

Apple Pro Training Series

# OS X Server Essentials 10.10

Using and Supporting OS X Server on Yosemite

Arek Dreyer and Ben Greisler

Lesson and media files available for download



Certification Exam Preparation For  
Apple Certified Technical Coordinator 10.10

Apple Pro Training Series

# OS X Server Essentials 10.10

Arek Dreyer and Ben Greisler



Apple Pro Training Series: OS X Server Essentials 10.10  
Arek Dreyer and Ben Greisler  
Copyright © 2015 by Peachpit Press

Peachpit Press  
www.peachpit.com

To report errors, please send a note to [errata@peachpit.com](mailto:errata@peachpit.com). Peachpit Press is a division of Pearson Education.

**Apple Series Editor:** Lisa McClain  
**Production Editor:** Tracey Croom  
**Technical Editor:** Adam Karneboge  
**Apple Reviewer:** Susan Najour  
**Apple Project Manager:** Debra Otterstetter  
**Copy Editor:** Kim Wimpsett  
**Proofreader:** Darren Meiss

**Production Services:** Happenstance  
Type-O-Rama  
**Indexer:** Jack Lewis  
**Cover Illustration:** Paul Mavrides  
**Cover Production:** Happenstance  
Type-O-Rama

### Notice of Rights

All rights reserved. No part of this book may be reproduced or transmitted in any form by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher. For information on getting permission for reprints and excerpts, contact [permissions@peachpit.com](mailto:permissions@peachpit.com).

### Notice of Liability

The information in this book is distributed on an “As Is” basis, without warranty. While every precaution has been taken in the preparation of the book, neither the authors nor Peachpit shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the instructions contained in this book or by the computer software and hardware products described in it.

**IMPORTANT:** Some of the exercises contained in this guide can be temporarily disruptive, and some exercises, if performed incorrectly, could result in data loss or damage to system files. As such, it’s recommended that you perform these exercises on a Mac computer that is not critical to your daily productivity.

### Trademarks

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and Peachpit was aware of a trademark claim, the designations appear as requested by the owner of the trademark. All other product names and services identified throughout this book are used in editorial fashion only and for the benefit of such companies with no intention of infringement of the trademark. No such use, or the use of any trade name, is intended to convey endorsement or other affiliation with this book.

ISBN 13: 978-0-13-403350-1

ISBN 10: 0-13-403350-7

9 8 7 6 5 4 3 2 1 Printed and bound in the United States of America

Alternate Binding:

ISBN 13: 978-0-13-403417-1

ISBN 10: 0-13-403417-1

9 8 7 6 5 4 3 2 1 Printed and bound in the United States of America

*Thanks to my lovely wife, Heather Jagman, for her cheerful support.*

*—Arek Dreyer*

*My love and appreciation to my wife, Ronit, and my children, Galee and  
Noam, for their continued support through this project.*

*—Ben Greisler*

*This page intentionally left blank*

**Acknowledgments** With the memory of Steve Jobs still fresh in our minds, thank you to Tim Cook, Jonathan Ive, and everyone at Apple for continually innovating, surprising, and delighting customers.

Thank you to all the people who continue to help their users get the most out of OS X and iOS. Keep learning, and don't expect the pace of change to let up any time soon.

Thanks to the amazingly capable Lisa McClain, for gently making sure these materials made it into your hands, and to Scout Festa and Kim Wimpsett, for working their editorial and production magic.

Thanks to Adam Karneboge for adept corrections and suggestions.

Thanks to Schoun Regan for all his help.

Thank you, also, to the following people. Without your help, this book would be much less than what it is:

|                   |                     |                 |
|-------------------|---------------------|-----------------|
| Mark Bulthaupt    | Scott George        | Alby Rose       |
| Craig Cohen       | Charlie Heizer      | John Signa      |
| Gordon Davisson   | Andre LaBranche     | Cindy Waller    |
| Weldon Dodd       | Ben Levy            | Simon Wheatley  |
| Josh Durham       | Tip Lovingood       | Kevin White     |
| Charles Edge      | Jussi-Pekka Mantere | Josh Wisenbaker |
| Ed Faulkner       | Sean Murphy         | Eric Zelenka    |
| Patrick Gallagher | Susan Najour        |                 |



# Contents at a Glance

|  |      |
|--|------|
| About This Guide. . . . .  | xvii |
| <b>Configuring and Monitoring OS X Server</b>                              |      |
| <b>Lesson 1</b> Installing OS X Server. . . . .                            | 3    |
| <b>Lesson 2</b> Providing DNS Records. . . . .                             | 63   |
| <b>Lesson 3</b> Exploring the Server App. . . . .                          | 93   |
| <b>Lesson 4</b> Configuring SSL Certificates. . . . .                      | 123  |
| <b>Lesson 5</b> Using Status and Notifications. . . . .                    | 165  |
| <b>Lesson 6</b> Backing Up OS X Server. . . . .                            | 183  |
| <b>Configuring Accounts</b>  |      |
| <b>Lesson 7</b> Managing Local Users. . . . .                              | 201  |
| <b>Lesson 8</b> Configuring Open Directory Services. . . . .               | 253  |
| <b>Lesson 9</b> Managing Local Network Accounts. . . . .                   | 277  |
| <b>Managing Devices with Configuration Profiles</b>                        |      |
| <b>Lesson 10</b> Configuring OS X Server to Provide Device Management. . . | 305  |
| <b>Lesson 11</b> Managing with Profile Manager. . . . .                    | 327  |
| <b>Sharing Files</b>   |      |
| <b>Lesson 12</b> Configuring the File Sharing Service. . . . .             | 369  |
| <b>Lesson 13</b> Defining File Access. . . . .                             | 407  |
| <b>Implementing Deployment Solutions</b>                                   |      |
| <b>Lesson 14</b> Leveraging NetInstall. . . . .                            | 451  |
| <b>Lesson 15</b> Caching Content from Apple. . . . .                       | 483  |
| <b>Lesson 16</b> Implementing the Software Update Service. . . . .         | 497  |

