einer höheren Anzahl Accounts pro Datei wird zwar unterstützt, es ist allerdings einfacher, mit einer kleineren Accountanzahl zu arbeiten.

1 Wählen Sie im Arbeitsgruppenmanager auf Ihrem Mac OS X Computer Server > Importieren.

2 Navigieren Sie im Importfenster zur Datei *Benutzer/Für alle Benutzer/ Student_ Materials/Lesson_03/01employees* und wählen Sie diese aus.

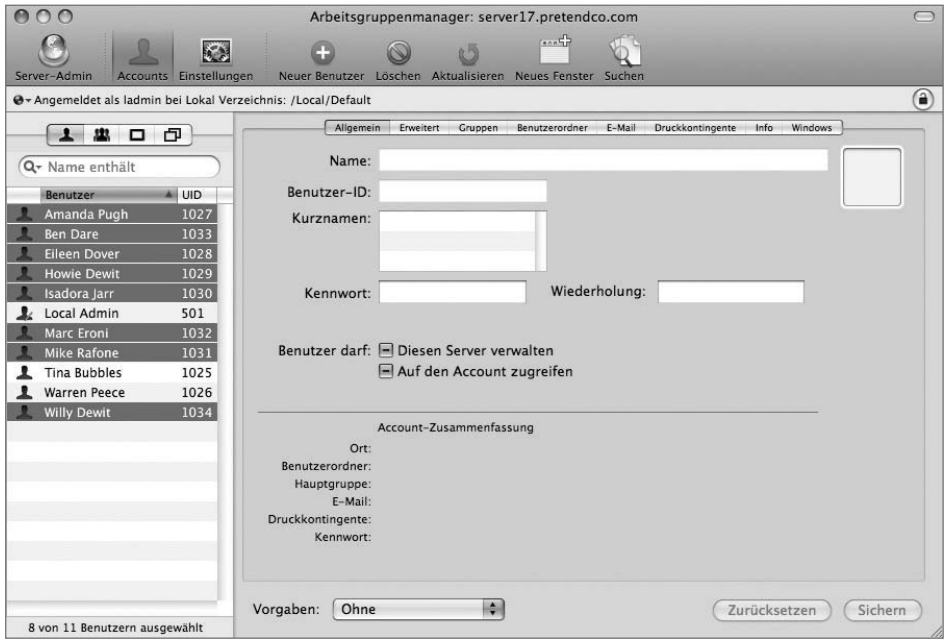
Übernehmen Sie für alle Einstellungen die Standardwerte.



3 Klicken Sie auf IMPORTIEREN.

Weitere acht Benutzer werden importiert. Da die Importdatei der Benutzer keine Kennwörter enthält, müssen Sie für alle neuen Accounts ein Kennwort festlegen. Legen Sie vorerst für alle Accounts dasselbe Kennwort fest.

4 Wählen Sie in der Liste der Benutzer alle neu importierten Accounts aus.



5 Wählen Sie im Bereich ERWEITERT die Option »SHADOW«-KENNWORT aus dem Einblendmenü BENUTZERKENNWORT aus.

Diese Option wird angezeigt, wenn mehrere Accounts ausgewählt sind.

6 Geben Sie im Dialogfenster, das nach der Auswahl von »SHADOW«-KENNWORT angezeigt wird, *changeme* in die Felder KENNWORT und WIEDERHOLUNG ein. Klicken Sie auf OK.

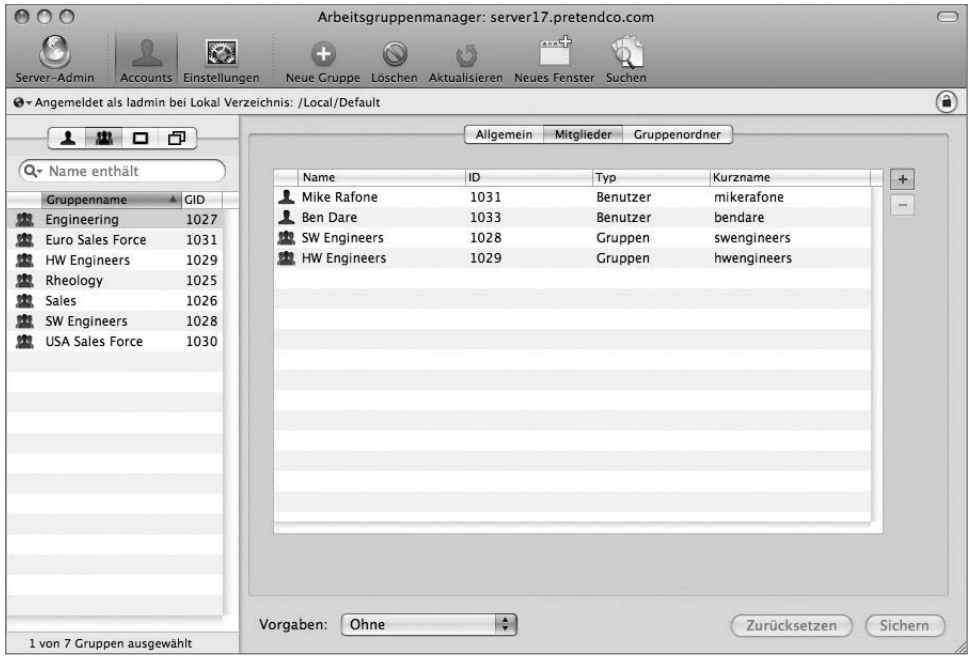
7 Klicken Sie auf SICHERN.

Sie haben nun für alle neuen Accounts dasselbe Kennwort festgelegt. In Lektion 4 lernen Sie, wie Sie Benutzer mit den Kennwortrichtlinien des Arbeitsgruppenmanagers auffordern, ein neues Kennwort festzulegen.

Arbeiten mit Gruppenaccounts im Arbeitsgruppenmanager

Gruppenaccounts sind unter Mac OS X Server eng mit Benutzeraccounts verknüpft. Mithilfe von Gruppenaccounts können Administratoren mehreren Benutzern schnell bestimmte Berechtigungen zuweisen. Mac OS X Client bietet eine einfache Möglichkeit, Gruppenzuweisungen und -berechtigungen mit dem Befehl INFORMATIONEN zu ändern und stellt eine einfache Oberfläche zum Erstellen kleiner Gruppen mit der Systemeinstellung BENUTZER bereit. Für Mac OS X Server werden Sie in der Regel jedoch bedeutend mehr Gruppen mit deutlich mehr Mitgliedern anlegen.

Wenn Sie unter Mac OS X Server eine Gruppe erstellen wollen, öffnen Sie den Arbeitsgruppenmanager, klicken Sie in der Symbolleiste auf NEUE GRUPPE und geben Sie einen Namen für die Gruppe ein. Für die Gruppe sind noch weitere Optionen verfügbar, diese sind für eine korrekte Funktionsweise der Gruppe aber nicht erforderlich.

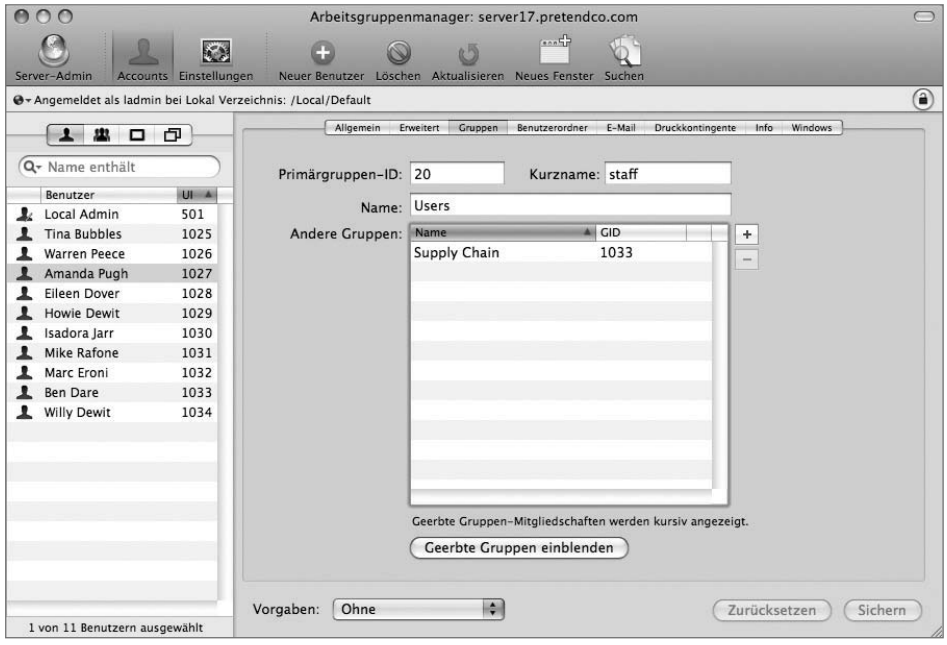


Lange Benutzer- und Gruppennamen dürfen nicht-lateinische Zeichen enthalten. Abhängig vom Zeichensatz haben Sie u. U. nur 85 Zeichen für den vollständigen Namen zur Verfügung. Wenn Sie für Benutzernamen ausschließlich lateinische Zeichen verwenden, sind 255 Zeichen möglich. Die Kurznamen von Benutzern und Gruppen dürfen aus maximal 255 lateinischen Zeichen bestehen.

Seit Mac OS X Server 10.4 wurden einige Einschränkungen aufgehoben, die bei der Verwendung von Gruppen in älteren Mac OS X Server Versionen galten. So wurde beispielsweise die Einschränkung entfernt, dass Benutzer nur bis maximal 16 Gruppen angehören können. Gruppen können auch innerhalb anderer Gruppen verschachtelt sein, wodurch Benutzer in einer Unternehmenshierarchie auf natürlichere Weise dargestellt werden können.

Arbeiten mit Benutzeraccounts und Gruppen-IDs

Alle Benutzer besitzen eine Primärgruppen-ID (GID). Die Primärgruppen-ID des Benutzers wird vom System im zu Grunde liegenden Benutzeraccount-Eintrag gespeichert. Alle anderen Informationen zu Gruppenmitgliedschaften werden in den zu Grunde liegenden Gruppeneinträgen gespeichert. Wenn ein Benutzer eine Datei erstellt, wird die Primärgruppe für Leserechte verwendet.



Mit dem Arbeitsgruppenmanager können Sie einen Benutzer aus einer Gruppe entfernen, indem Sie entweder das Feld ANDERE GRUPPEN im Bereich GRUPPEN des jeweiligen Benutzers oder den Gruppenaccount selbst bearbeiten. Die Primärgruppen-ID lässt sich mit diesen Methoden allerdings nicht ändern. Benutzer, die aufgrund ihrer Primärgruppen-ID Mitglieder einer Gruppe sind, werden in der Liste der Gruppenmitgliedschaften kursiv aufgelistet. Daran können Sie erkennen, dass Sie diese Mitglieder nicht wie gewohnt aus dem Gruppenaccount entfernen können, indem Sie den Benutzer auswählen und auf die Taste ENTFERNEN (–) klicken. Stattdessen müssen Sie die Primärgruppen-ID im Benutzeraccount bearbeiten.

Erstellen von Gruppen mit dem Arbeitsgruppenmanager

Mit dem Arbeitsgruppenmanager können Sie lokale Gruppen erstellen und verwalten.

1 Klicken Sie im Arbeitsgruppenmanager auf Ihrem Mac OS X Computer in der Symbolleiste auf ACCOUNTS.

2 Klicken Sie links im Fenster auf die Taste GRUPPEN.

3 Klicken Sie in der Symbolleiste auf NEUE GRUPPE, um eine neue Gruppe zu erstellen.

4 Geben Sie die folgenden Informationen für die erste neue Gruppe ein:

- Name: *Engineering*
- Kurzname: *engr*

5 Übernehmen Sie in allen anderen Feldern die Standardwerte und klicken Sie auf SICHERN.

6 Erstellen Sie eine zweite Gruppe:

- Name: *Marketing*
- Kurzname: *mktg*

7 Übernehmen Sie in allen anderen Feldern die Standardwerte und klicken Sie auf SICHERN.

Erstellen Sie jetzt zwei weitere Gruppen: *Project X* und *Project Y*:

8 Erstellen Sie eine Gruppe für das Team »Project X«:

- Name: *Project X*
- Kurzname: *projectx*

9 Übernehmen Sie in allen anderen Feldern die Standardwerte und klicken Sie auf SICHERN.

10 Erstellen Sie eine weitere Gruppe für das Team »Project Y«:

- Name: *Project Y*
- Kurzname: *projecty*

11 Übernehmen Sie in allen anderen Feldern die Standardwerte und klicken Sie auf SICHERN.

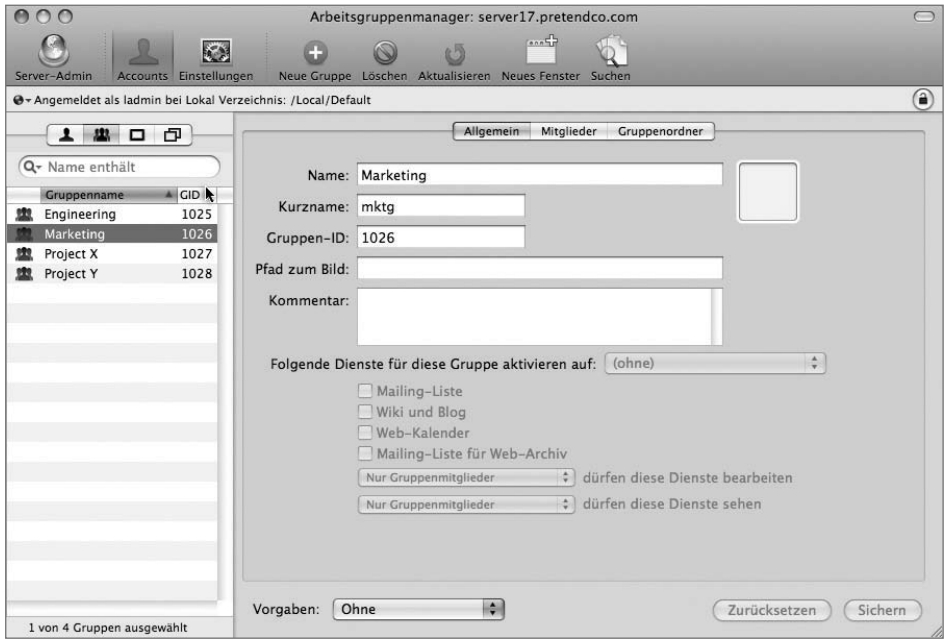
Zuordnen von Benutzern zu Gruppen

Nachdem Sie nun vier Gruppen erstellt haben, müssen Sie diesen die zuvor erstellten Benutzer zuweisen. Hierzu verwenden Sie zwei verschiedene Methoden: das Hinzufügen von Benutzern zu einer Gruppe und das Hinzufügen einer Gruppen-Mitgliedschaft zu einem Benutzeraccount.

Hinzufügen von Benutzern zu Gruppen

Der gängigste Ansatz beim Zuordnen von Benutzern zu Gruppen besteht darin, eine Gruppe auszuwählen und dann einen oder mehrere Benutzer hinzuzufügen. Dazu wählen Sie auf Ihrem Server eine Gruppe aus und fügen dann Benutzer basierend auf Schlüsselwörtern zur Gruppe hinzu.

1 Wählen Sie die Gruppe *Marketing* in der Liste der Gruppen aus.



2 Klicken Sie im Bereich MITGLIEDER auf die Taste HINZUFÜGEN (+) rechts neben der Mitgliederliste.

Das Fach mit den Benutzern und Gruppen wird angezeigt.

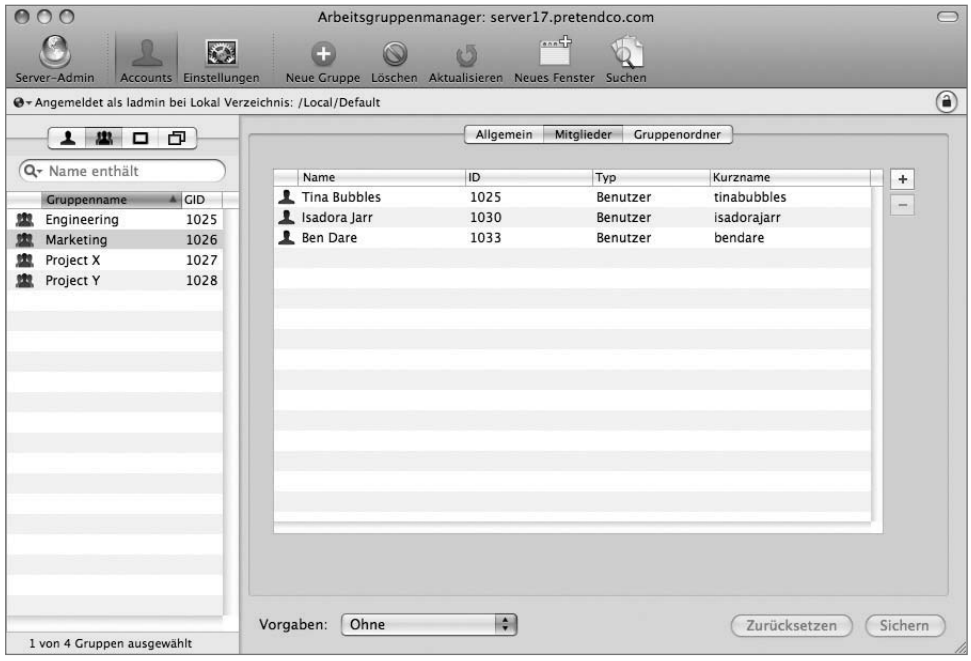
3 Wählen Sie aus dem Einblendmenü im Suchfeld des Fachs für Benutzer und Gruppen SCHLÜSSELWORT ENTHÄLT aus und geben Sie *Mar* ein.

Damit werden alle Benutzer mit dem Schlüsselwort *Marketing* gesucht.

HINWEIS ► Bei Suchvorgängen muss die Groß-/Kleinschreibung beachtet werden. Es werden die vollständigen Namen und nicht die Kurznamen durchsucht.

4 Wählen Sie alle angezeigten Benutzer aus und bewegen Sie sie in die Mitgliederliste.

Nun sollten die Benutzer im Bereich MITGLIEDER für die Gruppe *Marketing* aufgelistet werden.



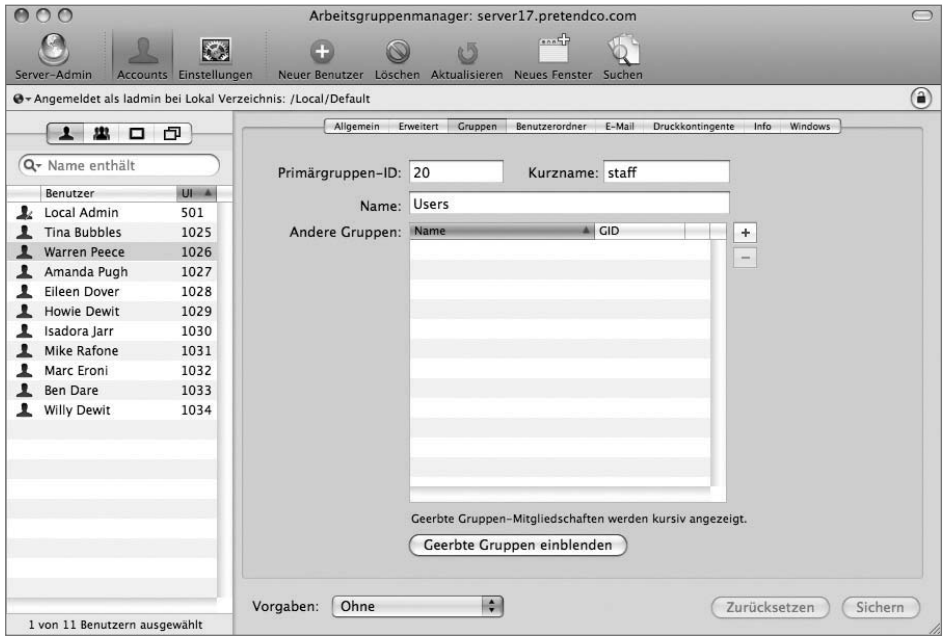
5 Klicken Sie auf SICHERN.