**Providing Network Services**

|                  |  |     |
|------------------|--|-----|
| <b>Lesson 17</b> | Offering Time Machine Network Backup. . . . .    | 503 |
| <b>Lesson 18</b> | Providing Security via the VPN Service . . . . . | 515 |
| <b>Lesson 19</b> | Configuring DHCP. . . . .                        | 531 |
| <b>Lesson 20</b> | Hosting Websites. . . . .                        | 551 |

**Using Collaborative Services**

|                  |  |     |
|------------------|--|-----|
| <b>Lesson 21</b> | Providing Mail Service. . . . .            | 585 |
| <b>Lesson 22</b> | Configuring the Wiki Service. . . . .      | 611 |
| <b>Lesson 23</b> | Implementing the Calendar Service. . . . . | 623 |
| <b>Lesson 24</b> | Managing the Contacts Service. . . . .     | 639 |
| <b>Lesson 25</b> | Providing the Messages Service. . . . .    | 649 |
|                  | Index. . . . .                             | 667 |

|                   |  |     |
|-------------------|--|-----|
| <b>Appendix A</b> | Lesson Review Questions and Answers. . . . . | A-1 |
| <b>Appendix B</b> | Additional Resources. . . . .                | B-1 |
| <b>Appendix C</b> | Where Are the Lesson Files?. . . . .         | C-1 |

*Bonus chapters mentioned in this eBook are available after the index.*

*See last page of this eBook for instructions on downloading your lesson files.*

# Table of Contents

|                           |      |
|---------------------------|------|
| About This Guide. . . . . | xvii |
|---------------------------|------|

## **Configuring and Monitoring OS X Server**

|                 |   |    |
|-----------------|---|----|
| <b>Lesson 1</b> | Installing OS X Server. . . . .   | 3  |
| Reference 1.1   | Evaluating OS X Server Requirements. . . . .  | 4  |
| Reference 1.2   | Preparing to Install OS X Server. . . . .   | 7  |
| Reference 1.3   | Installing OS X Server. . . . .   | 16 |
| Reference 1.4   | Upgrading or Migrating to OS X Server. . . . .                                      | 18 |
| Reference 1.5   | Updating OS X Server. . . . .   | 19 |
| Reference 1.6   | Troubleshooting. . . . .  | 20 |
| Exercise 1.1    | Configure OS X Before Installing OS X Server on Your<br>Server Computer . . . . .   | 21 |
| Exercise 1.2    | Perform the Initial Installation of OS X Server on Your<br>Server Computer. . . . . | 39 |
| Exercise 1.3    | Configure Your Administrator Computer. . . . .                                      | 48 |
| <b>Lesson 2</b> | Providing DNS Records. . . . .  | 63 |
| Reference 2.1   | What Is DNS?. . . . .   | 63 |
| Reference 2.2   | Evaluating OS X DNS Hosting Requirements. . . . .                                   | 65 |
| Reference 2.3   | Configuring DNS Service in OS X Server. . . . .                                     | 68 |
| Reference 2.4   | Troubleshooting DNS Service in OS X Server. . . . .                                 | 70 |
| Exercise 2.1    | Create DNS Zones and Records. . . . .   | 71 |
| Exercise 2.2    | Restrict Access to the DNS Service. . . . .   | 84 |

|                 |   |            |
|-----------------|---|------------|
| <b>Lesson 3</b> | <b>Exploring the Server App. . . . .</b>                                      | <b>93</b>  |
| Reference 3.1   | Allowing Remote Access. . . . .   | 93         |
| Reference 3.2   | Using Server Sidebar Elements. . . . .  | 96         |
| Reference 3.3   | Using the Manage Menu. . . . .  | 108        |
| Reference 3.4   | Using the Tools Menu. . . . .   | 109        |
| Reference 3.5   | Using Help and Server Tutorials. . . . .                                      | 110        |
| Reference 3.6   | Troubleshooting. . . . .  | 112        |
| Exercise 3.1    | Turn On Screen Sharing and Remote Management. . . . .                         | 113        |
| Exercise 3.2    | Inspect the Service Data Volume. . . . .                                      | 115        |
| Exercise 3.3    | Explore the Access Tab. . . . .   | 116        |
| <br>            |   |            |
| <b>Lesson 4</b> | <b>Configuring SSL Certificates. . . . .</b>                                  | <b>123</b> |
| Reference 4.1   | Describe SSL Certificate Basics . . . . .                                     | 123        |
| Reference 4.2   | Configuring SSL Certificates. . . . .   | 127        |
| Reference 4.3   | Troubleshooting. . . . .  | 149        |
| Exercise 4.1    | Examine the Default SSL Certificate. . . . .                                  | 150        |
| Exercise 4.2    | Configure an Open Directory Certificate Authority. . . . .                    | 152        |
| Exercise 4.3    | Configure Your Administrator Computer to Trust an SSL<br>Certificate. . . . . | 159        |
| Exercise 4.4    | Clean Up. . . . .   | 163        |
| <br>            |   |            |
| <b>Lesson 5</b> | <b>Using Status and Notifications. . . . .</b>                                | <b>165</b> |
| Reference 5.1   | Using Monitoring and Status Tools. . . . .                                    | 165        |
| Reference 5.2   | Configuring OS X Server Alerts. . . . .                                       | 166        |
| Reference 5.3   | Using Logs in OS X Server . . . . .   | 169        |
| Reference 5.4   | Using Stats in OS X Server. . . . .   | 171        |
| Reference 5.5   | Viewing Storage Space. . . . .  | 172        |
| Exercise 5.1    | Use the Server App to Monitor Your Server. . . . .                            | 173        |
| <br>            |   |            |
| <b>Lesson 6</b> | <b>Backing Up OS X Server. . . . .</b>  | <b>183</b> |
| Reference 6.1   | Describing Backup Concepts. . . . .   | 183        |
| Reference 6.2   | Backing up with Time Machine . . . . .  | 185        |

|              |  |     |
|--------------|--|-----|
| Exercise 6.1 | Use Time Machine to Back Up OS X Server. . . . . | 187 |
| Exercise 6.2 | Inspect Time Machine Backup Files. . . . .       | 192 |