Hinzufügen einer Gruppenmitgliedschaft zu einem Benutzeraccount

Mit den im vorherigen Abschnitt beschriebenen Schritten könnten Sie Warren mühelos zu den Gruppen *Project X* und *Project Y* hinzufügen. Probieren Sie nun einen anderen Ansatz aus, indem sie die Gruppen zu Warrens Account hinzufügen.

1 Klicken Sie links im Fenster des Arbeitsgruppenmanagers auf die Taste BENUTZER und wählen Sie Warren Peece in der Liste der Benutzer aus.

2 Klicken Sie rechts im Bereich auf GRUPPEN.



3 Klicken Sie auf die Taste HINZUFÜGEN (+).

Das Fach für Gruppen mit einer Liste der derzeit auf dem System definierten Gruppen wird angezeigt. Diese Liste enthält sowohl die Gruppen, die Sie erstellt haben, als auch die vom System definierten Gruppen, die Mac OS X Server während der Installation angelegt hat.

4 Wählen Sie die Gruppe *Project X* aus und bewegen Sie sie aus dem Fach für Gruppen in die Liste ANDERE GRUPPEN.

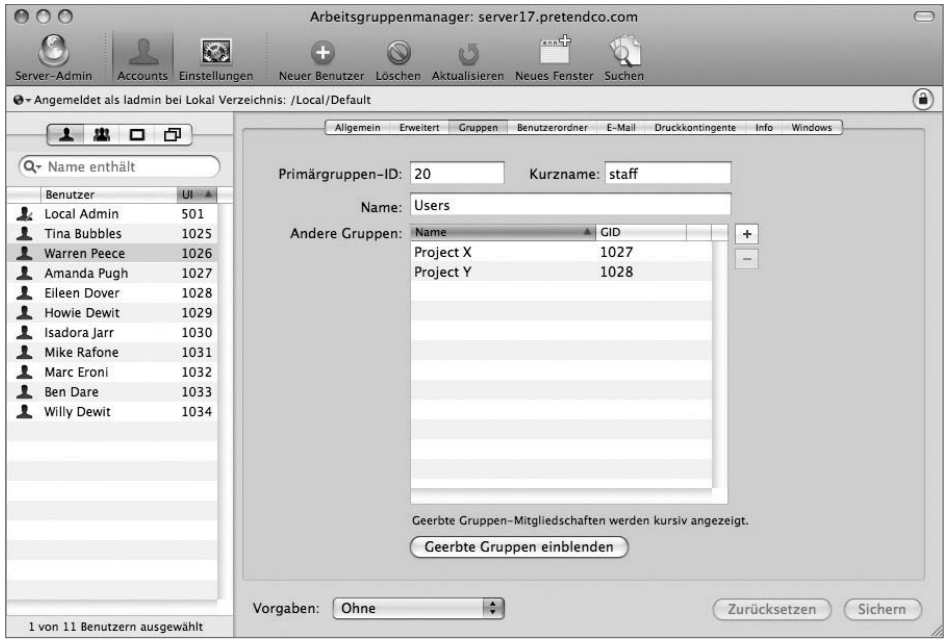
Beachten Sie, dass sich das Zeigersymbol beim Bewegen der Gruppe in ein Pluszeichen ändert. Dies weist darauf hin, dass Sie diese Gruppe zum Textfeld hinzufügen.

5 Klicken Sie auf SICHERN.

Sie haben nun die Mitgliedschaft der Gruppe *Project X* erfolgreich zu Warrens Account hinzugefügt. Warren benötigt allerdings auch Zugriff auf die Gruppe *Project Y*.

6 Wiederholen Sie die Schritte 3, 4 und 5, um die Gruppe *Project Y* zu Warrens Benutzeraccount hinzuzufügen.

Damit haben Sie nun mehrere Gruppen (Project X und Project Y) zu Warrens Benutzeraccount hinzugefügt.



Hinzufügen von Gruppen zu Gruppen

Angenommen, Sie benötigen eine Gruppe, mit der Sie die Berechtigungen der gesamten Engineering-Abteilung steuern können und die aus zwei Teilgruppen (Project X und Project Y) besteht. Sie könnten alle Benutzeraccounts der Mitarbeiter der Engineering-Abteilung einzeln zur Gruppe *Engineering* hinzufügen. Einfacher ist es jedoch, die beiden Projektgruppen zur Gruppe *Engineering* hinzuzufügen. Damit werden alle Mitglieder dieser Gruppen zur Hauptgruppe hinzugefügt, was die Verwaltung von Gruppen im Vergleich zu älteren Mac OS X Server Versionen vereinfacht.

1 Klicken Sie links im Fenster des Arbeitsgruppenmanagers auf die Taste GRUPPEN und wählen Sie die Gruppe *Engineering* in der Liste der Gruppen aus.

2 Klicken Sie im Bereich MITGLIEDER auf die Taste HINZUFÜGEN (+) rechts neben der Mitgliederliste, um das Fach für Benutzer und Gruppen zu öffnen.

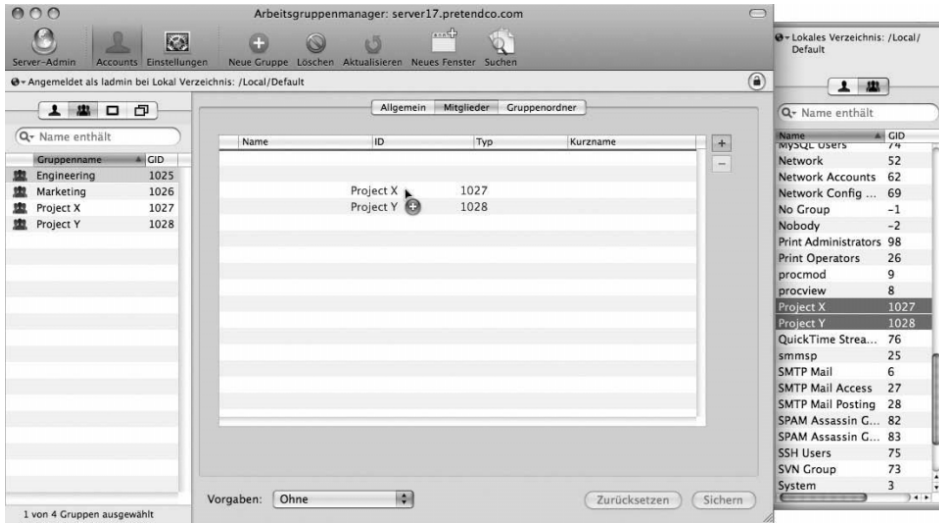
3 Klicken Sie im Fach für Benutzer & Gruppen auf die Taste GRUPPEN.

4 Bewegen Sie die Gruppen *Project X* und *Project Y* in die Mitgliederliste.

Alle Mitglieder der Gruppen *Project X* und *Project Y* haben jetzt Zugriff auf die von der Gruppe *Engineering* ausgeführten Aufgaben.

5 Klicken Sie auf SICHERN.

Nun haben Sie Benutzer und Gruppen zu Ihrem Server hinzugefügt sowie Gruppen zu Gruppen.



Steuern des Zugriffs über Serveraccounts

Das Autorisierungsverfahren kommt unter Mac OS X und Mac OS X Server gleichermaßen zum Einsatz. Das gängigste Beispiel ist für den Benutzer meist leicht nachvollziehbar: Jedes Mal, wenn ein Benutzer auf eine Datei zugreift, vergleicht der Computer die Zugriffsrechte für die Datei mit den Accountinformationen des Benutzers und ermittelt so, ob der Benutzer zur Verwendung der Datei berechtigt ist. Unter Mac OS X und Mac OS X Server sind allen Dateien, Ordnern und Programmen Eigentümer- und Gruppenberechtigungen zugeordnet.

Beim Zugriff auf einen Dateiserver müssen Sie sich in der Regel anmelden (identifizieren) und können anschließend aus einer Reihe aktivierbarer Netzwerkordner wählen. Wenn Sie innerhalb eines aktivierten Netzwerkordners navigieren, werden Ordnerkennzeichnungen eingeblendet (kleine Symbole auf oder unter den Ordnersymbolen), die angeben, ob Sie Lese-/Schreibzugriff, nur Lesezugriff, nur Schreibzugriff oder gar keinen Zugriff haben.

Wenn Sie über Server-Admin oder den Arbeitsgruppenmanager eine Verbindung zu einem Server herstellen, wird Ihr Benutzername nach der Anmeldung überprüft und ermittelt, ob Sie mit diesem Account zur Ausführung administrativer Aufgaben berechtigt sind. Versucht ein Benutzer auf einen Dienst wie den Podcast-Produzenten auf Ihrem Server zuzugreifen, wird ebenfalls geprüft, ob der Benutzer zur Verwendung dieses Dienstes berechtigt ist.

Verwenden der Autorisierung unter Mac OS X Server

POSIX-Berechtigungen (Portable Operating System Interface) wurden bereits mit den ersten Mac OS X und Mac OS X Server Systemen verwendet. Auch heute finden sie unter Mac OS X und Mac OS X Server noch Verwendung und sind für alle Dateien oder Ordner im Dateisystem vorhanden. Bei POSIX-Berechtigungen handelt es sich um traditionelle, auf UNIX basierende Berechtigungen, die es Ihnen ermöglichen, Lese-, Schreib- und Ausführungsrechte folgenden Benutzergruppen zuzuweisen: dem Eigentümer, der Gruppe und allen anderen Benutzern. Die Berechtigungen, die anfangs im Fenster INFORMATIONEN von Mac OS X angezeigt werden, sind POSIX-Berechtigungen.

In Mac OS X Versionen vor 10.4 konnte der Dateizugriff unter Mac OS X Server nur anhand von POSIX-Berechtigungen gesteuert werden. Mac OS X Server 10.4 basierte zwar immer noch auf den bewährten POSIX-Berechtigungen, bot aber zusätzlich die Möglichkeit, komplexe Zugriffsregeln zu definieren, was mit den standardmäßigen POSIX-Berechtigungen nicht möglich war. Umgesetzt wurde dieses mithilfe von *Zugriffssteuerungslisten* oder ACLs (Access Control Lists). ACLs werden von Volumes unterstützt, die im Format MAC OS EXTENDED formatiert sind. Sie werden im Dateisystem selbst gespeichert und verwenden erweiterte Attribute, die in Mac OS Extended-Dateisystemen schon immer vorhanden waren, aber nicht genutzt wurden. Auf diese Weise können ACLs unterstützt werden, ohne das Volume mit einem neuen Dateisystemformat formatieren zu müssen. Unter Mac OS X 10.5 ist die ACL-Unterstützung standardmäßig aktiviert.

Für Benutzer, die über das Netzwerk auf den Server zugreifen, werden ACLs bei AFP- und SMB-Protokoll-Verbindungen unterstützt. Die ACLs sind auch mit den Windows-ACLs kompatibel. Damit wird die Benutzerfreundlichkeit beim Zugriff auf Mac OS X Server von Windows-Clients aus erhöht, da diese Benutzer feiner abgestufte Berechtigungseinstellungen erwarten können als bisher bei Mac OS X Server verfügbar waren. Diese Zugriffsrechte können so eingestellt werden, dass sie einen komplexen Arbeitsablauf unterstützen, in dem viele verschiedene Benutzerberechtigungen erforderlich sind, damit ein Dokument von verschiedenen Autoren und Lektoren bearbeitet werden kann. Wenn Sie über das Fenster INFORMATIONEN von Mac OS X weitere Benutzer oder Gruppen zur Berechtigungsliste hinzufügen, geschieht dies mithilfe von ACLs.

Berücksichtigen Sie, dass ACLs Windows-Administratoren bekannt sind, für Macintosh-Administratoren jedoch ein neues Konzept darstellen. Mac OS X Server lässt sich aus diesem Grund besonders einfach in eine Windows-Umgebung integrieren.

Überprüfen von POSIX-Berechtigungen

Alle Dateien und Ordner unter Mac OS X besitzen Informationen zu Eigentümer und Berechtigungen, mit denen die verfügbaren Zugriffsrechte für die Dateien und Ordner definiert werden. Der Begriff »Eigentümer« umfasst die Konfiguration eines Eigentümers und einer Gruppe, der Begriff »Berechtigungen« bezieht sich auf das Festlegen bestimmter Zugriffseinstellungen für die Eigentümer, die Gruppe und alle anderen Benutzer, die meist als »Andere« (everyone, other) bezeichnet werden. Bei einer Festlegung im Finder können diese Berechtigungen LESEN & SCHREIBEN, NUR LESEN, NUR SCHREIBEN (BRIEFKASTEN) und KEINE RECHTE lauten. Bei Verwendung der Befehlszeile gibt es einige weitere Möglichkeiten. Wenn Sie den Eigentümer oder die Berechtigungen eines Objekts über die Befehlszeile ändern, werden die Änderungen im Fenster INFORMATIONEN zu diesem Objekt angezeigt. Wenn Sie die Berechtigungen im Fenster INFORMATIONEN ändern, werden die Änderungen ebenfalls übernommen, wenn Sie das Objekt in der Befehlszeile anzeigen.

Der Buchstabe »d« vor den Berechtigungen in der Abbildung oben weist darauf hin, dass es sich um einen Ordner handelt (das »d« steht für das englische Wort *directory* (Verzeichnis, Ordner)). Die Berechtigungen für den Eigentümer (rwx) entsprechen den Berechtigungen LESEN & SCHREIBEN im Fenster INFORMATIONEN dieses Ordners. Die Berechtigungen für die Gruppe (r-x) entsprechen der Berechtigung NUR LESEN im Fenster INFORMATIONEN. Die Berechtigungen für EVERYONE (-wx) geben an, dass alle anderen in den Ordner schreiben, aber dessen Inhalt nicht lesen können. Bei einer Datei weist die Berechtigung »x« (für »Ausführen«) darauf hin, dass es sich um ein ausführbares Programm handelt. Bei einem Ordner wird mit der Berechtigung zum Ausführen festgelegt, ob der Ordner durchsucht werden kann. Damit Sie auf eine Datei in einem Ordner zugreifen können, benötigen Sie eine Suchberechtigung für alle Ordner vom root-Ordner bis einschließlich zu dem Ordner, der die Datei enthält.

HINWEIS ► Für Verzeichnisse und Dateien werden die Berechtigungen für EVERYONE/OTHER (oder ANDERE) in der Regel auf NUR LESEN eingestellt. Das scheint zwar sicher zu sein, denken Sie jedoch daran, dass auf Ihrem Server u. U. der Gastzugriff aktiviert ist und somit möglicherweise beliebige Computer, die eine Verbindung zum Server herstellen können, diese Dateien lesen können.

Bei Verwendung von POSIX wird über die Benutzer-ID der Zugriff als Eigentümer auf eine Datei oder einen Ordner definiert. Stimmt die numerische Benutzer-ID der Datei oder des Ordners mit der im Benutzeraccount definierten Benutzer-ID überein, gilt dieser Benutzer als Eigentümer der Datei oder des Ordners. Der Gruppenzugriff wird ähnlich festgelegt: Allen Dateien oder Ordnern ist eine Gruppen-ID zugeordnet. Jeder Gruppenaccount verfügt über eine numerische Gruppen-ID. Ist der Benutzer ein Mitglied einer Gruppe mit einer Gruppen-ID, die mit der Gruppen-ID der Datei oder des Ordners übereinstimmt, erhält der Benutzer den in den Einstellungen der Gruppenberechtigungen festgelegten Zugriff.

Einschränkungen von POSIX-Berechtigungen

Ein einfaches Beispiel für das Festlegen von Zugriffsrechten: Angenommen, in einer Schule soll ein gemeinsam genutzter Mathematikordner mit der Bezeichnung *Math Files* konfiguriert werden. Die Administratoren der Schule möchten den Mathematiklehrern das Lesen, Schreiben und Löschen von Dateien ermöglichen und den Schülern Leserechte für dieselben Dateien erteilen. Idealerweise wird der Ordner *Math Files* so eingerichtet, dass nur die Mathematikschüler und nicht alle Schüler darauf zugreifen können. Die Umsetzung dieses Beispiels wäre mit standardmäßigen POSIX-Berechtigungen schwierig, da Sie die Zugriffsrechte nur über eine einzige Gruppe steuern könnten.

Es gibt verschiedene Ansätze zur Lösung dieses Problems, die alle jedoch unterschiedliche Einschränkungen aufweisen. Bei der ersten Methode weisen Sie die Gruppe *Math_Teachers* dem Ordner zu und erteilen ihr Lese- und Schreibzugriff. Dann legen Sie fest, dass Mathematikschüler nicht in den Ordner schreiben, indem Sie für EVERYONE Lesezugriff festlegen. Der Nachteil dieser Lösung ist, dass Sie damit allen anderen Benutzern in der Schule Lesezugriff auf den Ordner *Math Files* gewähren.

Ein anderer Ansatz besteht darin, die Nutzer des Ordners – Lehrer und Schüler – zu einer Gruppe zusammenzufassen (Math Department). Dieser Gruppe können Sie dann Zugriff gewähren und den Zugriff aller anderen Benutzer unterbinden. Damit haben Sie das Problem beseitigt, dass die gesamte Schule auf den Ordner *Math Files* zugreifen kann, haben jedoch gleichzeitig ein neues Problem geschaffen: Da Schüler und Lehrer nun einer gemeinsamen Gruppe angehören, haben sie dieselben Zugriffsrechte. Schüler sollen aber nur Lesezugriff und keinen Schreibzugriff erhalten. Damit haben Sie diese Granularität verloren. Möglicherweise könnten Sie zwei Unterordner mit verschiedenen Zugriffsrechten für die Mathematikschüler und die Mathematiklehrer erstellen. Doch wie gehen Sie vor, wenn Sie den Zugriff noch genauer steuern möchten? Vielleicht sollen auch Lehrer anderer Fachbereiche ebenso wie die Mathematikschüler Lesezugriff erhalten.

Ihr Ziel ist es also, die Einschränkungen des Berechtigungssystems zu umgehen, um die gewünschten Zugriffsrechte einzurichten. Glücklicherweise können Sie mit dem Zugriffssteuerungssystem von Mac OS X Server Zugriffsrechte auf einfache Weise – mithilfe von ACLs – einrichten und umsetzen.

Festlegen von POSIX-Berechtigungen mit Server-Admin

Gehen Sie wie folgt vor, um die POSIX-Berechtigungen für einen Ordner zu ändern:

1 Stellen Sie mit Server-Admin auf Ihrem Mac OS X Computer eine Verbindung zum Mac OS X Server Computer her.

HINWEIS ► Sie müssen Ihren Server für die Nutzung mindestens eines File-Sharing-Dienstes wie AFP konfiguriert haben, um die File-Sharing-Konfigurationsfunktionen zum Festlegen von Zugriffsrechten verwenden zu können. Der File-Sharing-Dienst muss nicht gestartet werden, muss aber vorhanden sein. Ist er nicht vorhanden, können Sie ihn durch Auswahl von NAME.IHRES.SERVERS > EINSTELLUNGEN > DIENSTE hinzufügen.

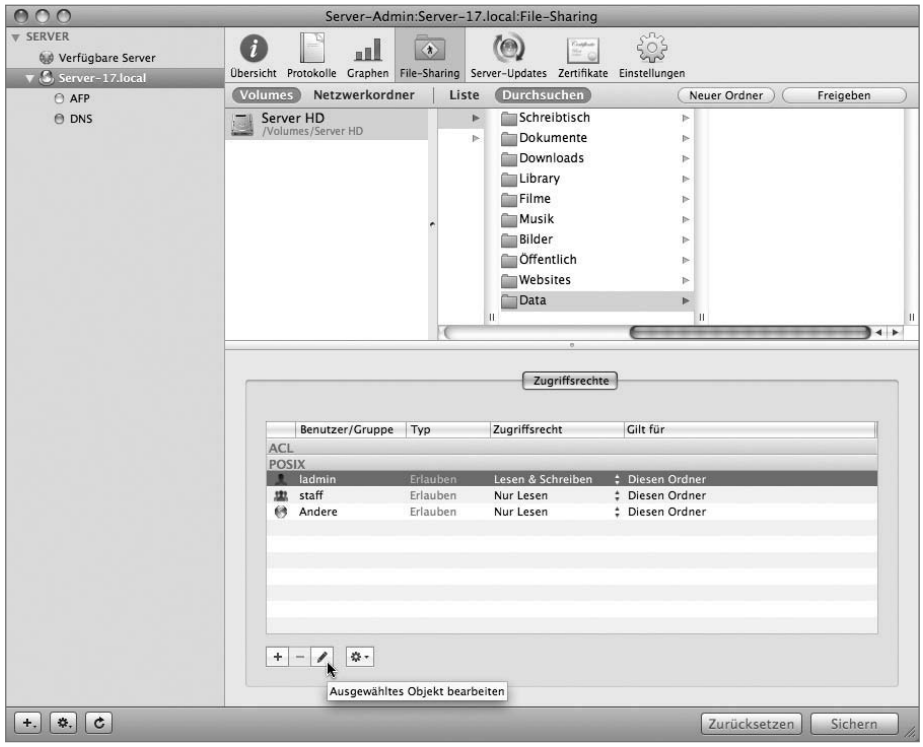
2 Klicken Sie in der Symbolleiste auf FILE-SHARING.

3 Klicken Sie unter der Symbolleiste auf die Taste DURCHSUCHEN.

4 Wählen Sie einen Ordner im Dateisystem aus, auf den Sie Einstellungen anwenden möchten.

5 Wählen Sie den Benutzer oder die Gruppe in der Liste POSIX im Bereich ZUGRIFFSRECHTE aus.

6 Klicken Sie auf die Taste BEARBEITEN (das Stiftsymbol).



7 Geben Sie einen anderen Kurznamen für den Benutzer oder die Gruppe ein und klicken Sie auf die Markierungsfelder, um die aktuellen Einstellungen zu ändern. Klicken Sie dann auf OK.

8 Weisen Sie mithilfe der Einblendmenüs Berechtigungen für Eigentümer, Gruppe und Andere zu.

9 Klicken Sie auf SICHERN.

Versucht ein Benutzer auf eine Datei oder einen Ordner zuzugreifen, wird der Benutzeraccount wie unter Mac OS X mit dem Eigentümer und der Gruppe der Datei oder des Ordners verglichen. Entspricht der Benutzeraccount dem Eigentümer, werden die dem Eigentümer zugewiesenen Berechtigungen umgesetzt und die Berechtigungen für die Gruppe und für ANDERE für diesen Account ignoriert. Entspricht der Benutzeraccount nicht dem Eigentümer sondern einem Gruppenmitglied, gelten die Gruppenberechtigungen. Gehört der Account weder dem Eigentümer noch einem Gruppenmitglied, gelten die Berechtigungen von ANDERE. Besitzt nur der Eigentümer die Berechtigung zum Löschen, wie etwa in einem gemeinsam genutzten temporären Arbeitsbereich, haben berechtigte Benutzer Lese- und Schreibzugriff auf die Datei, doch nur der Eigentümer kann sie löschen. Diese Option kann nur in der Befehlszeile mit dem Befehl `chmod +t` festgelegt werden.

Festlegen von ACLs

In den Client- und Serverversionen von Mac OS X 10.5 sind ACLs standardmäßig aktiviert. Sollten Sie jedoch einem bestimmten Volume keine ACLs zuweisen können, müssen die ACLs möglicherweise erst mit dem Befehl `fsaclctl` im Programm TERMINAL aktiviert werden.

Festlegen von ACLs mit Server-Admin

Unter Mac OS X Server 10.4 wurden Dateisystem-ACLs mit dem Arbeitsgruppenmanager definiert, in Version 10.5 verwenden Sie jedoch Server-Admin. Nachfolgend werden die Schritte genannt, die Sie zum Aktualisieren der Zugriffssteuerungseinträge (Access Control Entrys oder ACEs) innerhalb einer ACL gewöhnlich ausführen müssen (diese ähneln der Verwaltung von POSIX-Berechtigungen abgesehen vom Bereich, innerhalb des Arbeitsgruppenmanagers, in den Sie die Benutzer und Gruppen hineinbewegen):

1. Verwenden Sie Server-Admin auf Ihrem Mac OS X Computer, um eine Verbindung zum Mac OS X Server herzustellen.

   Wenn bereits eine Verbindung zum Server besteht, wählen Sie den Server in der Liste der verfügbaren Server rechts im Server-Admin-Fenster aus.

2. Klicken Sie in der Symbolleiste auf FILE-SHARING.

3. Klicken Sie unter der Symbolleiste auf die Taste DURCHSUCHEN.

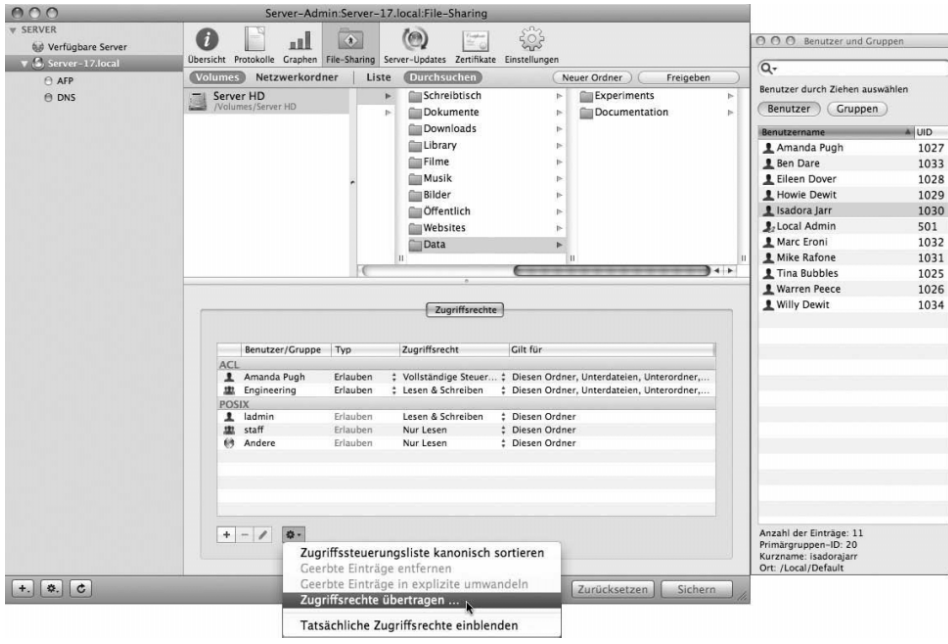
4. Wählen Sie einen Ordner im Dateisystem aus, auf den Sie Einstellungen anwenden möchten.

5 Klicken Sie auf die Taste HINZUFÜGEN (+), um das Fach BENUTZER UND GRUPPEN zu öffnen.

6 Bewegen Sie einen bestimmten Benutzer oder eine bestimmte Gruppe in die ACL-Liste.

Enthält die Liste ACL derzeit keine Einträge, wird zwischen den Listen ACL und POSIX nur eine blaue Linie angezeigt, sobald Sie den Benutzer oder die Gruppe dorthin bewegen.

7 Verwenden Sie für jeden Berechtigungseintrag die Einblendmenüs in der Spalte ZUGRIFFSRECHT, um eine Berechtigung aus den vorgegebenen Standardeinstellungen auszuwählen. Klicken Sie alternativ dazu auf die Taste BEARBEITEN (das Stiftsymbol), um eigene Einstellungen zu konfigurieren.



8 Konfigurieren Sie wie erforderlich weitere Benutzer oder Gruppen.

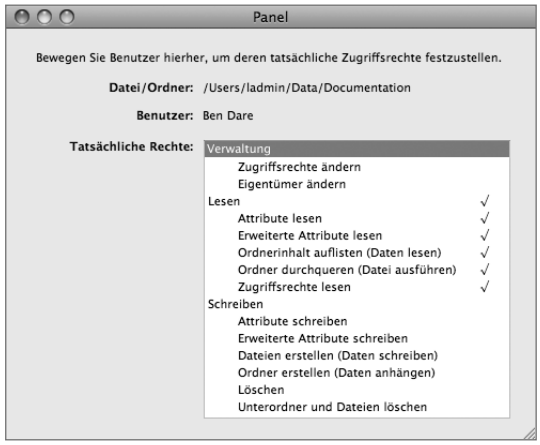
9 Ändern Sie falls gewünscht die Regeln für die Vererbung, indem Sie für jeden Benutzer- oder Gruppeneintrag eine Option aus dem Einblendmenü in der Spalte GILT FÜR auswählen.

10 Klicken Sie auf SICHERN.

11 Verwenden Sie bei Bedarf das Aktionsmenü (das Zahnradsymbol), um Einstellungen auf enthaltene Dateien oder Ordner zu übertragen.

Festlegen des Benutzerzugriffs auf einen Ordner

ACLs können in großen Organisationen ziemlich komplex werden. Durch eine durchdachte Verwendung von Gruppenmitgliedschaften lässt sich leichter feststellen, welche Benutzer Zugriff auf welche Objekte haben. Möglicherweise sind Sie sich aber dennoch nicht sicher, wer auf welchen Ordner zugreifen darf. Im Informationsfenster TATSÄCHLICHE ZUGRIFFSRECHTE EINBLENDEN wird genau angegeben, welche Zugriffsrechte ein bestimmter Benutzer für den ausgewählten Ordner hat. Sie öffnen dieses Fenster, indem Sie TATSÄCHLICHE ZUGRIFFSRECHTE EINBLENDEN aus dem Aktionsmenü (Zahnradsymol) auswählen. Bewegen Sie nach dem Öffnen des Informationsfensters einen Benutzer oder eine Gruppe in das Fenster. Nun werden detailliert die Zugriffsrechte des jeweiligen Benutzers bzw. der Gruppe und der ausgewählten Datei bzw. des ausgewählten Ordners oder Volumes angezeigt.



Unterschiede bei der Verwendung von Benutzer-ID, Gruppen-ID und GUID

Sie haben gelernt, dass POSIX-Eigentümer und -Gruppen durch Benutzer- und Gruppen-IDs bestimmt werden. Da Benutzer-IDs und Gruppen-IDs schlicht aus ganzen Zahlen bestehen, haben möglicherweise mehrere Benutzer dieselbe Benutzer-ID. Dies führt im Normalfall zu Problemen, doch unter bestimmten Umständen wählt ein Administrator bewusst dieselbe POSIX-Benutzer-ID für zwei verschiedene Benutzer.

ACLs sind bedeutend komplexer und erfordern eine eindeutige Identifizierung eines Benutzers oder einer Gruppe. Aus diesem Grund besitzen alle Benutzer und Gruppen eine GUID (Globally Unique ID). Diese ist auf der Benutzeroberfläche nicht zu sehen, da im Normalfall kein Grund zu ihrer Änderung besteht. Immer, wenn ein Benutzer erstellt wird, wird eine neue 128-Bit-Nummer generiert (z. B.: 835E78F0-7808-4758-8C92-CF8AB428B99B), die auf dem Zeitwert und anderen Informationen basiert. Auf diese Weise wird eine eindeutige Identifizierung in ACLs für Benutzer und Gruppen praktisch gewährleistet.

TIPP Möglicherweise beschweren sich Benutzer, die auf einen komplexen Server zugreifen, dass sie bestimme Dateien nicht sehen können. Informieren Sie sich das nächste Mal bei solch einer Anfrage mit Hilfe des Informationsfensters TATSÄCHLICHE ZUGRIFFSRECHTE EINBLENDEN, über welche Berechtigungen der Benutzer verfügt.

Beispiele für ACL-Arbeitsabläufe

Wenn Sie mit ACLs arbeiten, müssen Sie die Konfiguration sorgfältig planen, um Konflikte bei den Berechtigungeinstellungen zu vermeiden. Diese treten beispielsweise auf, wenn ein Benutzer Mitglied zweier Gruppen ist, von denen eine Lesezugriff auf einen Ordner besitzt und die andere keinen Zugriff. Diese Art von Konflikten kann auftreten, wenn Sie Ihre ACL-Modelle nicht sorgfältig planen.

Mehrere Gruppen

Die POSIX-Berechtigungen funktionieren gut auf einem Client-Computer wie Mac OS X . Wenn das System jedoch komplexer wird, etwa in größeren Unternehmen, lässt sich das POSIX-Modell nur schlecht skalieren.

Für komplexe Arbeitsabläufe muss eine besser abgestufte Einteilung als bei den POSIX-Bereichen *Eigentümer*, *Gruppe* und *Andere* verfügbar sein. Es sind insbesondere mehr Gruppen erforderlich. Der POSIX-Eigentümer muss über einen individuellen Benutzeraccount verfügen (eine Gruppe kann nicht verwendet werden). Werden Berechtigungen den Benutzern ANDERE zugewiesen, werden die Dateien meist für mehr Benutzer zugänglich als gewünscht. ACLs erlauben das Zuweisen mehrerer Gruppen zu einem Ordner. Dabei erhält jede Gruppe eine eindeutige Berechtigungseinstellung. In Umgebungen, in denen mehrere Gruppen an einem gemeinsamen Projekt arbeiten, ist dies eine gängige Anforderung. Ein gutes Beispiel ist etwa eine Produktionsumgebung mit Autoren, Grafikeditoren, Redakteuren und Herausgebern. Hier arbeiten verschiedene Gruppen zu unterschiedlichen Zeitpunkten an denselben Dateien. Da mit ACLs mehreren Gruppen unterschiedliche Berechtigungen zugewiesen werden können, müssen Sie Ihre Gruppenstruktur sorgfältig planen, um Konflikte zu vermeiden.

In unserem Beispiel erhält jede Gruppe spezifische Berechtigungen für jeden Ordner. Ein Benutzer in der Gruppe *Autoren* kann ein Dokument im Ordner *Abgabe* ablegen und besitzt Lese- und Schreibzugriff auf diese Datei, solange sie sich in diesem Ordner befindet. Die Gruppe *Redakteure* kann die Dateien im Ordner jedoch nur lesen. Den Benutzern der Gruppen *Produktionsmitarbeiter* und *Grafikeditoren* wurde kein Lese- oder Schreibzugriff auf den Ordner *Abgabe* gewährt.

Die Benutzer der Gruppe *Autoren* können das Dokument in den Ordner *Editoren* bewegen, erhalten aber keinen Lesezugriff auf diesen Ordner. Benutzer der Gruppe *Redakteure* besitzen Lesezugriff sowie bestimmte Schreibrechte zum Erstellen von Ordnern oder Dateien innerhalb des Ordners *Editoren*. Damit erhalten sie die Möglichkeit, eine Kopie des Dokuments im Ordner zu erstellen. Benutzer der Gruppe *Grafikeditoren* besitzen ebenfalls Lesezugriff, können jedoch nur Attribute in das Dokument schreiben und keine neuen Dateien im Ordner *Editoren* erstellen. Benutzer der Gruppe *Produktionsmitarbeiter* können die Dateien lesen.

Ferner können Benutzer der Gruppe *Produktionsmitarbeiter* das Dokument in den Ordner *Produktion* kopieren und dort alle Dokumente lesen und bearbeiten. Benutzer der Gruppe *Autoren* haben keinen Lese- und Schreibzugriff auf den Ordner *Produktion* und alle darin enthaltenen Dokumente. Benutzer der beiden Editorengruppen verfügen über alle Leserechte, können jedoch nur erweiterte Attribute schreiben.

Verschachtelte Gruppen

Mit Mac OS X Server können nicht nur mehrere Gruppen einem einzigen Ordner zugewiesen werden, sondern auch Gruppen innerhalb *anderer Gruppen* erstellt werden. Die Gruppe *Autoren* kann beispielsweise in weitere Gruppen unterteilt werden, etwa basierend auf der Art der Artikel, die die jeweiligen Mitarbeiter schreiben (z. B. Feuilleton oder Kolumnen).

Vielleicht wundern Sie sich, warum verschachtelte Gruppen benötigt werden, wenn mit ACLs doch mehrere Gruppen einem Ordner zugewiesen werden können. Warum sollten Sie die Gruppe *Autoren* etwa dem Ordner *Abgabe* zuweisen, statt den drei Gruppen (*Feuilletonisten*, *Journalisten* und *Werbetexter*) den Zugriff direkt zu ermöglichen? Der Effekt wäre derselbe.

Das Unterteilen von Gruppen in Untergruppen kann dazu beitragen, dass die Zugriffsrechte für Sie als Administrator einfacher nachzuvollziehen sind. Wenn Sie nach einem Monat allen Autoren Zugriff auf einen neuen Ordner gewähren müssen, müssen Ihnen die verwaltungsbezogenen Details Ihrer Gruppen noch bekannt sein.

Werden Sie sich daran erinnern, dass Sie die Gruppen *Feuilletonisten*, *Journalisten* und *Werbetexter* zum neuen Ordnern hinzufügen müssen, damit alle Autoren Zugriff darauf erhalten? Mit einer übergeordneten Gruppe wie *Autoren* werden solche Aufgaben vereinfacht.

Sie können die Struktur Ihrer Organisation auf die verschachtelten Gruppen übertragen. Statt des Verlagsbeispiels kann auch eine Schule verwendet werden: die Klassenstufe kann als Gruppe dienen, die die einzelnen Schulklassen enthält.

Verschachtelte Gruppen bieten zwar viele Vorteile, sollten jedoch sorgfältig durchdacht werden. Wenn Sie eine verzweigte, komplexe Hierarchie erstellen, ist der Zugriff möglicherweise schwieriger anstatt einfacher verständlich. Meist ist eine Anlehnung an die Struktur der Organisation eine sichere und nützliche Methode. Vermeiden Sie jedoch die kurzfristige Erstellung von Gruppen, die sich auf keine externe Struktur beziehen. Damit können Sie zwar bestimmten Benutzern rasch Zugriff gewähren, sie lassen sich jedoch zu einem späteren Zeitpunkt nur schwer zuordnen.

Vererbung

Ein weiteres Merkmal von ACLs ist die *Vererbung*: Objekte in einem Ordner übernehmen die ACLs des übergeordneten Ordners. Benutzer arbeiten in der Regel mit übernommenen Dateiberechtigungen. Wenn Benutzer Dateien auf dem Server erstellen, werden von den verwendeten Programmen, auch dem Finder, keine expliziten ACLs für die kopierten Objekte festgelegt. In diesem Fall gelten für die Datei die Berechtigungen des übergeordneten Ordners.