## Configuring Accounts

|                 |   |            |
|-----------------|---|------------|
| <b>Lesson 7</b> | <b>Managing Local Users. . . . .</b>  | <b>201</b> |
| Reference 7.1   | Describing Authentication and Authorization. . . . .                          | 202        |
| Reference 7.2   | Creating and Administering User and Administrator<br>Server Accounts. . . . . | 203        |
| Reference 7.3   | Managing Access to Services. . . . .  | 215        |
| Reference 7.4   | Troubleshooting. . . . .  | 218        |
| Exercise 7.1    | Create and Configure Local User Accounts. . . . .                             | 219        |
| Exercise 7.2    | Import Local User Accounts. . . . .   | 229        |
| Exercise 7.3    | Create and Configure Local Groups. . . . .                                    | 235        |
| Exercise 7.4    | Troubleshoot Problems with Importing Accounts. . . . .                        | 240        |
| Exercise 7.5    | Manage Service Access. . . . .  | 241        |
| Exercise 7.6    | Clean Up. . . . .   | 250        |
| <b>Lesson 8</b> | <b>Configuring Open Directory Services. . . . .</b>                           | <b>253</b> |
| Reference 8.1   | Introducing Directory Service Concepts. . . . .                               | 253        |
| Reference 8.2   | Configuring Open Directory Services. . . . .                                  | 262        |
| Reference 8.3   | Troubleshooting. . . . .  | 271        |
| Exercise 8.1    | Inspect Your Open Directory Master. . . . .                                   | 273        |
| Exercise 8.2    | Use Logs to Troubleshoot Using Open Directory. . . . .                        | 275        |
| <b>Lesson 9</b> | <b>Managing Local Network Accounts. . . . .</b>                               | <b>277</b> |
| Reference 9.1   | Using the Server App to Manage Network User Accounts. . . . .                 | 277        |
| Reference 9.2   | Configuring Authentication Methods on OS X Server. . . . .                    | 282        |
| Reference 9.3   | Using Single Sign-On and Kerberos . . . . .                                   | 286        |
| Reference 9.4   | Troubleshooting. . . . .  | 291        |
| Exercise 9.1    | Create and Import Network Accounts. . . . .                                   | 292        |
| Exercise 9.2    | Configure Password Policies. . . . .  | 298        |

## Managing Devices with Configuration Profiles

|                  |   |     |
|------------------|---|-----|
| <b>Lesson 10</b> | Configuring OS X Server to Provide Device Management. . . . . | 305 |
| Reference 10.1   | Administering the Profile Manager Service. . . . .            | 305 |
| Reference 10.2   | Configuring Profile Manager. . . . .                          | 306 |
| Exercise 10.1    | Turn On Profile Manager. . . . .                              | 312 |
| <b>Lesson 11</b> | Managing with Profile Manager. . . . .                        | 327 |
| Reference 11.1   | Introducing Account Management. . . . .                       | 327 |
| Reference 11.2   | Troubleshooting. . . . .                                      | 340 |
| Exercise 11.1    | Use Profile Manager for Shared Devices . . . . .              | 341 |
| Exercise 11.2    | Use Profile Manager for One-to-One Devices . . . . .          | 351 |

## Sharing Files

|                  |  |     |
|------------------|--|-----|
| <b>Lesson 12</b> | Configuring the File Sharing Service. . . . .                | 369 |
| Reference 12.1   | Addressing the Challenges of File Sharing. . . . .           | 369 |
| Reference 12.2   | Creating Share Points. . . . .                               | 378 |
| Reference 12.3   | Troubleshooting File-Sharing Services. . . . .               | 388 |
| Reference 12.4   | Providing FTP Service . . . . .                              | 389 |
| Exercise 12.1    | Explore the File Sharing Service. . . . .                    | 392 |
| Exercise 12.2    | Use Logs to Troubleshoot Problems with File Sharing. . . . . | 404 |
| <b>Lesson 13</b> | Defining File Access. . . . .                                | 407 |
| Reference 13.1   | Configuring Access to Share Points and Folders. . . . .      | 407 |
| Reference 13.2   | POSIX Permissions Compared to ACL Settings. . . . .          | 413 |
| Exercise 13.1    | Configure Access Control. . . . .                            | 429 |

## Implementing Deployment Solutions

|                  |  |     |
|------------------|--|-----|
| <b>Lesson 14</b> | Leveraging NetInstall. . . . .                     | 451 |
| Reference 14.1   | Managing Computers with NetInstall. . . . .        | 452 |
| Reference 14.2   | Creating Images with System Image Utility. . . . . | 456 |

|                                       |   |            |
|---------------------------------------|---|------------|
| Reference 14.3                        | Describing Shadow Files. . . . .                            | 461        |
| Reference 14.4                        | Troubleshooting NetInstall. . . . .                         | 463        |
| Exercise 14.1                         | Prepare the NetInstall Service. . . . .                     | 463        |
| Exercise 14.2                         | Create a Customized NetInstall Image. . . . .               | 465        |
| Exercise 14.3                         | Start the NetInstall Service. . . . .                       | 473        |
| Exercise 14.4                         | Start Up from a NetInstall Image. . . . .                   | 478        |
| Exercise 14.5                         | Monitor the NetInstall Service. . . . .                     | 480        |
| <b>Lesson 15</b>                      | <b>Caching Content from Apple. . . . .</b>                  | <b>483</b> |
| Reference 15.1                        | Describing the Caching Service. . . . .                     | 483        |
| Reference 15.2                        | Configuring and Maintaining the Caching Service. . . . .    | 486        |
| Reference 15.3                        | Comparing the Software Update and Caching Services. . . . . | 490        |
| Reference 15.4                        | Troubleshooting the Caching Service. . . . .                | 492        |
| <b>Lesson 16</b>                      | <b>Implementing the Software Update Service. . . . .</b>    | <b>497</b> |
| Reference 16.1                        | Managing Software Updates. . . . .                          | 497        |
| Reference 16.2                        | Troubleshooting the Software Update Service. . . . .        | 499        |
| <br><b>Providing Network Services</b> |   |            |
| <b>Lesson 17</b>                      | <b>Offering Time Machine Network Backup. . . . .</b>        | <b>503</b> |
| Reference 17.1                        | Configuring Time Machine as a Network Service. . . . .      | 503        |
| Exercise 17.1                         | Configure and Use the Time Machine Service. . . . .         | 506        |
| <b>Lesson 18</b>                      | <b>Providing Security via the VPN Service . . . . .</b>     | <b>515</b> |
| Reference 18.1                        | Describing VPNs. . . . .                                    | 515        |
| Reference 18.2                        | Configuring the VPN Service with the Server App. . . . .    | 516        |
| Reference 18.3                        | Troubleshooting. . . . .                                    | 522        |
| Exercise 18.1                         | Configure the VPN Service. . . . .                          | 523        |
| Exercise 18.2                         | Clean Up. . . . .   | 529        |
| <b>Lesson 19</b>                      | <b>Configuring DHCP. . . . .</b>                            | <b>531</b> |
| Reference 19.1                        | Describing How DHCP Works. . . . .                          | 532        |

|                  |  |            |
|------------------|--|------------|
| Reference 19.2   | Configuring DHCP Service. . . . .              | 535        |
| Reference 19.3   | Troubleshooting DHCP. . . . .                  | 541        |
| Exercise 19.1    | Configure the DHCP Service (Optional). . . . . | 544        |
| <b>Lesson 20</b> | <b>Hosting Websites. . . . .</b>               | <b>551</b> |
| Reference 20.1   | Identifying the Web Service Software . . . . . | 551        |
| Reference 20.2   | Describing Basic Website Structure. . . . .    | 552        |
| Reference 20.3   | Monitoring Web Services . . . . .              | 558        |
| Reference 20.4   | Troubleshooting. . . . .                       | 559        |
| Exercise 20.1    | Turn On Web Services. . . . .                  | 559        |
| Exercise 20.2    | Modify the Default Websites. . . . .           | 563        |
| Exercise 20.3    | Create and Remove a New Website. . . . .       | 569        |
| Exercise 20.4    | Restrict Access to a Website. . . . .          | 578        |
| Exercise 20.5    | Monitor Web Services . . . . .                 | 580        |

**Using Collaborative Services**

|                  |   |            |
|------------------|---|------------|
| <b>Lesson 21</b> | <b>Providing Mail Service. . . . .</b>              | <b>585</b> |
| Reference 21.1   | Hosting Mail Services. . . . .                      | 585        |
| Reference 21.2   | Troubleshooting Mail Services. . . . .              | 593        |
| Exercise 21.1    | Turn On the Mail Service. . . . .                   | 594        |
| Exercise 21.2    | Send and Receive Mail. . . . .                      | 602        |
| Exercise 21.3    | Examine Mail Service Logs. . . . .                  | 609        |
| <b>Lesson 22</b> | <b>Configuring the Wiki Service. . . . .</b>        | <b>611</b> |
| Reference 22.1   | Configuring and Managing a Wiki. . . . .            | 611        |
| Reference 22.2   | Troubleshooting the Wiki Service. . . . .           | 614        |
| Exercise 22.1    | Turn On the Wiki Service. . . . .                   | 615        |
| Exercise 22.2    | Edit a Wiki. . . . .                                | 618        |
| <b>Lesson 23</b> | <b>Implementing the Calendar Service. . . . .</b>   | <b>623</b> |
| Reference 23.1   | Describing Calendar Service Data Locations. . . . . | 623        |
| Reference 23.2   | Using the Calendar Service. . . . .                 | 624        |

|                   |  |            |
|-------------------|--|------------|
| Reference 23.3    | Troubleshooting the Calendar Service. . . . .              | 628        |
| Exercise 23.1     | Configure and Start the Calendar Service. . . . .          | 629        |
| Exercise 23.2     | Use the Server App to Add Resources and Locations. . . . . | 631        |
| Exercise 23.3     | Use the Calendar Service. . . . .                          | 633        |
| <b>Lesson 24</b>  | <b>Managing the Contacts Service. . . . .</b>              | <b>639</b> |
| Reference 24.1    | Introducing the Contacts Service. . . . .                  | 639        |
| Reference 24.2    | Troubleshooting the Contacts Service. . . . .              | 640        |
| Exercise 24.1     | Configure the Contacts Service. . . . .                    | 641        |
| Exercise 24.2     | Configure OS X to Use the Contacts Service. . . . .        | 642        |
| <b>Lesson 25</b>  | <b>Providing the Messages Service. . . . .</b>             | <b>649</b> |
| Reference 25.1    | Managing the Messages Service. . . . .                     | 649        |
| Reference 25.2    | Troubleshooting the Messages Service. . . . .              | 654        |
| Exercise 25.1     | Set Up the Messages Service. . . . .                       | 654        |
| Exercise 25.2     | Use the Messages Service. . . . .                          | 656        |
|                   | Index. . . . .   | 667        |
| <b>Appendix A</b> | <b>Lesson Review Questions and Answers. . . . .</b>        | <b>A-1</b> |
| <b>Appendix B</b> | <b>Additional Resources. . . . .</b>                       | <b>B-1</b> |
| <b>Appendix C</b> | <b>Where Are the Lesson Files?. . . . .</b>                | <b>C-1</b> |

*Bonus chapters mentioned in this eBook are available after the index.*

*See last page of this eBook for instructions on downloading your lesson files.*



# About This Guide

This guide serves as a tour of the breadth of functionality of OS X Server and the best methods for effectively supporting users of OS X Server systems. It is for both self-paced learners working independently and those participating in an instructor-led course. This guide is the curriculum for the Apple official training course Yosemite 201: OS X Server Essentials 10.10, a three-day, hands-on course that provides an in-depth exploration of how to configure and support OS X Server for Yosemite. This course is facilitated by an Apple Certified Trainer and is organized into multiple lessons, each containing instructor presentations followed by related student exercises.

The primary goal of this guide is to prepare technical coordinators and entry-level system administrators for the tasks demanded of them by OS X Server; you will learn how to install and configure OS X Server to provide network-based services, such as configuration profile distribution and management, file sharing, authentication, and collaboration services. To help you become truly proficient, this guide covers the theory behind the tools you will use. For example, not only will you learn how to use Server app—the tool for managing services and accounts—but you will also learn about the ideas behind profile management, how to think about access to and control of resources, and how to set up and distribute profiles to support your environment.