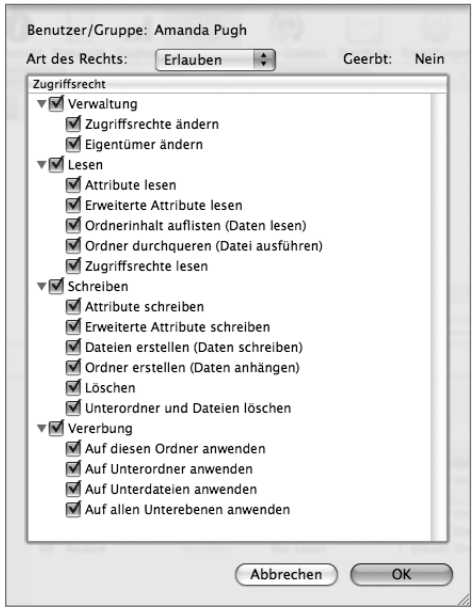
Die Vererbung oder Übernahme von Berechtigungen bietet Ihnen eine weitere Möglichkeit, Ihre Struktur umzusetzen. Das Beispiel des Arbeitsablaufs im Verlag ist insofern relativ einfach, als ein Benutzer entweder vollständigen Lese-/Schreibzugriff auf einen Ordner und dessen Inhalt besitzt oder in diesem Ordner nichts sehen kann.

Werden Berechtigungen übernommen, sind feinere Abstufungen möglich. Möglicherweise möchten Sie der Gruppe *Editors* Lesezugriff für den Ordner *Abgabe* gewähren, es aber weiterhin nur der Gruppe *Autoren* ermöglichen, Änderungen an Dateien vorzunehmen oder neue Dateien hinzuzufügen. Mithilfe der Vererbung kann dies umgesetzt werden. Weisen Sie der Gruppe *Editoren* Lesezugriff für den Ordner *Abgabe* zu. Die Benutzer erhalten dann durch die Vererbung auch Lesezugriff auf alle Dateien im Ordner *Abgabe*.

POSIX-Berechtigungen im Vergleich zu ACL-Einstellungen

ACLs bieten Ihnen die Möglichkeit, Zugriffseinstellungen genauer zu steuern, die darüber hinaus auch mit der Windows-Umgebung kompatibel sind. Für einen Ordner (oder Netzwerkordner) können in Server-Admin siebzehn zusätzliche Einstellungen vorgenommen werden. Dies bedeutet, dass für den Lese- und Schreibzugriff sowie für die administrative Steuerung umfassendere Einstellungen zur Auswahl stehen (etwa, wer die Berechtigungen oder den Eigentümer eines Ordners ändern kann). In Server-Admin werden diese Einstellungen für Ordner, nicht aber für einzelne Dateien aktiviert. Die enthaltenen Dateien können dann die Einstellungen der jeweiligen Ordner übernehmen. Diese Steuerung auf Ordnerebene ermöglicht eine feiner abgestufte Verwaltung ohne den Aufwand, der beim Verwalten von Berechtigungen für Tausende oder Millionen einzelner Dateien anfallen würde.

Die im Finder verfügbaren POSIX-Einstellungen sind auf Lesen & Schreiben, Nur Lesen, Nur Schreiben und Keine Rechte begrenzt. Im folgenden Dialogfenster werden die ACL-Einstellungen angezeigt, die in Server-Admin zur Verfügung stehen.



HINWEIS ► Zugriffssteuerungseinstellungen werden auf Basis von Behältern also Ordnern und Netzwerkordnern festgelegt, nicht aber für einzelne Dateien. Die enthaltenen Dateien übernehmen die jeweiligen ACL-Einstellungen der ihnen übergeordneten Ordner.

Die Vererbungskonfiguration bestimmt, welche Objekte die ACL-Einstellungen übernehmen, etwa der Ordner selbst, alle Dateien oder Ordner eine Stufe darunter oder alle Dateien oder Ordner innerhalb dieses Ordners. Die zu Beginn festgelegte Vererbungseinstellung gilt nur für danach erstellte Dateien und Ordner, doch Sie können diese Einstellungen manuell für untergeordnete Dateien oder Ordner übernehmen.

Funktionsweise von Dateisystem-ACLs

Wenn Sie ACLs mithilfe von Server-Admin definieren, erstellen sie einzelne *Zugriffssteuerungseinträge* (ACEs). Diese Einträge und Listen sind spezifisch für einen Speicherort im Dateisystem und werden für Container-Objekte – entweder Netzwerkordner oder Ordner – festgelegt. Jeder ACE enthält die folgenden Informationen:

- Der bzw. die diesem Eintrag zugeordnete Benutzer oder Gruppe
- Eintragstyp (Erlauben oder Ablehnen)
- Berechtigungen (VOLLSTÄNDIGE STEUERUNG, LESEN & SCHREIBEN, LESEN, SCHREIBEN oder ANGEPASST zusammen mit Vererbungseinstellungen)

Die Reihenfolge der Einträge ist wichtig, da Listen von Mac OS X Server von oben nach unten ausgewertet werden.

Treffer für ERLAUBEN und ABLEHNEN verhalten sich bei ACLs unterschiedlich. Treffer für ERLAUBEN sind kumulativ für den Benutzer, egal ob es sich um Treffer auf Benutzer- oder Gruppenebene handelt. Treffer für ABLEHNEN wirken beim ersten Auftreten.

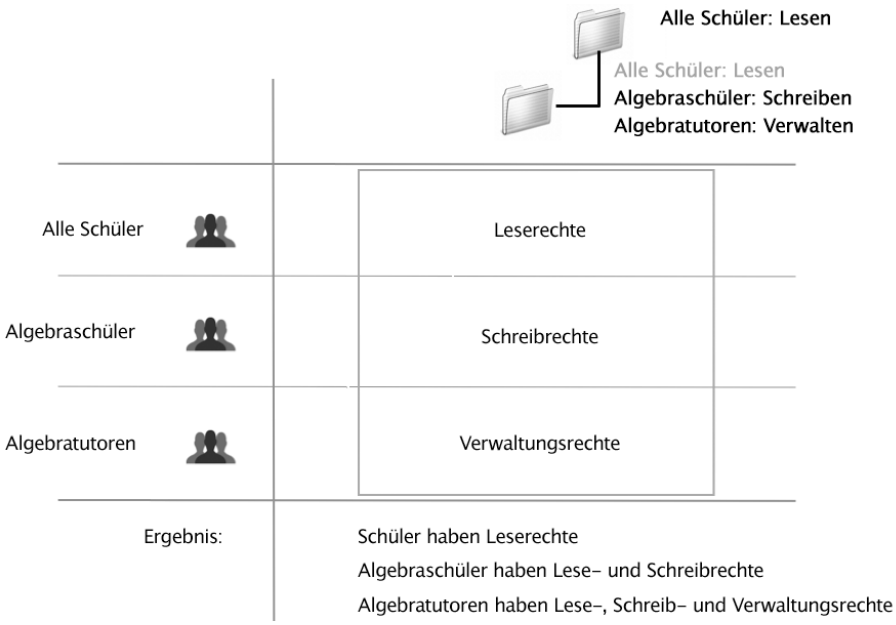
Die ACLs einer Datei ändern sich nicht, wenn Sie eine Datei aus einem Ordner in einen anderen Ordner auf demselben Volume bewegen. Die Datei wird in dieser Situation nicht kopiert und gelöscht. Stattdessen wird der Zeiger geändert, der auf den Speicherort der Datei verweist. Bewegen Sie die Datei auf ein anderes Volume, wird die Datei kopiert und gelöscht und übernimmt die ACLs des neuen übergeordneten Ordners.

Kumulativer Zugriff »Erlauben«

Gehen Sie in der folgenden Abbildung davon aus, dass die Algebratutoren die Rechte der Algebraschüler und die Algebraschüler wiederum die Rechte der Schüler erben. Der Ordner verfügt über drei Einträge in der ACL:

- Alle Schüler können den Inhalt des Ordners lesen (vom übergeordneten Ordner übernommen).
- Algebraschüler können in den Ordner schreiben.
- Algebratutoren können den Ordner verwalten.

Alle Schüler in der Schule können den gewählten Ordner und die Dateien in diesem Ordner sehen. Die Algebraschüler besitzen Schreibzugriff, da sie der Gruppe *Algebraschüler* angehören, verfügen aber auch über Lesezugriff, da sie Mitglieder der Gruppe *Alle Schüler* sind. Die Algebraschüler besitzen also Lese- und Schreibzugriff. Die Algebratutoren, die beiden Gruppen übergeordnet sind, können lesen, schreiben und administrative Änderungen vornehmen, wie etwa Berechtigungen oder Eigentümer ändern.



Beachten Sie, dass übernommene Berechtigungen für den kumulativen Zugriff ERLAUBEN berücksichtigt werden müssen. Algebraschüler und Algebratutoren erhalten aufgrund ihrer Mitgliedschaft in der Gruppe *Alle Schüler* Leserechte. Falls Sie das nicht beabsichtigten, können Sie die übernommenen Rechte mithilfe des Arbeitsgruppenmanagers für den Ordner entfernen.

Nehmen wir nun einmal an, im Ordner *Mathe* befindet sich ein Ordner mit Schülerbewertungen. Es ist wichtig, dass kein Schüler Zugriff auf diesen Ordner oder dessen Inhalt erhält. Beachten Sie, dass Schüler aufgrund der Vererbung im Normalfall Lesezugriff auf diesen Ordner erhalten. Damit die Schüler nicht auf den Ordner zugreifen können, können Sie für den Ordner die Zugriffssteuerung ABLEHNEN für die Gruppe *Alle Schüler* festlegen. Diese Zugriffssteuerung sollte sich oberhalb der Zugriffssteuerungen ERLAUBEN befinden, da die ACEs von oben nach unten ausgewertet werden.

Die Zugriffssteuerung ABLEHNEN ganz oben überschreibt alle anderen Zugriffssteuerungen des Ordners für die jeweilige Gruppe. Obwohl Algebratutoren einen Lesezugriff-ACE (durch ihre Mitgliedschaft in der Gruppe *Schüler*), einen Schreibzugriff-ACE (durch ihre Mitgliedschaft in der Gruppe *Algebraschüler*) und einen Administratorzugriff-ACE (durch ihre Mitgliedschaft in der Gruppe *Algebratutoren*) besitzen, überschreibt die für alle Schüler geltende Zugriffssteuerung ABLEHNEN alle diese ACEs. Grund hierfür ist, dass sie ganz oben in der Liste platziert ist, sodass kein Schüler auf diesen Ordner zugreifen kann.

Gruppenmitgliedschaft und ACLs

Die Steuerung des Zugriffs auf Serverressourcen mithilfe von ACLs kann äußerst nützlich sein, sofern Sie von Anfang an darauf achten, Ihre Benutzer- und Gruppenaccounts entsprechend zu verwalten. Hierfür wird empfohlen, mit kleineren Gruppen zu arbeiten, um die Anforderungen Ihrer Organisation korrekt zu simulieren und u. a. Gruppen innerhalb anderer Gruppen zu verschachteln. Verwenden Sie diese Gruppenaccounts, um den Zugriff auf einer Basis mit erhöhter Granularität zu verwalten.

Sie könnten für das Beispiel der Schule eine Gruppe für alle Lehrer erstellen, die aus zwei Gruppen besteht: Lehrer und Referendare. Anschließend können Sie beide Gruppen unabhängig voneinander verwalten und wie erforderlich Zugriffsrechte zuweisen. Wird aus einem Referendar schließlich ein fertig ausgebildeter Lehrer, können Sie den Account des Referendars einfach in die Gruppe der Lehrer bewegen. So können Sie die Verwaltung auf Gruppen-/Organisationsbasis fortsetzen und müssen keine Zugriffssteuerungseinträge für einzelne Lehrer verwalten, was ziemlich aufwändig ist.

Konfiguration der Zugriffssteuerung

In diesem Abschnitt erstellen Sie eine Ordnerhierarchie und erarbeiten eine Möglichkeit, den Zugriff zu steuern, um den Arbeitsablauf der Benutzer und Gruppen auf Ihrem Server zu vereinfachen. Sie verwenden nur Dateisystem-ACLs und vollziehen die Schritte eines Beispielprojekts nach. Sie lernen, dass die Möglichkeit, eine Datei zu bearbeiten, durch ihren Speicherort im System bestimmt wird und nicht durch den Autor oder Eigentümer der Datei.

Denken Sie unbedingt daran, dass die Änderungen nur dann übernommen werden, wenn Sie sie sichern. Es empfiehlt sich, Ihre Arbeit häufig zu sichern.

Damit Sie Ihren Server richtig konfigurieren können, müssen Sie den voraussichtlichen Arbeitsablauf Ihrer Benutzer kennen. Sie haben die zwei Gruppen *Engineering* und *Marketing* eingerichtet. Beide Gruppen benötigen zu bestimmten Zeitpunkten im Verlauf des Projekts unterschiedliche Zugriffsrechte auf Dateien. In dieser Übung fügen Sie neue Gruppen zum Szenario hinzu: die Gruppe *Projects* und die Gruppe *Contractors*.

Erstellen der Ordnerstruktur

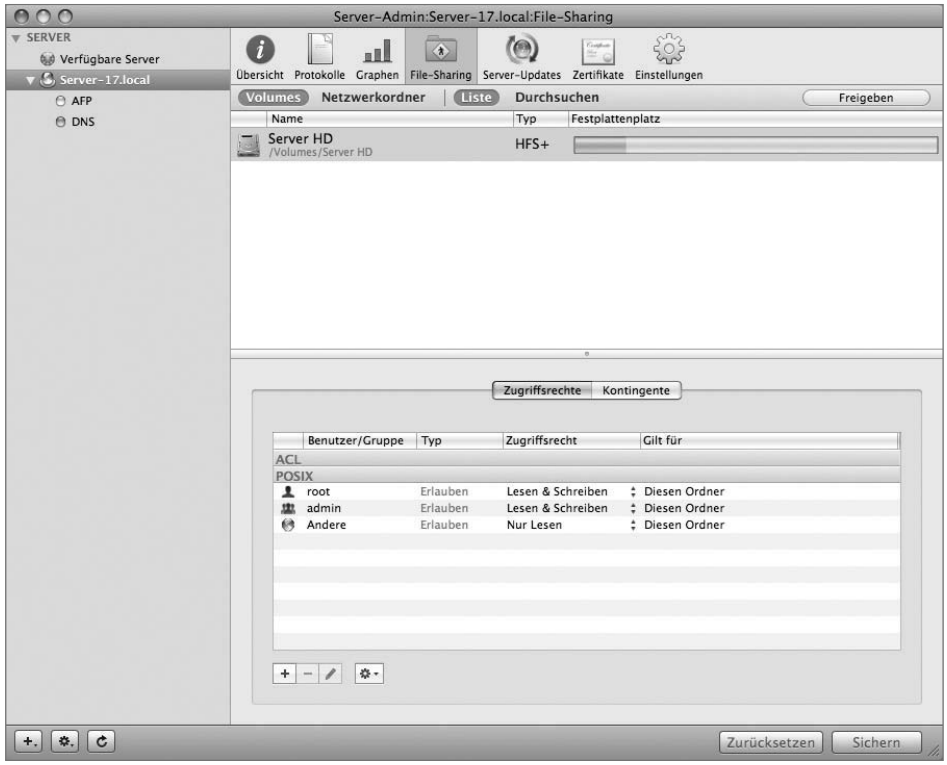
In dem in dieser Lektion verwendeten Beispiel ist die Ordnerstruktur projektbasiert, nicht abteilungsbasiert. Sobald ein Dokument bestimmte Anforderungen erfüllt, wird es vom bisherigen Speicherort an einen anderen bewegt. Sie erstellen Projektordner und verwenden für diese Ordner ACLs, um den Arbeitsablauf zu steuern. Diese Vorgehensweise unterscheidet sich ggf. von Ihrer Dokumentverwaltung mithilfe von POSIX-Berechtigungen.

Der erste Schritt besteht darin, eine Hierarchie für die Projektordner anzulegen. Sie können die Ordner im Finder erstellen, können aber auch Server-Admin verwenden. Mit Server-Admin haben Sie die Möglichkeit, Ordner per Fernzugriff auf Ihrem Server zu erstellen, ohne physisch darauf zuzugreifen.

1. Öffnen Sie Server-Admin auf dem Client-Computer und stellen Sie eine Verbindung zum Server her.

2. Klicken Sie auf die Taste FILE-SHARING in der Symbolleiste des Arbeitsgruppenmanagers.

Im Hauptfenster werden die Volumes oder die aktuellen Netzwerkordner angezeigt, entweder als Liste oder in der Spaltenansicht DURCHSUCHEN. Außerdem sind die jeweils zugewiesenen Eigentümer und Gruppen sowie die Zugriffsrechte zu sehen.

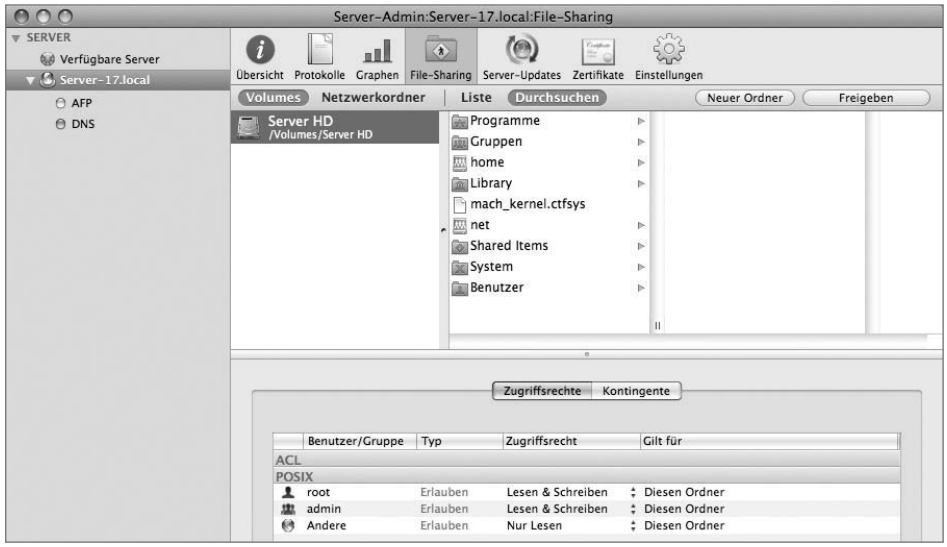


3 Klicken Sie auf VOLUMES und dann auf DURCHSUCHEN.

In dieser Ansicht können Sie auf der lokalen Festplatte navigieren und Berechtigungen für Ordner festlegen, die nicht in einem Netzwerkordner enthalten sind.

4 Wählen Sie in der linken Spalte das Startvolume aus.

Im vorliegenden Beispiel lautet der Name des Volumes *Server HD*.



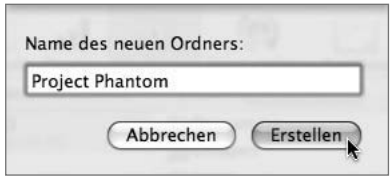
5 Klicken Sie auf den Ordner *Shared Items* in der Liste der Ordner.

6 Klicken Sie auf die Taste NEUER ORDNER oben rechts im Fenster.

Damit wird ein neuer Ordner innerhalb des Ordners *Shared Items* erstellt.

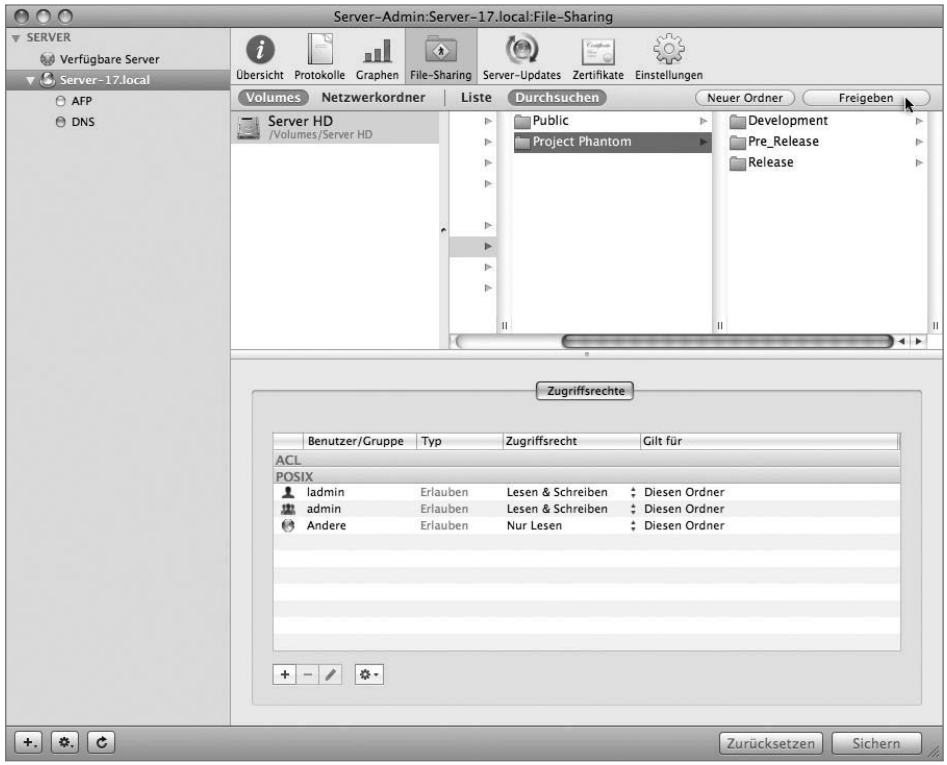
7 Geben Sie in das Namensfeld den Namen *Project Phantom* ein.

Dieser Ordner wird für die Produktentwicklung verwendet.



8 Erstellen Sie innerhalb des neuen Ordners drei Unterordner: *Development*, *Pre_Release* und *Release*.

HINWEIS ► Wenn Sie die Auswahl des übergeordneten Ordner nicht aufheben und ihn dann erneut auswählen, werden danach erstellte Ordner im neu angelegten Ordner verschachtelt.



9 Wählen Sie den Ordner *Project Phantom* ggf. erneut aus und klicken Sie oben rechts auf die Taste FREIGEBEN.

HINWEIS ► Heben Sie vor dem Klicken auf die Taste FREIGEBEN die Auswahl des Ordners *Project Phantom* erneut auf und wählen Sie ihn dann wieder aus. So vermeiden Sie, dass Sie nur einen der neu erstellten Unterordner des Ordners freigeben.

10 Klicken Sie auf SICHERN.

Damit wird der Ordner *Project Phantom* in einen Netzwerkordner umgewandelt, der von Ihren Benutzern aktiviert werden kann.

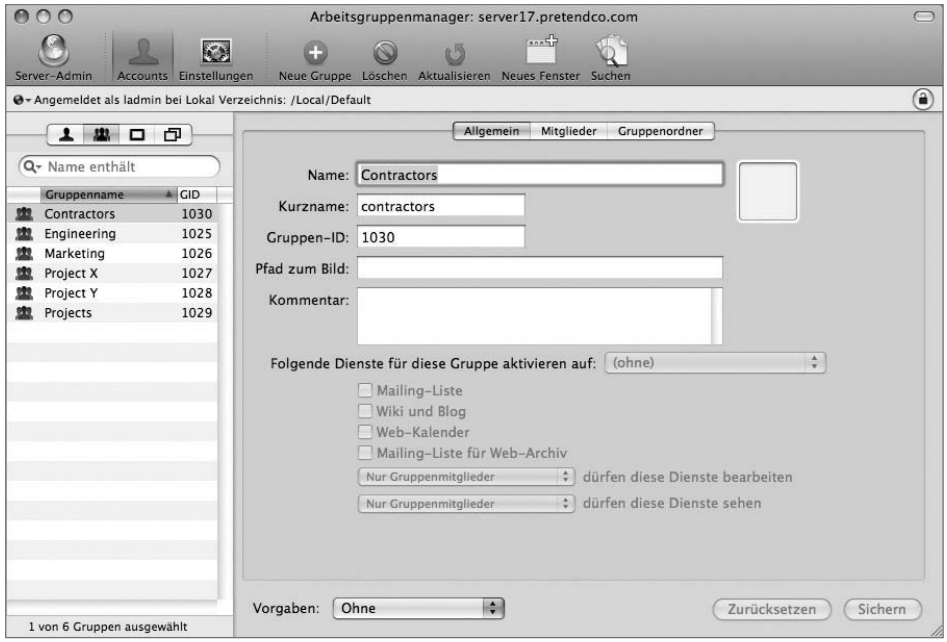
Erstellen zusätzlicher Gruppen und Entfernen eines Mitglieds aus einer Gruppe

Wie zuvor erwähnt verwenden Sie in dieser Übung nicht nur die vorhandenen Gruppen *Marketing* und *Engineering*, sondern erstellen noch zwei zusätzliche Gruppen: *Projects* und *Contractors*. Diese Gruppen sind für Projektmanager und temporäre Mitarbeiter gedacht. Sorgen Sie außerdem dafür, dass der Benutzer Warren nur Mitglied der Gruppe *Engineering* und nicht der Gruppe *Marketing* ist, um die sich ändernden Zugriffsrechte zeigen zu können.

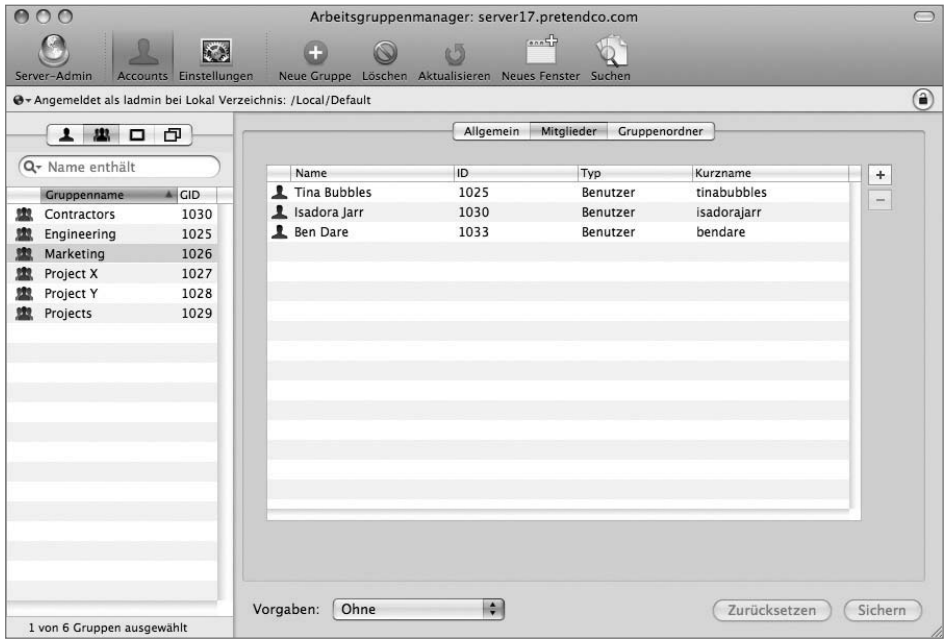
1 Kehren Sie zum Arbeitsgruppenmanager zurück und stellen Sie falls erforderlich wieder eine Verbindung zum Server her.

2 Klicken Sie in der Symbolleiste auf ACCOUNTS und klicken Sie links auf das Symbol GRUPPEN. Erstellen Sie dann die zwei neuen Gruppen *Projects* und *Contractors*. Verwenden Sie beim Erstellen der Gruppen einfach deren Standardeinstellungen.

   Die Gruppen bleiben vorerst leer, Sie fügen später Benutzer hinzu.



3 Wählen Sie die Gruppe *Marketing* aus.



4 Entfernen Sie Isadora Jarr aus der Gruppe *Marketing*, falls sie Mitglied ist, indem Sie sie auswählen und auf die Taste ENTFERNEN (–) klicken. Klicken Sie dann auf SICHERN.

Festlegen von Eigentümer und Zugriffsrechten für die Ordner *Development*

Nachdem Sie nun die Ordnerstruktur erstellt haben, müssen Sie allen Ordnern Gruppeneigentümer und Zugriffsrechte zuweisen.

1 Kehren Sie zu Server-Admin zurück und stellen Sie falls erforderlich wieder eine Verbindung zum Server her.

2 Klicken Sie in der Symbolleiste auf FILE-SHARING und wählen Sie den Ordner *Development* aus. Haben Sie das Fenster zuvor geschlossen, müssen Sie im Netzwerkordner *Project Phantom* zu diesem Ordner navigieren.

Den Einträgen in den Feldern im Bereich ZUGRIFFSRECHTE lässt sich entnehmen, dass der Benutzer *ladmin* der derzeitige Eigentümer des Ordners ist und *admin* die dem Ordner zugewiesene Gruppe.

Bei der Gruppe *admin* handelt es sich um einen Gruppenaccount, der bei der Installation von Mac OS X Server erstellt wird. Der root-Account, auch als Systemadministrator- oder Superuser-Account bezeichnet, wird ebenfalls bei der Installation von Mac OS X Server erstellt. Da es sich um einen Account auf Systemebene handelt, wird er nicht in der Liste der Benutzeraccounts im Bereich ACCOUNTS aufgelistet, sondern in der Liste BENUTZER im Fach BENUTZER UND GRUPPEN.

In der folgenden Abbildung ist zu sehen, dass der Eigentümer *ladmin* Lese- und Schreibzugriff auf diesen Ordner besitzt, ebenso wie Mitglieder der Gruppe *admin*. Die Berechtigung für *Andere* ist auf NUR LESEN eingestellt.

Für den Ordner *Development* werden in dieser Übung vorerst die POSIX-Berechtigungen übernommen, um die Vorteile von ACLs aufzuzeigen. Denken Sie daran, nun kommen die Gruppe *Contractors* und deren zugehörige Benutzer ins Spiel.

3 Klicken Sie auf die Taste HINZUFÜGEN (+), um das Fach BENUTZER UND GRUPPEN zu öffnen.

Bewegen Sie jetzt Benutzer und Gruppen in die Liste *POSIX* im Bereich ZUGRIFFSRECHTE, um die vorhandenen Berechtigungen zu ersetzen:

- Weisen Sie die Eigentümerrechte des Ordners *Development* dem Benutzer *Warren* zu, indem Sie Warren zum Symbol des einzelnen Benutzers bewegen, für das bisher der Benutzer *ladmin* definiert ist.
- Weisen Sie die Gruppenrechte des Ordners *Development* der Gruppe *Engineering* zu, indem Sie die Gruppe zum Symbol der mehreren Benutzer bewegen, für das bisher die Gruppe *admin* definiert ist.
- Legen Sie für die Rechte von *Andere* für den Ordner *Development* die Einstellung OHNE fest, indem Sie diese Einstellung aus dem Einblendmenü in der Spalte ZUGRIFFSRECHT auswählen.

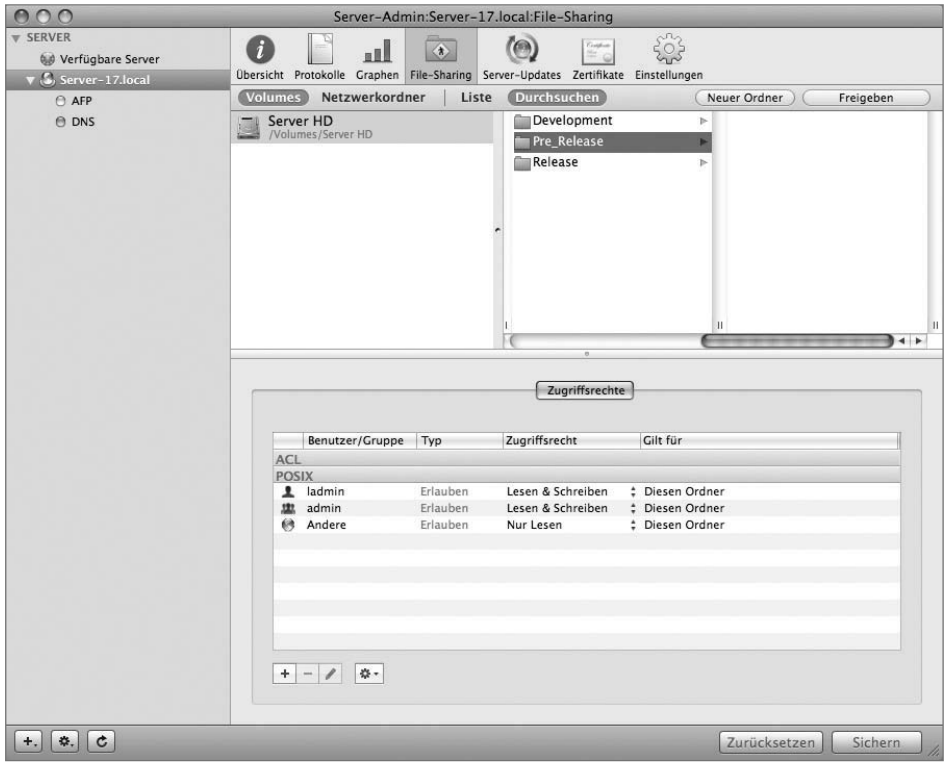
4 Klicken Sie auf SICHERN.

Können die Mitglieder der Gruppe *Contractors* auf den Ordner *Development* zugreifen, wenn deren Eigentümer Warren Peece ist, der zur Gruppe *Engineering* gehört, und wenn für *Andere* das Zugriffsrecht OHNE festgelegt ist? Nein. Dazu müssten diese Benutzer zur Gruppe *Engineering* hinzugefügt werden oder für *Andere* müsste ein Zugriffsrecht definiert werden. Welche POSIX-Berechtigungen müssten Sie festlegen, um den Benutzern Zugriff zu gewähren? Für *Andere* müsste Lese- und Schreibzugriff definiert werden.

Festlegen der Zugriffssteuerung für den Ordner *Pre_Release*

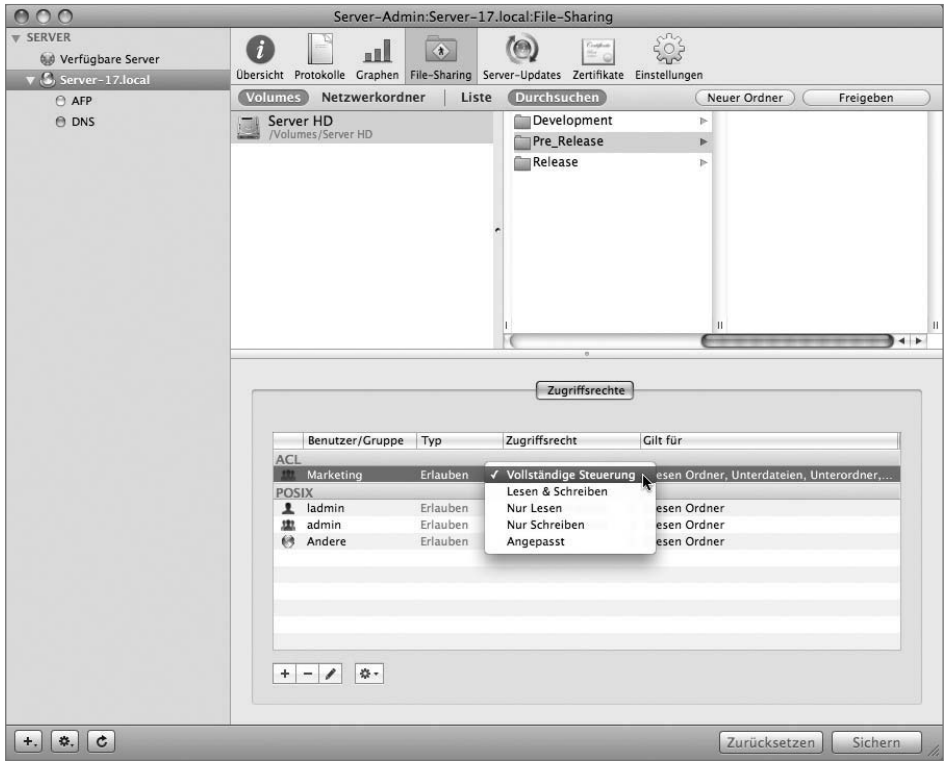
Für den Ordner *Pre_Release* verwenden Sie anstelle von POSIX-Berechtigungen eine ACL.

1 Klicken Sie in der Symbolleiste auf FILE-SHARING und wählen Sie den Ordner *Pre_Release* im Netzwerkordner *Project Phantom* aus.



2 Klicken Sie auf die Taste HINZUFÜGEN (+), um das Fach BENUTZER UND GRUPPEN zu öffnen. Bewegen Sie dann die Gruppe *Marketing* in die Liste *ACL* im Bereich ZUGRIFFSRECHTE. Klicken Sie auf SICHERN.

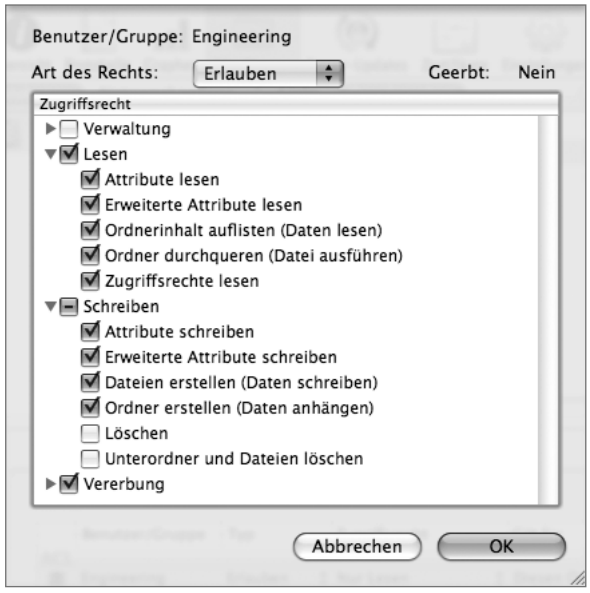
3 Wählen Sie den Eintrag *Marketing* in der Liste *ACL* aus und weisen Sie der Gruppe *Marketing* in der Spalte ZUGRIFFSRECHT vollständige Steuerung zu.



4 Bewegen Sie die Gruppe *Engineering* aus der Liste *Gruppen* in die Liste *ACL*. Klicken Sie auf SICHERN.

5 Wählen Sie die Gruppe *Engineering* in der Liste *ACL* aus und weisen Sie das Zugriffsrecht ANGEPASST zu, das Lesen und Schreiben, aber nicht das Löschen von Dateien oder Ordnern ermöglicht. Klicken Sie auf OK.

Damit haben Sie der Gruppe *Engineering* die vollständige Steuerung erlaubt, Gruppenmitglieder können allerdings keine Objekte entfernen.