You will learn to develop processes to help you understand and work with the complexity of your system as it grows. Even a single OS X Server computer can grow into a complicated system, and creating documentation and charts can help you develop processes so that additions and modifications can integrate harmoniously with your existing system.

This guide assumes you have some knowledge of OS X, because OS X Server is an app that you install on OS X (Yosemite). Therefore, you should be comfortable with basic navigation, troubleshooting, and networking in OS X. When working through this guide, a basic understanding and

## GOALS

- ▶ Learn how this guide is organized to facilitate learning
- ▶ Set up an environment for self-paced exercises
- ▶ Introduce Apple Authorized Training and Certification

knowledge of OS X is preferred, including knowledge of how to troubleshoot the operating system. Refer to *Apple Pro Training Series: OS X Support Essentials 10.10* from Peachpit Press if you need to develop a solid working knowledge of OS X.

**NOTE** ► Unless otherwise specified, all references to OS X refer to version 10.10 or later, and references to OS X Server refer to version 4.0, which at the time of this writing is the most current version available. Some screenshots, features, and procedures may be slightly different from those presented on these pages because of subsequent upgrades.

## Learning Methodology

Each lesson in this guide is designed to give technical coordinators and entry-level system administrators the skills, tools, and knowledge to implement and maintain a network that uses OS X Server by doing the following:

- Providing knowledge of how OS X Server works
- Showing how to use configuration tools
- Explaining troubleshooting and procedures

The exercises contained within this guide are designed to let you explore and learn the tools necessary to manage OS X Server for Yosemite. They move along in a predictable fashion, starting with installing and setting up OS X Server and moving to more advanced topics such as performing multiprotocol file sharing, using access control lists, and permitting OS X Server to manage network accounts. It is required that you start from a Mac that is not yet running OS X Server and that you do not use this server as a production server.

This guide serves as an introduction to OS X Server and is not meant to be a definitive reference. Because OS X and OS X Server contain several open source initiatives and can be configured at the command line, it is impossible to include all the possibilities and permutations here. First-time users of OS X Server and users of other server operating systems who are migrating to OS X Server have the most to gain from this guide; still, others who are upgrading from previous versions of OS X Server will also find this guide a valuable resource.

OS X Server is by no means difficult to set up and configure, but how you use OS X Server should be planned in advance. Accordingly, this guide is divided into seven parts:

- ▶ Part 1, “Configuring and Monitoring OS X Server,” covers planning, installation, initial configuration, and monitoring of OS X Server.
- ▶ Part 2, “Configuring Accounts,” defines authentication and authorization, access control, and Open Directory and the vast functionality it can provide.
- ▶ Part 3, “Managing Devices with Configuration Profiles,” covers managing devices with the Profile Manager service.
- ▶ Part 4, “Sharing Files,” introduces the concept of sharing files over multiple protocols and controlling access to files with access control lists.
- ▶ Part 5, “Implementing Deployment Solutions,” teaches you how to effectively use deployment services, NetInstall, the Caching service, and the Software Update service.
- ▶ Part 6, “Providing Network Services,” introduces the network services, including Time Machine, VPN, DHCP, and Websites.
- ▶ Part 7, “Using Collaborative Services,” focuses on setting up collaboration services together, starting with Mail, moving through Wiki, Calendar, and Contacts, and finishing with the Messages service.

## Lesson Structure

Most lessons in this guide contain a reference section followed by an exercise section (the lessons on Caching and Software Update services do not contain exercises).

**NOTE** ▶ “Note” resources, like this one, offer important information to help clarify a subject. For example, some of the exercises in this guide may be disruptive. Consequently, it’s recommended that you perform these exercises on an OS X computer that is not critical to your daily productivity.

The reference sections contain initial explanatory material that teaches essential concepts. The exercise sections augment your understanding of concepts and develop your skills through step-by-step instruction for both self-paced learners and the hands-on portions of an instructor-led course.

**TIP** ▶ “Tip” resources, like this one, provide helpful hints, tricks, or shortcuts. For example, each lesson begins with an opening page that lists the learning goals and necessary resources for the lesson.

**MORE INFO ►** The “More Info” resources, like this one, provide ancillary information. These resources are merely for your edification and are not considered essential for the coursework.

Throughout this guide you’ll find references to Apple Support articles. You can find these articles at the Apple Support website ([www.apple.com/support](http://www.apple.com/support)), a free online resource containing the latest technical information for Apple products. We strongly encourage you to read the suggested articles and search the Apple Support website for answers to any problems you encounter.

We encourage you to explore two additional resources that Apple provides specifically for OS X Server: OS X Server Support (<https://www.apple.com/support/osxserver/>) and OS X Server: Advanced Administration (<https://help.apple.com/advancedserveradmin/mac/4.0/>).

Lesson files and bonus materials are available online when you redeem the access code supplied with your guide at [www.peachpit.com/redeem](http://www.peachpit.com/redeem). Detailed instructions for downloading files are provided later in this guide. Appendix A, “Lesson Review Questions & Answers,” recaps each lesson through a series of questions that reinforce the material you learned in the guide. Try to answer each question yourself before looking at the answer. You can refer to various Apple resources, such as the Apple Support website and OS X Server documentation, as well as the lessons themselves to help you answer these questions. Appendix B, “Additional Resources,” lists relevant Apple Support articles and recommended documents related to the topic of each lesson. You’ll also find supplemental exercise material for exercises in Lesson 20 and Lesson 23. An “Updates & Errata” document will contain updates and corrections to the guide if any are available.

## Exercise Setup

This guide is written so that both the self-paced learner and the attendee at an Apple Authorized Training Center (AATC) or Apple Authorized Training Center for Education (AATCE) can complete most of the exercises using the same techniques. Those attending Yosemite 201 at an AATC or AATCE will have the appropriate exercise setup provided as part of the training experience. Self-paced learners attempting these exercises will have to set up an appropriate environment using their own equipment.