6 Klicken Sie auf OK und anschließend auf SICHERN.

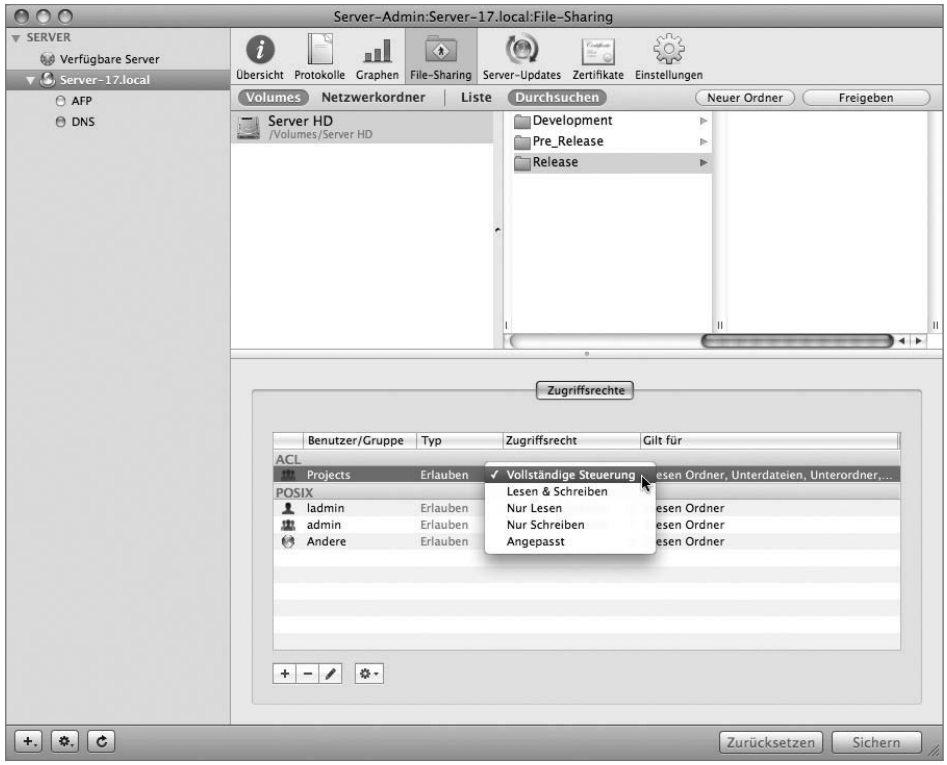
Festlegen von Zugriff und Berechtigungen für den Ordner *Release*

Wie für den Ordner *Pre_Release* müssen Sie auch für den Ordner *Release* die Zugriffssteuerung festlegen. Der Ordner *Release* soll der Gruppe *Projects* angehören. Sie müssen dieser Gruppe keine Mitglieder zuweisen, um den Zugriff festzulegen. Der gesamte Zugriff wird wie beim Ordner *Pre_Release* über die ACLs bestimmt. Möchten Sie später Zugriff auf diesen Ordner gewähren, können Sie zu den Ordner-ACLs Benutzer oder Gruppen hinzufügen.

1 Klicken Sie in der Symbolleiste auf FILE-SHARING und wählen Sie den Ordner *Release* aus.

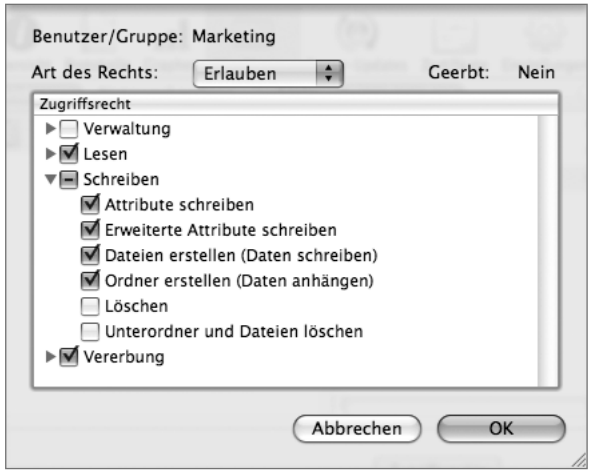
2 Klicken Sie im Fach BENUTZER UND GRUPPEN auf die Taste GRUPPEN und bewegen Sie die Gruppe *Projects* in die Liste *ACL* im Bereich ZUGRIFFSRECHTE. Klicken Sie auf SICHERN.

3 Wählen Sie den Eintrag *Projects* in der Liste *ACL* aus und weisen Sie der Gruppe *Projects* die VOLLSTÄNDIGE STEUERUNG zu.



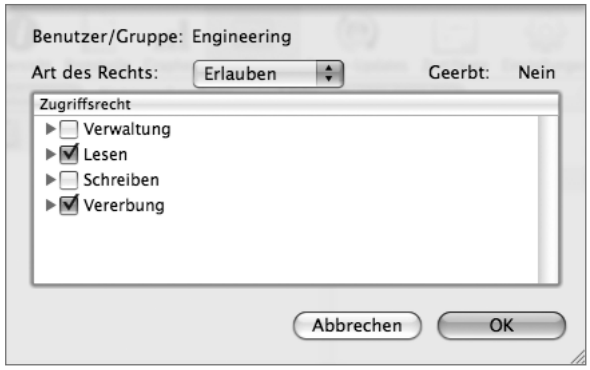
4 Bewegen Sie die Gruppe *Marketing* in die Liste *ACL*.

5 Wählen Sie den Eintrag *Marketing* in der Liste aus und weisen Sie das Zugriffsrecht ANGEPASST zu, das Lesen und Schreiben, aber nicht das Löschen von Dateien oder Ordnern ermöglicht. Klicken Sie auf OK.



6 Bewegen Sie die Gruppe *Engineering* in die Liste *ACL*.

7 Wählen Sie den Eintrag *Engineering* in der Liste *ACL* durch Doppelklicken aus und klicken Sie auf OK, um der Gruppe *Engineering* Lesezugriff zu gewähren.



8 Klicken Sie auf SICHERN.

Hinzufügen neuer Benutzer

Nachdem Sie die Ordnerstruktur angelegt haben, erstellen Sie nun zwei weitere Benutzer und weisen sie Gruppen zu, wie es zu Beginn der Lektion im Abschnitt »Konfigurieren lokaler Benutzeraccounts« beschrieben wurde:

- Projektmanager *Pamela Clarke*, Kurzname *pclarke*, Kennwort *pclarke* in der Gruppe *Projekte*
- Auftragnehmer *Mike Smith*, Kurzname *msmith*, Kennwort *msmith* in der Gruppe *Contractors*

Starten des Dateiservers

Nachdem nun ein Netzwerkordner erstellt wurde, muss der Dateiserver gestartet werden, falls nicht bereits geschehen.

1 Wählen Sie in Server-Admin den AFP-Dienst links im Fenster aus.

2 Klicken Sie unten auf AFP STARTEN.

Betrachten des Arbeitsablaufs

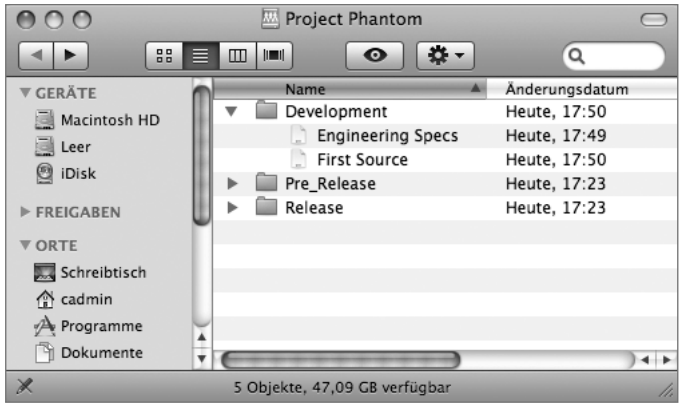
Der Server wurde nun mit den korrekten Projektordnern und den entsprechenden Benutzern und Gruppen konfiguriert. Im nächsten Schritt erstellen Sie Dokumente und beobachten den Zugriff auf diese Dateien während eines standardmäßigen Arbeitsablaufs.

1 Stellen Sie vom Client-Computer als Warren eine Verbindung zum Server her.

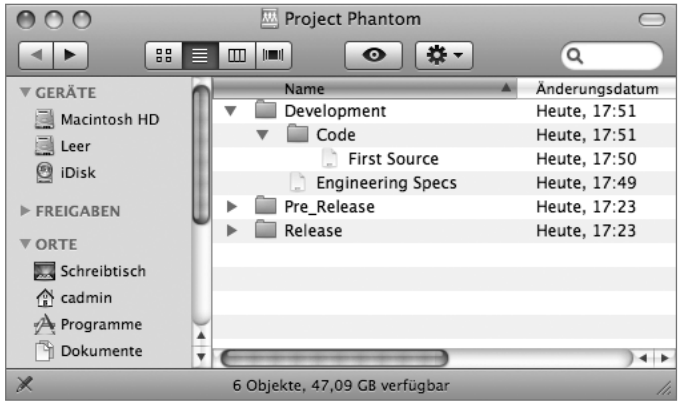
2 Wählen Sie den Netzwerkordner *Project Phantom* aus. Klicken Sie auf OK.

3 Erstellen Sie mithilfe von TextEdit zwei Textdateien mit den Namen *Engineering Spec* und *First Source* und legen Sie diese im Ordner *Development* ab.

Warren verfügt über uneingeschränkte Zugriffsrechte für den Ordner *Development*.

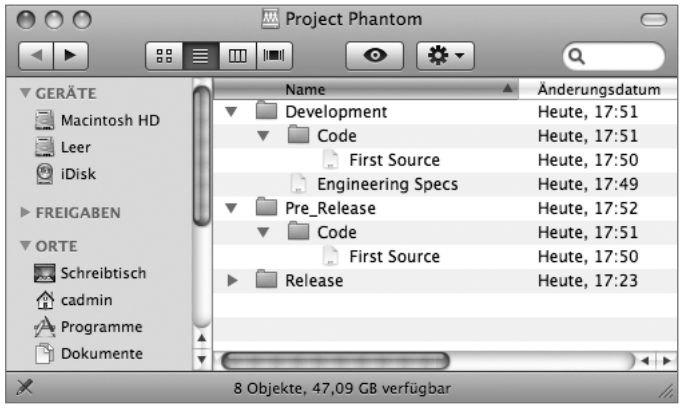


4 Erstellen Sie innerhalb des Ordners *Development* einen Unterordner mit der Bezeichnung *Code* und bewegen Sie die Datei *First Source* in diesen Unterordner.



5 Bewegen Sie den Ordner *Code* bei gedrückter Wahltaste aus dem Ordner *Development* in den Ordner *Pre_Release*.

Dabei wird der Ordner und dessen Inhalt kopiert, anstatt bewegt.



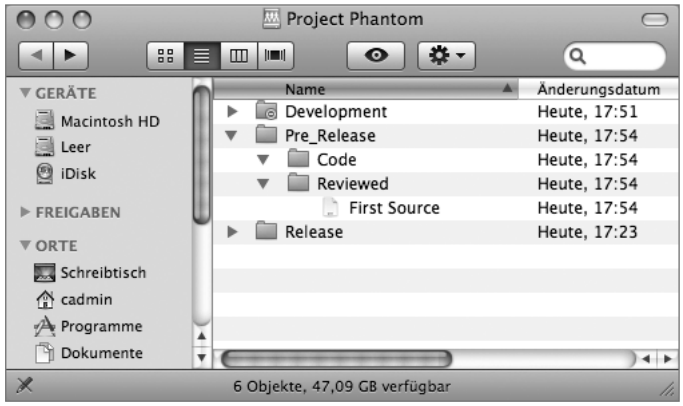
6 Trennen Sie die Verbindung als Warren und stellen Sie sie als Tina Bubbles erneut her.

7 Zeigen Sie die Berechtigungen für die Dateien im Ordner *Development* an.

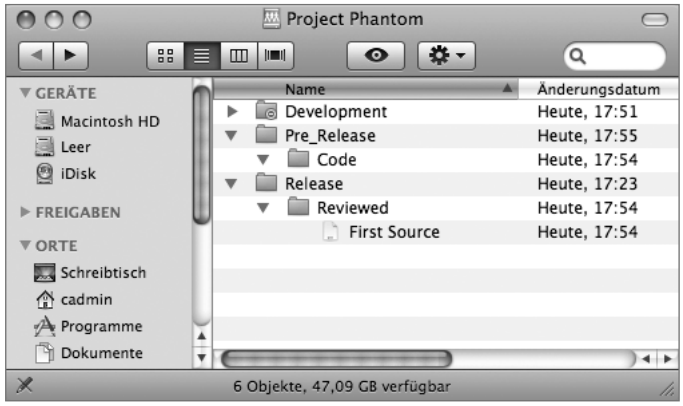
Als Mitglied der Gruppe *Marketing* hat Tina derzeit keinen Zugriff auf den Ordner *Development*. Da für den Ordner *Development* keine ACLs vorhanden sind und Tina nicht Mitglied der Gruppe *Engineering* ist, kann sie die Dateien im Ordner *Development* nicht sehen.

8 Zeigen Sie die Dateien im Ordner *Pre_Release* an.

9 Bearbeiten Sie die Datei *First Source*, indem Sie Text hinzufügen und die Datei in einem neuen Ordner mit der Bezeichnung *Reviewed* sichern.



10 Bewegen Sie den Ordner *Reviewed* aus dem Ordner *Pre_Release* in den Ordner *Release*.



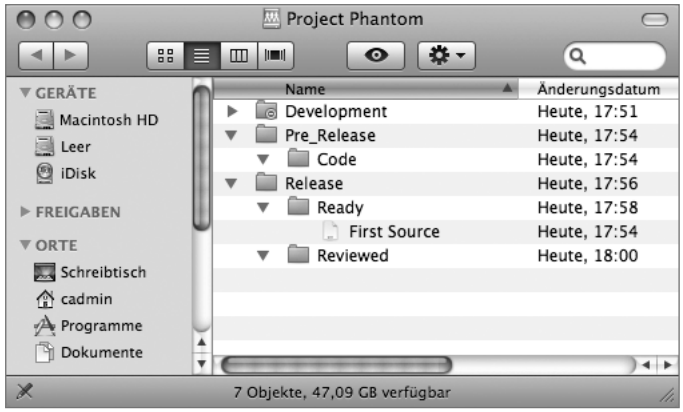
Damit wird verdeutlicht, dass das Projekt zur Produktion freigegeben ist.

11 Trennen Sie die Verbindung als Tina und stellen Sie sie als Pamela Clarke erneut her.

12 Zeigen Sie die Dokumente in den anderen Ordnern an.

13 Erstellen Sie innerhalb des Ordners *Release* einen neuen Ordner mit der Bezeichnung *Ready* und bewegen Sie die Datei *First Source* dort hinein.

Die anderen Gruppen sollten weiterhin Lesezugriff auf den Ordner *Ready* besitzen. Zeigen Sie die Datei- und Ordnerinformationen im Finder an, indem Sie den Befehl INFORMATIONEN verwenden.

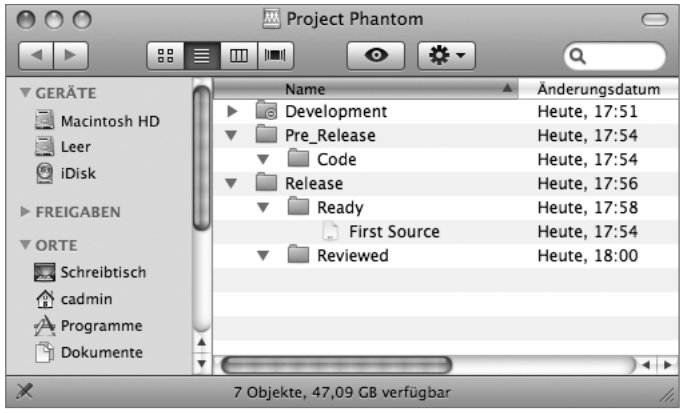


Hinzufügen von Gruppen zum Zugriffspfad

Sie haben jetzt die grundlegenden Zugriffsrechte für die Programmordner eingerichtet und gesehen, wie sich der Zugriff ändert, wenn ein Dokument oder Ordner von einem übergeordneten Objekt in ein anderes bewegt wird. Im nächsten Schritt fügen Sie Gruppen zu Gruppen hinzu und beobachten, welche Auswirkungen das auf den Zugriff hat.

1 Trennen Sie die Verbindung als Pamela und stellen Sie sie als der Auftragnehmer Mike Smith wieder her.

2 Überprüfen Sie, ob Sie auf die Daten in den Ordnern *Pre_Release* und *Release* zugreifen können.



3 Melden Sie sich als Mike Smith ab.

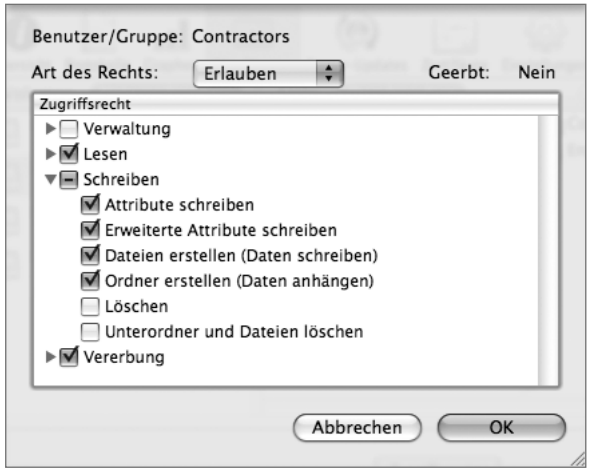
4 Öffnen Sie Server-Admin, klicken Sie auf FILE-SHARING und navigieren Sie in der Liste *Netzwerkordner* zum Ordner *Development*.

5 Klicken Sie auf die Taste HINZUFÜGEN (+) und dann auf die Taste GRUPPEN im Fach BENUTZER UND GRUPPEN.

6 Bewegen Sie die Gruppe *Engineering* in die Liste *ACL* und weisen Sie ihr das Recht VOLLSTÄNDIGE STEUERUNG zu. Klicken Sie auf SICHERN.

Sie haben ACLs zum Ordner *Development* hinzugefügt. Jetzt weisen Sie der Gruppe *Contractors* Zugriff auf den Ordner *Development* zu.

7 Bewegen Sie die Gruppe *Contractors* in die Liste *ACL* und gewähren Sie Lese- und Schreibzugriff, ohne das Löschen von Dateien oder Ordnern zu erlauben. Hierfür verwenden Sie die Einstellung ANGEPASST.



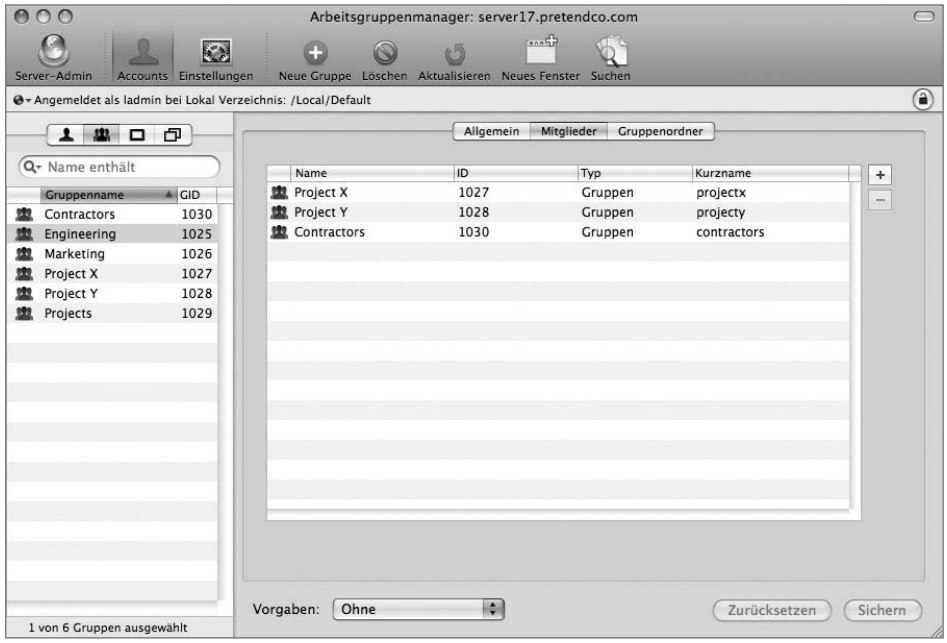
8 Klicken Sie auf SICHERN.