**NOTE** ▶ Some of these exercises can be disruptive (for example, turning on the DHCP service may prevent devices on the local network from being able to browse Internet), and some exercises, if performed incorrectly, could result in data loss or damage to files. As such, it's recommended that you perform these exercises on an isolated network, using OS X computers and iOS devices that are not critical to your daily productivity. Apple, Inc., and Peachpit Press are not responsible for any data loss or any damage to any equipment that occurs as a direct or indirect result of following the procedures described in this guide.

### **Mandatory Requirements**

Here's what you will need to complete the lessons in the guide:

- ▶ Two Mac computers, each with OS X Yosemite. One Mac is referred to as your “administrator computer,” and the Mac on which you will install OS X Server is referred to as your “server computer” or, more simply, your “server.” After you are done using your server computer with this guide, you should erase and reinstall OS X on its startup volume before using it again in a production environment.
- ▶ An Apple ID that is associated with a verified email address so you can obtain Apple Push Notification service (APNs) certificates for Server app notifications and for the Profile Manager service. You can create an Apple ID at the appropriate time during an exercise if you don't already have an Apple ID.
- ▶ A valid licensed copy of OS X Server from the Mac App Store.
- ▶ An Internet connection for obtaining APNs certificates for alerts and for the Profile Manager service.
- ▶ An isolated network or subnet with an exercise-specific configuration. This can be facilitated with something as simple as a small network Wi-Fi router with multiple Ethernet ports. For example, Apple AirPort Extreme would be a good choice. You can find instructions for the general setup of an exercise network and specific instructions for the configuration of AirPort Extreme at [www.apple.com/airport-extreme](http://www.apple.com/airport-extreme).
- ▶ A router (such as AirPort Extreme) to connect the small isolated network to the Internet. It will be helpful to be familiar with how to configure it.
- ▶ Two Ethernet network cables (to complete the NetInstall exercises); each Ethernet cable will connect a Mac to the Ethernet switch.
- ▶ Student Materials demonstration files, which you can download after registering your guide with Peachpit. Instructions for registration and download are included in “Exer-

cise 1.1 Configure OS X Before Installing OS X Server on Your Server Computer ” on page 21.

### **Optional Add-Ons**

If a specific resource is required for an optional exercise, it will be listed as a prerequisite at the beginning of that exercise. Here are some examples:

- ▶ An iOS device to test access to OS X Server services, including the Profile Manager service
- ▶ A Wi-Fi access point (preferably the same AirPort base station) to provide wireless access for iOS devices to your private network
- ▶ For “Exercise 19.1 Configure the DHCP Service (Optional)” on page 544: To provide DHCP on an extra isolated network: either an additional built-in Ethernet port on your Mac (for example, if your server computer is a Mac Pro) or a USB to Ethernet adapter or a Thunderbolt to Gigabit Ethernet Adapter; and an extra Ethernet network switch

If you lack the equipment necessary to complete a given exercise, you are still encouraged to read the step-by-step instructions and examine the screenshots to understand the procedures demonstrated.

### **Network Infrastructure**

As was previously stated, the exercises require an isolated network. You should replicate the instructor-led classroom environment, which is described in the next sections, as closely as possible so that you do not need to translate between the exercise instructions and your situation.

### **IPv4 Addresses**

The instructor-led environment provides an IPv4 network with a gateway of 10.0.0.1 and subnet mask of 255.255.255.0; if possible, configure your internal network with the same parameters.

Many consumer-level routers are configured with a gateway of 192.168.1.1 and a subnet mask of 255.255.255.0. You might not be able to change this on your router; in many cases you will be able to replace the “10.0.0” portion of an IPv4 address in the exercise with a value appropriate for your isolated network (for example, 192.168.1.171 instead of

10.0.0.171 for a server address for student 17). You will need to remember to substitute your network prefix throughout the exercises.

**DHCP**

The classroom DHCP service provides IPv4 addresses in the range of 10.0.0.180 to 10.0.0.254; if possible, configure your internal network's DHCP service with the same parameters. It will be helpful to know how to define the IP addresses of DNS servers being provided by DHCP.

If you can configure your isolated network's DHCP service, configure it to use a similar range of IPv4 addresses. If you are unable to change the range of IPv4 addresses, there is a possibility that the DHCP service will assign to a device an IPv4 address already in use by your server computer or your administrator computer. This is another reason to keep your network isolated; do not introduce new devices to it.

**Domain Names**

The exercises and reference material in this guide use the Internet domains pretendco.com, pretendco.private, and megaglobalcorp.com, which are for learning environments only; do not attempt to use these in your production environment.

The exercises are written in such a way that any existing DNS service on your isolated network will be ignored so that you can experience your server setting up the DNS service for itself.

**Advanced Administrators**

If you already have advanced server administration skills, you may choose to use different settings, including your organization's Internet domain (instead of pretendco.com), your organization's DNS service, and a different IPv4 address scheme, but be warned that this introduces a high level of variability that the exercises cannot address in the given space, and be prepared to modify the exercises on your own as necessary.

**Exercise Order**

The exercises in this guide are designed to be relatively independent of each other so that you can perform them out of order or skip exercises you are not interested in. However, some exercises you must perform in the correct order, and where appropriate, an exercise lists these prerequisites. Here are some examples:

- ▶ You must perform all the exercises in Lesson 1 “Installing OS X Server” to install OS X Server and configure your administrator computer before performing any other exercises.
- ▶ You must perform “Exercise 4.2 Configure an Open Directory Certificate Authority” on page 152 and “Exercise 9.1 Create and Import Network Accounts” on page 292 to create users who you will use in later exercises; otherwise, if the prerequisites for an exercise include the user account used in the lesson, you can simply create those user (and possibly) group accounts with the Server app’s Users pane.

## Apple Training and Certification

The Apple Training and Certification program is designed to keep you at the forefront of Apple technology. Certification creates a benchmark to demonstrate your proficiency in specific Apple technologies and can give you a competitive edge in today’s evolving job market.

Certification exams are delivered at Apple Authorized Training Centers around the world.

Reading this guide or attending the Yosemite 201 class will help prepare you to pass the OS X Server Essentials 10.10 exam and become an Apple Certified Technical Coordinator.

Passing both this exam and the OS X Support Essentials 10.10 exam earns Apple Certified Technical Coordinator (ACTC) 10.10 certification. This is the second level of the Apple certification program for Mac professionals, which includes the following:

- ▶ Apple Certified Support Professional (ACSP) certification verifies an understanding of OS X core functionality and an ability to configure key services, perform basic troubleshooting, and support multiple users with essential OS X capabilities. ACSP certification is designed for the help desk professional, technical coordinator, or power user who supports OS X users, manages networks, or provides technical support for the Mac. Students earn ACSP certification by passing the OS X Support Essentials 10.10 exam. Visit <http://training.apple.com/certification/osxyosemite> to review the OS X Support Essentials Exam Prep Guide. To prepare for this exam, attend the Yosemite 101 class or read *Apple Pro Training Series: OS X Support Essentials 10.10*.
- ▶ Apple Certified Technical Coordinator (ACTC) certification verifies a foundation in OS X and OS X Server core functionality and an ability to configure key services and perform basic troubleshooting. ACTC certification is intended for OS X technical coordinators and entry-level system administrators who maintain small to medium-

size networks of computers using OS X Server. Students earn ACTC certification by passing the OS X Support Essentials 10.10 exam and OS X Server Essentials 10.10 exam. Visit <http://training.apple.com/certification/osxyosemite> review the OS X Server Essentials Exam Prep Guide.

**MORE INFO** ► To read OS X technical white papers and learn more about all Apple certifications, visit <http://training.apple.com>.

**NOTE** ► Although all the questions in the OS X Server Essentials 10.10 exam are based on material in this guide, nothing can substitute for time spent learning the technology. After you read the guide or take the class, spend time increasing your familiarity with OS X Server on your own to ensure your success on the certification exam.

*This page intentionally left blank*

## Lesson 4

# Configuring SSL Certificates

You can use OS X Server without doing any additional work to secure its services. However, you can use the Secure Sockets Layer (SSL) technology to prove your server's identity to client computers and devices and to encrypt communication between your server and client computers and devices. This lesson starts by describing the basics of SSL and then shows you how to configure SSL certificates for use with OS X Server.

### Reference 4.1 Describe SSL Certificate Basics

You want the users who use your server's services to trust your server's identity and to be able to encrypt network traffic with your server.

The OS X solution is to use SSL, which is a system for transmitting data securely between hosts. You can configure your server to use an SSL certificate, which provides the ability to use the SSL system.

An "SSL certificate" (also referred to as simply a "certificate") is a file that identifies the certificate holder. A certificate specifies the permitted use of the certificate and has an expiration date. Importantly, a certificate includes a public key infrastructure (PKI) public key.

PKI involves the use of public and private keys. Grossly simplified, a "key" is a cryptographic blob of data, and within PKI, public and private keys are created in a way that they are mathematically linked: Data encrypted with one key can be decrypted only by using the other key. If you can decrypt data with one key, it proves that the data was encrypted with the other key. The public key is

### GOALS

- ▶ Describe the basics of SSL certificates
- ▶ Create a certificate signing request
- ▶ Create a self-signed SSL certificate
- ▶ Import a certificate signed by a certificate authority
- ▶ Archive your certificate
- ▶ Renew your certificate
- ▶ Configure which certificate your OS X Server services use

made publicly available, and the private key should be kept private. Fortunately, all of this encryption and decryption happens behind the scenes and is the basis for establishing secure communications.

Here are some definitions:

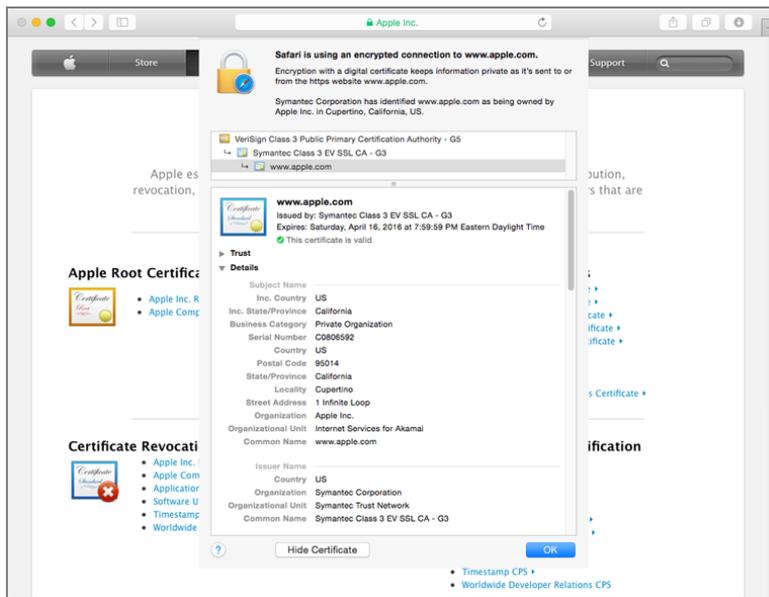
A “digital identity” (or more simply, an “identity”) is an electronic means of identifying an entity (such as a person or a server). An identity is the combination of a certificate (which includes the public key) and the corresponding private key. If you don’t have your private key, you can’t prove your identity. Similarly, if another entity has your private key, that other entity can claim your identity, so be sure to keep your private key private!

Again simplifying, a “digital signature” is a cryptographic scheme that uses PKI private and public keys to demonstrate that a given message (a digital file such as an SSL certificate) has not been changed since the signature was generated. If a message, which has been signed, changes or is otherwise tampered with, it will be clear that the signature no longer matches the underlying data. Therefore, you can use a digital signature on a certificate to prove its integrity.

A certificate must be either self-signed or signed by a “certification authority” (also known as a “certificate authority” or, more simply, a “CA”). In other words, you can sign your own certificate using your private key (remember that a certificate is a file that identifies the holder of the certificate and includes the public key), or you can have someone else, namely, a CA, use their private key to sign your certificate.

An “intermediate CA” is a CA whose certificate is signed by another CA. So, it’s possible to have a hierarchical “chain” of certificates, where an intermediate CA, which in turn is signed by yet another CA, signs a certificate.