Hinzufügen der Berechtigung des Typs »Ablehnen«

Sie haben der Gruppe *Contractors* Zugriff auf den Ordner *Development* gewährt. (Die Gruppen *Marketing* und *Projects* besitzen immer noch keinen Zugriff.) Eine einfache Möglichkeit hierfür wäre gewesen, die Gruppe *Contractors* zur Gruppe *Engineering* hinzuzufügen, nachdem die ACLs für die Gruppe *Development* festgelegt waren. Dann hätten allerdings die Mitglieder der Gruppe *Contractors* zusätzliche Rechte erhalten, die Sie ihnen nicht geben möchten. Mit der Berechtigung ABLEHNEN können Sie Benutzer und Gruppen einschränken und so Ihr gewünschtes Berechtigungsmodell besser abstufen.

1 Klicken Sie im Arbeitsgruppenmanager auf ACCOUNTS und dann auf die Taste GRUPPEN.

2 Fügen Sie die Gruppe *Contractors* zur Gruppe *Engineering* hinzu, indem Sie auf die Taste HINZUFÜGEN (+) klicken und die Gruppe in die Liste im Bereich MITGLIEDER der Gruppe *Engineering* bewegen. Klicken Sie anschließend auf SICHERN.



3 Klicken Sie in Server-Admin auf FILE-SHARING und navigieren Sie zum Ordner *Pre_Release*.

4 Klicken Sie auf die Taste HINZUFÜGEN (+) und dann auf die Taste GRUPPEN im Fach BENUTZER UND GRUPPEN.

5 Bewegen Sie die Gruppe *Contractors* in der Liste *ACL* nach oben.

6 Wählen Sie die Gruppe *Contractors* durch Doppelklicken aus, wählen Sie ABLEHNEN aus dem Einblendmenü ART DER ZUGRIFFSRECHTE aus und klicken Sie dann auf OK.

7 Klicken Sie auf SICHERN.

Obwohl die Gruppe *Contractors* nun normalerweise Zugriff hätte, da sie der Gruppe *Engineering* angehört, ist ihr der Zugriff nicht möglich.

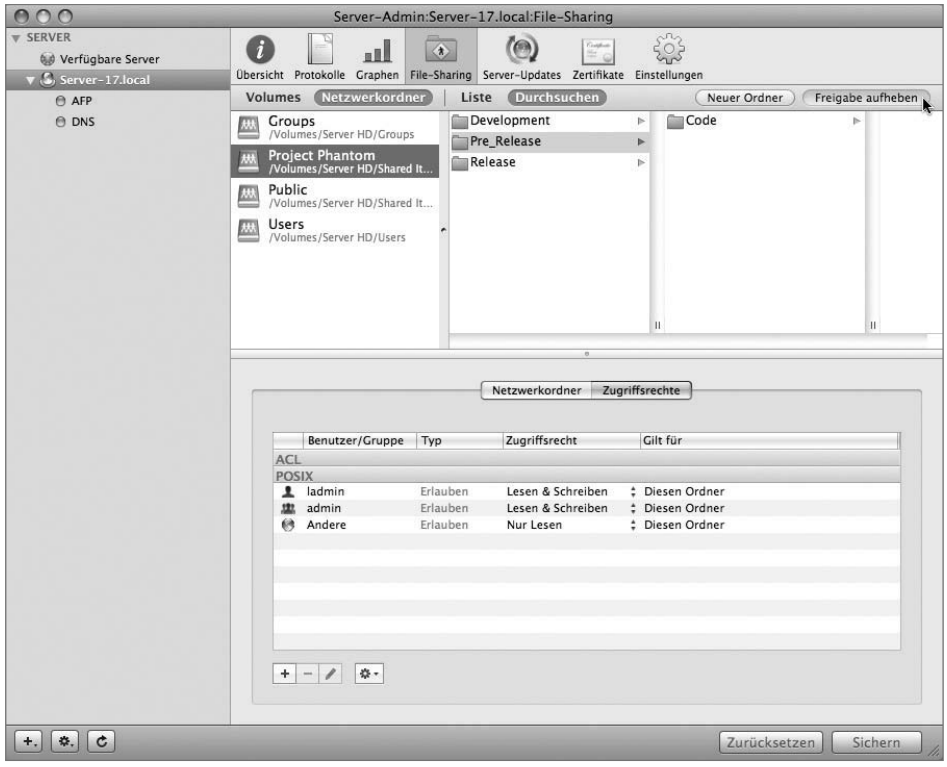
In dieser Übung werden die ACLs für den Ordner *Release* nicht geändert. Nehmen Sie sich die Zeit, sich mit verschiedenen Benutzernamen anzumelden und zu beobachten, wie sich Ihre Berechtigungen jeweils ändern. Der Gruppe *Contractors* wurde der Zugriff auf den Ordner *Pre_Release* verweigert, doch über die Gruppe *Engineering* wurde Zugriff auf Dokumente im Ordner *Release* gewährt.

Aufräumen von Ordnern auf dem Server

Sie haben den Ordner *Project Phantom* erstellt und gesehen, wie der Arbeitsablauf aussehen kann, wenn Dokumente von einem Ordner in andere bewegt werden. Jetzt können Sie den Ordner vom Server löschen.

1 Öffnen Sie Server-Admin auf dem Client-Computer und stellen Sie eine Verbindung zum Server her.

2 Klicken Sie in der Symbolleiste des Arbeitsgruppenmanagers auf FILE-SHARING und wählen Sie den Netzwerkordner *Project Phantom* aus. Klicken Sie dann oben rechts auf FREIGABE AUFHEBEN und klicken Sie anschließend auf SICHERN.



3 Beenden Sie Server-Admin.

4 Löschen Sie im Finder auf dem Server den Ordner *Project Phantom*.

Steuern des Zugriffs auf Ihren Server

Neben ACLs des Dateisystems unterstützt Mac OS X Server auch *ACLs für Dienste* (SACLs, Service Access Control Lists), die sich hinsichtlich Implementierung und Zweck von ACLs des Dateisystems unterscheiden, trotz ihrer ähnlichen Bezeichnungen. Mithilfe von SACLs können Sie festlegen, wer unter Mac OS X Server auf bestimmte Dienste zugreifen kann. Sie können mit SACLs Benutzern beispielsweise die Anmeldung über AFP-Verbindungen erlauben, SSH-Verbindungen (Secure Shell) aber auf Administratoren beschränken.

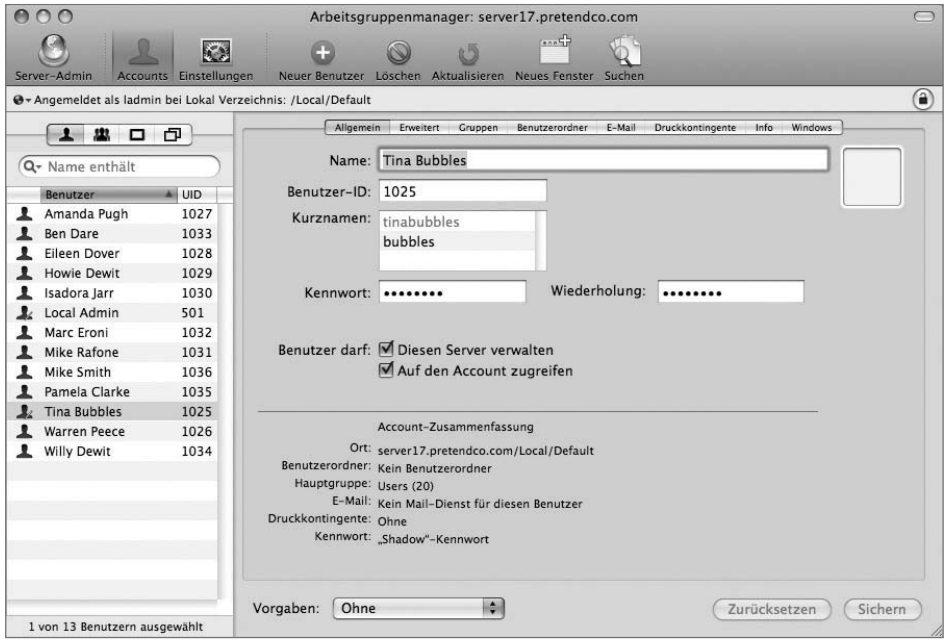
SACLs werden einfach durch die Mitgliedschaft in einer speziell benannten Gruppe gespeichert. Die SSH-SACL wird beispielsweise durch die Mitgliedschaft in der Gruppe *com.apple.access_ssh* gesteuert. Nach der Konfiguration von SACLs sind auf Ihrem System möglicherweise ähnlich benannte Gruppen vorhanden. In den meisten Fällen sollten Sie diese Gruppen nicht bearbeiten, sondern stattdessen mit Server-Admin SACLs wie in den Lektionen zu den jeweiligen Diensten in diesem Buch beschrieben definieren. Zum Bearbeiten von SACLs benötigen Sie Administratorzugriff auf den Server.

Umwandeln eines Benutzers in einen Administrator

Wie zuvor erwähnt, verwenden Sie den Arbeitsgruppenmanager, um einen Benutzer als Administrator zu definieren. Befolgen Sie diese Schritte, um einen Ihrer vorhandenen Benutzeraccounts in einen Administratoraccount umzuwandeln:

1. Öffnen Sie den Arbeitsgruppenmanager, falls dieser nicht bereits geöffnet ist.
2. Klicken Sie in der Symbolleiste auf ACCOUNTS.
3. Wählen Sie den Benutzer *Tina Bubbles* aus.

4 Markieren Sie im Bereich ALLGEMEIN das Feld BENUTZER DARF DIESEN SERVER VERWALTEN.



5 Klicken Sie auf SICHERN.

Nachdem ein Account als Administratoraccount definiert wurde, enthält das Symbol neben dem Benutzernamen einen Stift. Dies weist darauf hin, dass der Benutzer Servereinstellungen bearbeiten kann.

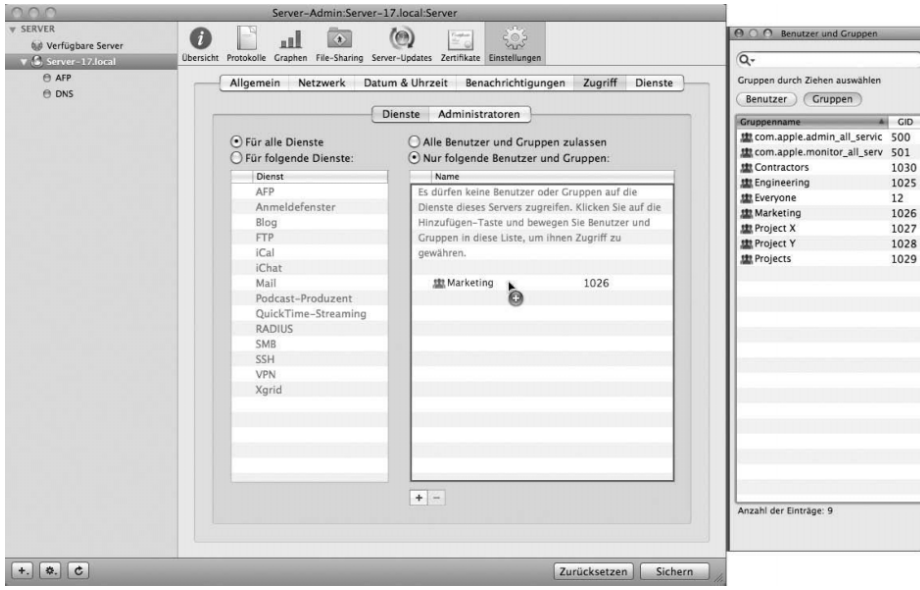
6 Testen Sie den neuen Administratorzugriff, indem Sie Server-Admin erneut öffnen und sich als Tina Bubbles anmelden.

Konfigurieren von Dienst-ACLs (SACLs)

Wie Dateien können Sie auch SACLs für einzelne Benutzer, Gruppen oder eine Mischung aus beiden konfigurieren. Möglicherweise stellen Sie auch fest, dass die Verwaltung auf Dauer einfacher ist, wenn Sie SACLs basierend auf Funktionen in der Organisation bestimmten Gruppen zuweisen anstatt einzelnen Personen. Gibt es innerhalb Ihres Unternehmens Veränderungen, können Sie diese bedeutend einfacher übernehmen, da Sie nur die Gruppenmitgliedschaften ändern müssen und keine einzelnen Datei- und Dienstberechtigungen für die jeweiligen Benutzer.

1. Öffnen Sie Server-Admin und stellen Sie als Tina Bubbles eine Verbindung her.
2. Wählen Sie den Namen Ihres Servers in der linken Spalte aus.
3. Klicken Sie auf die Taste Einstellungen in der Symbolleiste.
4. Klicken Sie auf Zugriff.
5. Klicken Sie auf Nur folgende Benutzer und Gruppen.
6. Klicken Sie unten im Fenster auf die Taste Hinzufügen (+), um das Fach Benutzer und Gruppen zu öffnen.
7. Klicken Sie im Fach Benutzer und Gruppen auf die Taste Gruppen.

8 Wählen Sie die Gruppe *Marketing* aus und bewegen Sie sie in die Liste der berechtigten Benutzer und Gruppen.



9 Klicken Sie auf SICHERN.

10 Versuchen Sie, als Mike Smith im Finder eine AFP-Verbindung zum Server herzustellen.

Da Mike Smith nicht der Gruppe *Marketing* angehört, wird beim Anmeldeversuch ein Fehler ausgegeben. Dieser Fehler wirkt sich wie bei der Eingabe eines falschen Kennwortes aus, auch wenn Sie dieses korrekt eingeben.

11 Fügen Sie in Server-Admin die Gruppe *Contractors* zu der Liste der zugelassenen Benutzer und Gruppen hinzu.

12 Klicken Sie auf SICHERN.

13 Versuchen Sie nun erneut, als Mike Smith *msmith* auf den Server zuzugreifen.

Da Mike Smith Mitglied der Gruppe *Contractors* ist, sollte der Verbindungsaufbau dieses Mal funktionieren.

Gewähren unterschiedlicher Zugriffsrechte für unterschiedliche Dienste

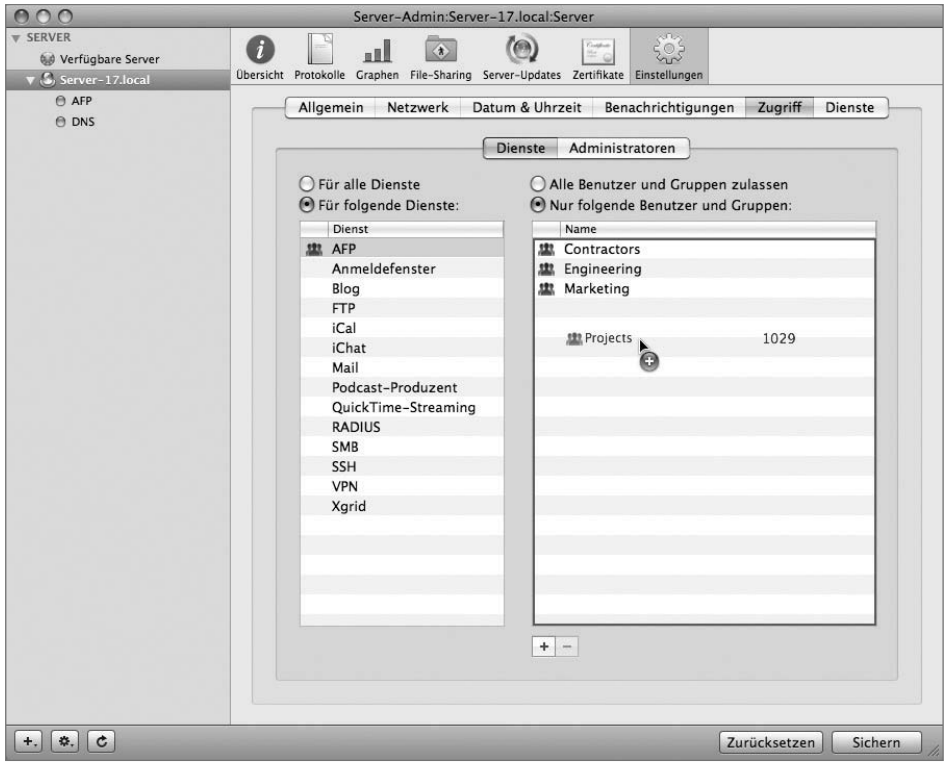
Wahrscheinlich bietet es sich in vielen Fällen an, unterschiedlichen Gruppen unterschiedliche Zugriffsrechte auf den Server zu ermöglichen. Möglicherweise möchten Sie z. B. einem Großteil der Gruppen Zugriff auf den AFP-Dienst gewähren, aber nur der Gruppe *Engineering* Zugriff auf den SSH-Dienst (entfernte Anmeldung).

1 Klicken Sie in Server-Admin auf FÜR FOLGENDE DIENSTE.

2 Wählen Sie den AFP-Dienst aus.

3 Klicken Sie auf NUR FOLGENDE BENUTZER UND GRUPPEN.

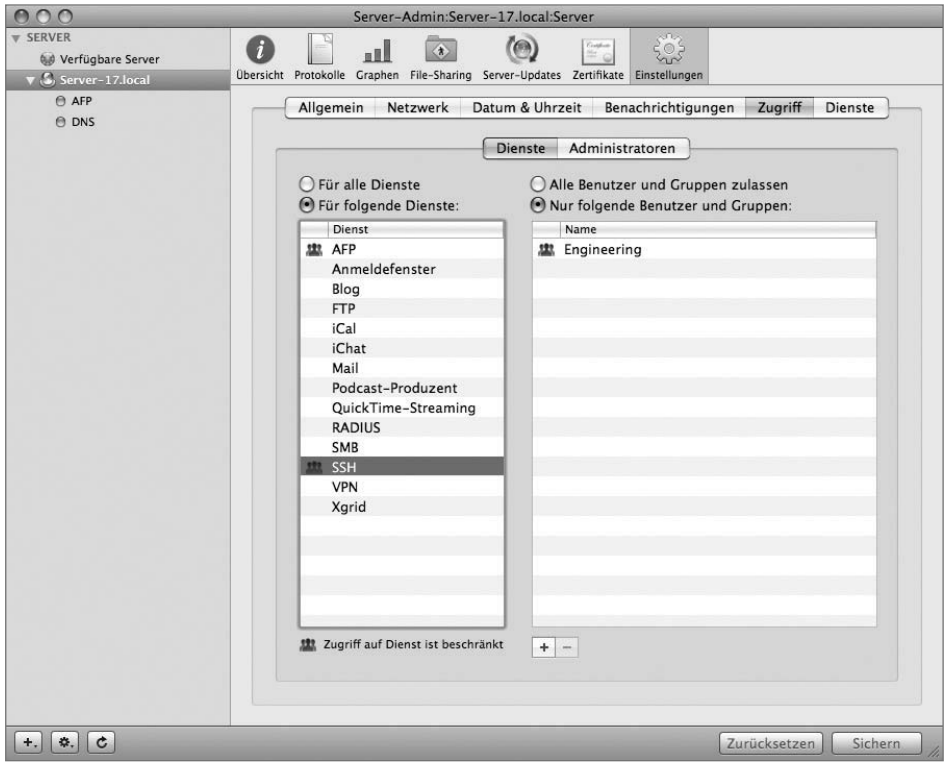
4 Bewegen Sie die Gruppen *Contractors*, *Engineering*, *Marketing* und *Projekte* in die Liste der berechtigten Benutzer und Gruppen.



5 Klicken Sie auf den SSH-Dienst.

6 Bewegen Sie die Gruppe *Engineering* in die Liste der berechtigten Benutzer und Gruppen.

7 Klicken Sie auf SICHERN.



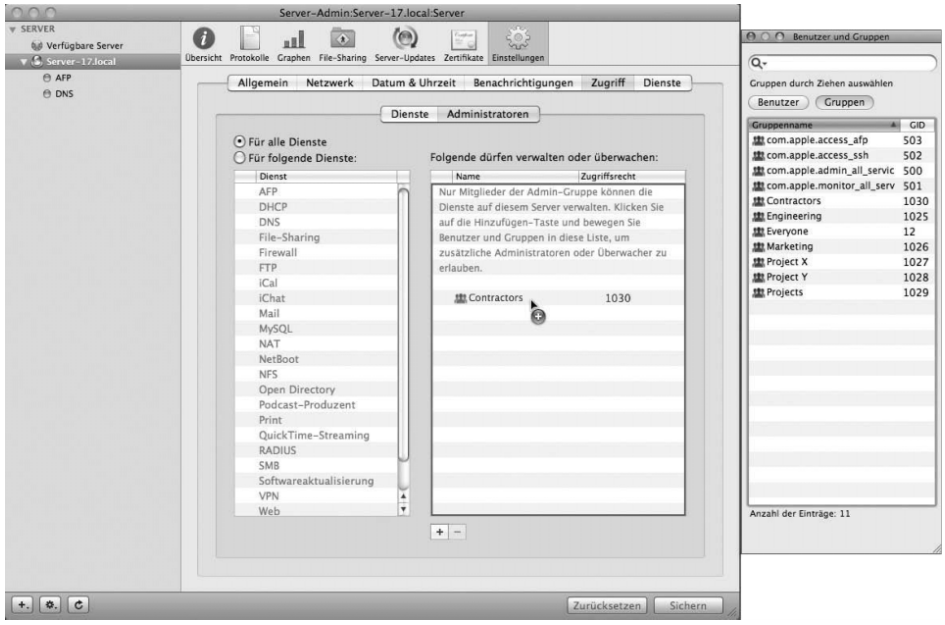
Sie werden bemerken, dass bei der Festlegung unterschiedlicher Zugriffsrechte für bestimmte Dienste neben dem Namen der Dienste mit gesteuertem Zugriff ein Symbol angezeigt wird und neben den anderen Diensten nicht. Ist ein Dienst nicht auf eine bestimmte Liste von Benutzern beschränkt, kann er von allen Benutzern verwendet werden. Unter Umständen empfiehlt es sich, diese anderen Dienste aus Sicherheitsgründen ebenfalls einzuschränken, es sei denn, sie sollen wirklich für alle zugänglich sein.

Einschränken der Verwaltungsfunktionen

Es gibt häufig Situationen, in denen Sie einer Gruppe von Benutzern nur eingeschränkte Verwaltungsmöglichkeiten zuweisen möchten. Dies ist der Fall, wenn eine Gruppe von Benutzern aufgrund ihrer Funktionen im Unternehmen Administratorrechte für bestimmte Aufgaben benötigt, Sie den Benutzern aber keine umfassenden Rechte gewähren möchten. Dies kann beispielsweise in einer Schulumgebung der Fall sein. Möglicherweise ist eine Gruppe von Schülern für die Überwachung Ihrer Dienste verantwortlich. Eine weitere Gruppe ist für die Verwaltung der Zugriffssteuerung Ihrer Benutzer auf das Programm *Podcast-Produzent* sowie der NetBoot-Filterung des NetBoot Servers verantwortlich. Mithilfe der neuen eingeschränkten Administratorfunktionen von Mac OS X Server 10.5 können Sie den Zugriff wie in den folgenden Schritten beschrieben konfigurieren, ohne Zugriff auf den gesamten Server zu gewähren.

1. Öffnen Sie das Programm *Server-Admin.*
2. Wählen Sie den Namen Ihres Servers in der linken Spalte aus.
3. Klicken Sie auf die Taste EINSTELLUNGEN in der Symbolleiste.
4. Klicken Sie auf ZUGRIFF.
5. Klicken Sie auf ADMINISTRATOREN.
6. Klicken Sie auf die Taste HINZUFÜGEN (+), um das Fach BENUTZER UND GRUPPEN zu öffnen.

7 Bewegen Sie die Gruppe *Contractors* in die Liste der Benutzer, die Verwaltungs- oder Überwachungsrechte erhalten sollen.



8 Klicken Sie auf SICHERN.

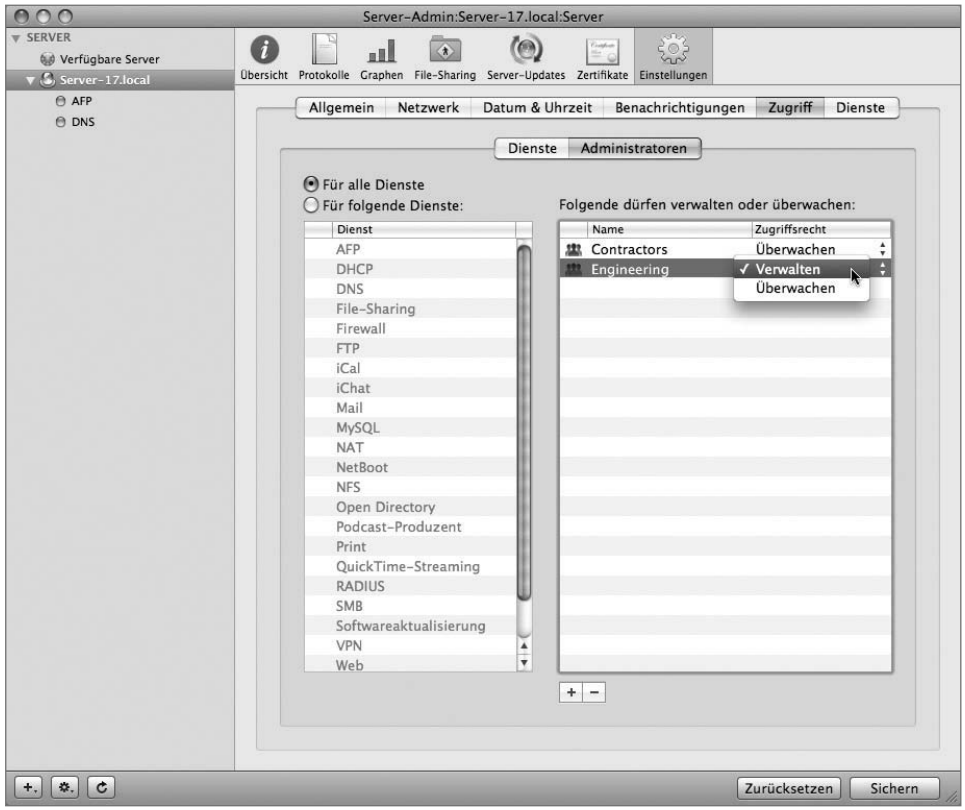
Sie bemerken, dass die Berechtigung standardmäßig auf ÜBERWACHEN eingestellt wird. Das bedeutet, dass neben den Benutzern, die im Arbeitsgruppenmanager als Administrator definiert sind, alle Mitglieder der Gruppe *Contractors* sämtliche Dienste auf Ihrem Server überwachen, aber nicht ändern können.

Möglicherweise möchten Sie noch eine andere Benutzergruppe hinzufügen, um dieser Verwaltungsrechte zuzuweisen.

9 Bewegen Sie die Gruppe *Engineering* in die Liste der Benutzer, die Verwaltungs- oder Überwachungsrechte erhalten sollen.

10 Ändern Sie die Option im Einblendmenü neben der Gruppe *Engineering* von ÜBERWACHEN in VERWALTEN.

11 Klicken Sie auf SICHERN.



Damit können alle Mitglieder der Gruppe *Engineering* auf beliebige der Dienste zugreifen und Änderungen daran vornehmen. Gleichzeitig können die Mitglieder der Gruppe *Contractors* weiterhin alle Dienste überwachen. In vielen Fällen ist jedoch auch dieser Zugriff u. U. noch zu umfassend und Sie möchten ihn auf nur bestimmte Dienste für diese Gruppen einschränken.

12 Klicken Sie auf die Option FÜR FOLGENDE DIENSTE.

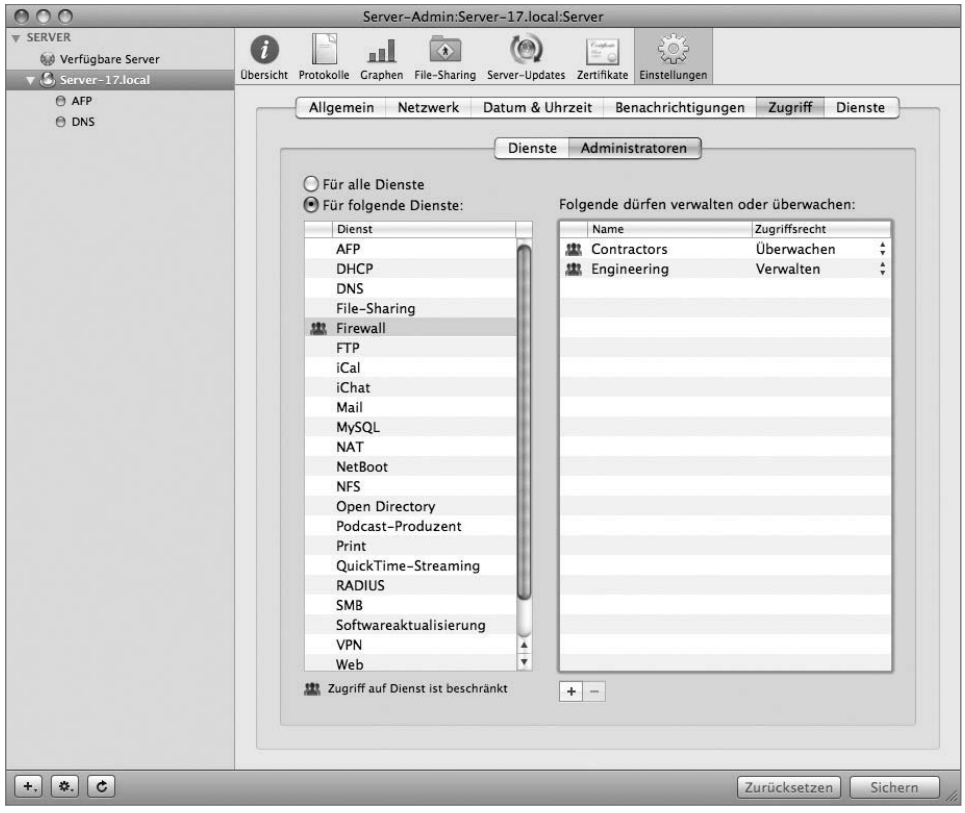
13 Wählen Sie FIREWALL aus.

14 Bewegen Sie die Gruppe *Contractors* in die Liste der Benutzer, die Verwaltungs- oder Überwachungsrechte besitzen.

15 Bewegen Sie die Gruppe *Engineering* in die Liste der Benutzer, die Verwaltungs- oder Überwachungsrechte besitzen.

16 Ändern Sie im Einblendmenü ZUGRIFFSRECHT neben der Gruppe *Engineering* die Einstellung in VERWALTEN.

17 Klicken Sie auf SICHERN.



Mit dieser Konfiguration erhalten nur die Mitglieder der Gruppe *Contractors* die erforderlichen Zugriffsrechte zum Überwachen des Firewall-Dienstes (z. B. von Protokollen) und die Mitglieder der Gruppe *Engineering* die Zugriffsrechte, um Änderungen an der Firewall-Konfiguration vorzunehmen. Bei allen anderen Diensten muss der Benutzer ein Serveradministrator mit umfassenden Rechten sein.

Aufheben der Autorisierung auf Ihrem Servern

Im letzten Teil dieses Kapitels geht es darum, den Server so zurückzusetzen, dass wieder alle Benutzer eine Verbindung herstellen können und nur Administratoren Administratorzugriff besitzen. Befolgen Sie die hier genannten Schritte, um wieder allen Benutzern Serverzugriff zu ermöglichen.

1. Öffnen Sie Server-Admin.
2. Klicken Sie in der Symbolleiste auf Einstellungen.
3. Klicken Sie auf Zugriff.
4. Klicken Sie auf Dienste.
5. Klicken Sie auf Für alle Dienste.
6. Klicken Sie auf Alle Benutzer und Gruppen zulassen.
7. Vergewissern Sie sich, dass die Liste der zugelassenen Benutzer und Gruppen leer ist. Sind Einträge vorhanden, wählen Sie diese aus und klicken Sie auf die Taste Entfernen (–).
8. Klicken Sie auf Sichern.
9. Klicken Sie auf Administratoren.
10. Klicken Sie auf Für alle Dienste.
11. Vergewissern Sie sich, dass die Liste der Benutzer und Gruppen leer ist. Sind Einträge vorhanden, wählen Sie diese aus und klicken Sie auf die Taste Entfernen (–).
12. Klicken Sie auf Sichern.

Fehlerbeseitigung

Dateisystem-ACLs können schnell unverständlich und unübersichtlich werden. Besitzt ein Benutzer keinen Zugriff auf eine Datei oder einen Ordner, den er eigentlich verwenden können sollte, prüfen Sie im Informationsfenster TATSÄCHLICHE ZUGRIFFSRECHTE EINBLENDEN im Aktionsmenü des Bereichs FILE-SHARING von Server-Admin die Berechtigungen des Benutzers für das jeweilige Objekt.

Versucht ein Benutzer auf einen Dienst zuzugreifen, für den er keine Berechtigung besitzt, ist der Grund für das Fehlschlagen der Verbindung bei SACLs u. U. nicht so einfach nachzuvollziehen. Auch wenn sie das Kennwort richtig eingegeben haben, sehen diese Benutzer möglicherweise eine Fehlermeldung, die auf eine falsche Kennworteingabe hinweist. In einem solchen Fall empfiehlt es sich, den Benutzer aufzufordern, sich bei einem Dienst anzumelden, auf den er zugreifen kann. Auf diese Weise können Sie sicherstellen, dass das Problem nicht das Kennwort ist.

Das Gelernte überprüfen

- Durch die Identifizierung erhält ein Benutzer Zugriff auf den Server. Durch die Autorisierung wird bestimmt, welche Schritte der Benutzer nach der Identifizierung ausführen kann.
- Benutzeraccounts für Mac OS X Server werden im Arbeitsgruppenmanager eingerichtet. Sie können zwei Arten von Accounts mit dem Arbeitsgruppenmanager erstellen: Benutzer- und Administratoraccounts. Ein Administratoraccount ist mit einem Benutzeraccount identisch, ermöglicht aber zusätzlich die Verwaltung des Servers.
- Mithilfe von Gruppenaccounts können Administratoren mehreren Benutzern schnell verschiedene Berechtigungen zuweisen. Gruppenaccounts werden mit dem Arbeitsgruppenmanager erstellt und verwaltet. Sie können Benutzer zu Gruppen und Gruppenmitgliedschaften zu Benutzeraccounts hinzufügen.
- Sie verwenden Server-Admin, um Netzwerkordner zu erstellen und ihnen Berechtigungen zuzuweisen.
- Mac OS X Server bietet Unterstützung für Zugriffssteuerungslisten (ACLs), die eine höhere Granularität für die Festlegung von Berechtigungen bereitstellen. Diese ACLs sind mit ACLs der Windows-Umgebung kompatibel und werden zusätzlich zu den standardmäßigen POSIX-Berechtigungen (UNIX) von Mac OS X eingesetzt.

- Mac OS X Server umfasst Unterstützung für Dienst-ACLs (SACLs), mit denen der Zugriff auf bestimmte Dienste für bestimmte Benutzer oder Gruppen eingeschränkt wird.
- Mac OS X Server 10.5 bietet jetzt Unterstützung für Serveradministratoren mit eingeschränkten Rechten.

Literatur

In den folgenden Dokumenten finden Sie weitere Informationen zu Benutzern, Gruppen und ACLs unter Mac OS X Server. (Alle genannten und weitere Dokumente stehen unter *www.apple.com/de/server/documentation* zur Verfügung.)

Administratorhandbücher

Dateidienste – Administration (*http://images.apple.com/server/macosx/docs/File_Services_Admin_v10.5.pdf*)

Serveradministration (*http://images.apple.com/server/macosx/docs/Server_Administration_v10.5.pdf*)

Benutzerverwaltung (*http://images.apple.com/server/macosx/docs/User_Management_v10.5.mnl.pdf*)

Aktualisieren und Migrieren (*http://images.apple.com/server/macosx/docs/Upgrading_and_Migrating_v10.5.pdf*)

Dokumente in der Apple Knowledge Base

Sie können unter *www.apple.com/de/support* nach neuen und aktualisierten Artikeln in der Apple Knowledge Base suchen.

Fragen

1. Beschreiben Sie die Unterschiede zwischen der Identifizierung und Autorisierung und geben Sie jeweils ein Beispiel.
2. Worin unterscheiden sich Benutzer- und Administratoraccounts unter Mac OS X und Mac OS X Server?
3. Mit welchem Programm werden Einstellungen von Benutzern, Gruppen und Netzwerkordnern unter Mac OS X Server konfiguriert? Mit welchem Programm werden Benutzer- und Gruppenberechtigungen unter Mac OS X geändert?
4. Wo legen Sie ACLs für den Datei- oder Ordnerzugriff fest?
5. Welcher Unterschied besteht zwischen Dienst-ACLs und Einstellungen für Administratoren mit eingeschränkten Rechten?

Antworten

1. Bei der Identifizierung fordert das System Informationen vom Benutzer an, bevor Zugriff auf einen bestimmten Account gewährt wird. Ein Beispiel ist die Eingabe von Namen und Kennwort beim Zugriff auf einen Apple-Dateiserver. Bei der Autorisierung wird mithilfe von Berechtigungen der Zugriff eines Benutzers auf bestimmte Ressourcen wie Dateien und Netzwerkordner gesteuert, nachdem sich der Benutzer erfolgreich angemeldet hat.
2. Benutzeraccounts ermöglichen den grundlegenden Zugriff auf einen Computer oder einen Server, Administratoraccounts ermöglichen dagegen die Verwaltung des Systems. Unter Mac OS X wird der Administratoraccount meist für die Änderung von Einstellungen oder das Hinzufügen neuer Software verwendet. Unter Mac OS X Server werden mit dem Administratoraccount in der Regel Einstellungen auf dem Server selbst geändert, meist mit Server-Admin oder dem Arbeitsgruppenmanager.
3. Mit dem Arbeitsgruppenmanager werden Benutzer und Gruppen konfiguriert, mit Server-Admin werden Netzwerkordner unter Mac OS X Server verwaltet. Mit dem Befehl INFORMATIONEN werden Berechtigungen unter Mac OS X geändert.
4. Server-Admin
5. SACLs bestimmen, welche Benutzer einen bestimmten Dienst verwenden dürfen. Die Einstellungen für Administratoren mit eingeschränkten Rechten steuern, wer einen Dienst überwachen oder ändern darf.