In the following figure, the certificate for [www.apple.com](http://www.apple.com) is signed by an intermediate CA with the name of Symantec Class 3 EV SSL CA - G3, and that intermediate CA is signed by a CA with the name of VeriSign Class 3 Public Primary Certification Authority - G5.

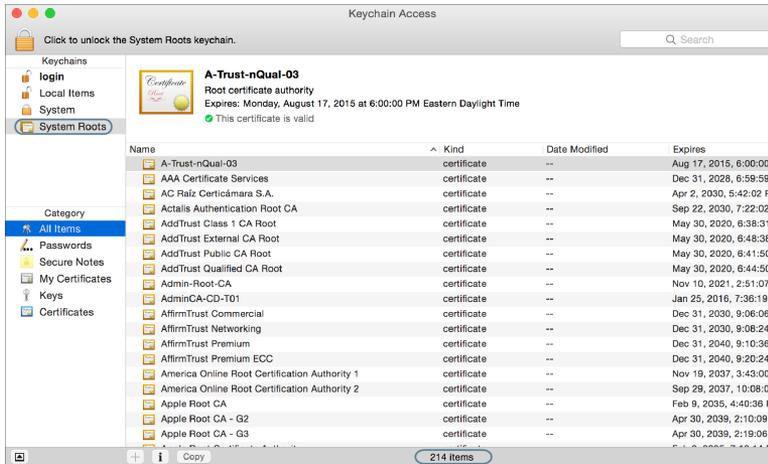


You can follow a chain of certificates, starting with a signed certificate, up to the intermediate CA and ending at the top of the chain. The certificate chain ends with a CA that signs its own certificate, which is called a “root CA.” It is not required to have an intermediate CA involved—you could simply have a root CA sign your certificate—but in practice, an intermediate CA is often involved.

How do you know if you can trust a CA? After all, since a root CA has signed its own SSL certificate, this effectively means that the organization in control of a root CA simply asserts that you should trust that it is who it claims to be.

The answer is that trust has to start somewhere. In OS X and iOS, Apple includes a collection of root and intermediate CAs that Apple has determined are worthy of trust (see the Apple Root Certificate Program page on the Apple site for the acceptance process: [www.apple.com/certificateauthority/ca\\_program.html](http://www.apple.com/certificateauthority/ca_program.html)). Out of the box, your Mac computers and iOS devices are configured to trust those CAs. By extension, your Mac computers and iOS devices also trust any certificate or intermediate CA whose certificate chain ends with one of these CAs. In OS X, these trusted CAs are stored in the System Roots keychain. (See Lesson 8, “Keychain Management,” in *Apple Pro Training Series: OS X Support Essentials 10.10* for more information about the various keychains in OS X.) You can use Keychain Access to view this collection of trusted root CAs. Open Keychain Access (in the Utilities folder). In the upper-left Keychains column, click System Roots. Note that in the

following figure the bottom of the window states that there are more than 200 trusted CAs or intermediate CAs by default in Yosemite.



**MORE INFO** ► Some third-party software companies, such as Mozilla, do not use the System Roots keychain and have their own mechanism to store CAs that their software is configured to trust.

In Lesson 8 “Configuring Open Directory Services”, you will learn that when you configure your server as an Open Directory master, the Server app automatically creates a new CA and a new intermediate CA and uses the intermediate CA to sign a new SSL certificate with your server’s host name as the common name (the Common Name value is part of what identifies the certificate holder). It is recommended that if you haven’t engaged a widely trusted CA to sign an SSL certificate for your server, you should use the SSL certificate signed by your Open Directory intermediate CA; in Lesson 10 “Configuring OS X Server to Provide Device Management”, you will learn how to use the Trust Profile to configure your iOS devices and OS X computers to trust your Open Directory CA and, by extension, the intermediate CA and the new SSL certificate.

But what about computers and devices that are outside your control and that you cannot configure? When people use computers and devices that are not configured to trust your server’s self-signed SSL certificate or your server’s Open Directory CA or intermediate CA and they try to securely access services on your server, they will still see a message that the identity of your server cannot be verified.

One way to prove your identity is for your server to use an SSL certificate that’s signed by a CA that most computers and devices are configured to trust or trust inherently.

### Deciding What Kind of Certificate to Use

Before going through the process of getting a widely trusted CA to sign a certificate for you, consider the services you'll use with the certificate, as well as the computers and devices that will access those services.

If you use a self-signed certificate, there is no additional server configuration to install the certificate on your server, but you do need to configure each client to trust that self-signed certificate. For a Mac client, this involves not only distributing the certificate to the Mac and adding it to the System keychain but also configuring how the operating system (OS) will trust the certificate.

**NOTE ►** If you use a self-signed certificate and are not able to configure all devices to trust that self-signed certificate, when users encounter a service that uses the self-signed certificate, they will be presented with a dialog informing them that the certificate may not be trustworthy and that to access services they must click Continue. This may undermine your efforts to train users not to automatically trust untrusted, expired, or otherwise invalid certificates.

If you use a certificate signed by a widely trusted CA, you need to generate a certificate signing request (CSR), submit the CSR to a CA, and then import the signed certificate.

Of course, it is possible to use a mix of certificates for different services; if your Websites service responds to multiple host names, you'd want a certificate for each host name that you use for web services secured by SSL.

In all cases, you need to configure your server's services to use the appropriate certificates.

The next section shows you how to obtain a certificate that's signed by a widely trusted CA so that you can use it to prove the identity of your server and to encrypt communications between your server and the users of your server's services.

## Reference 4.2 Configuring SSL Certificates

Your server has a default SSL certificate that's self-signed. That's a good start, but no other computers or devices will trust services that use that certificate without additional configuration. To get a CA to sign a certificate, start by using the Server app to create a certificate signing request. Specific steps to accomplish this objective follow in more detail, but generally they include the following:

- ▶ Generating a new CSR
- ▶ Submitting your CSR to a CA that is generally trusted
- ▶ Importing the signed certificate
- ▶ Configuring your server's services to use your newly signed certificate

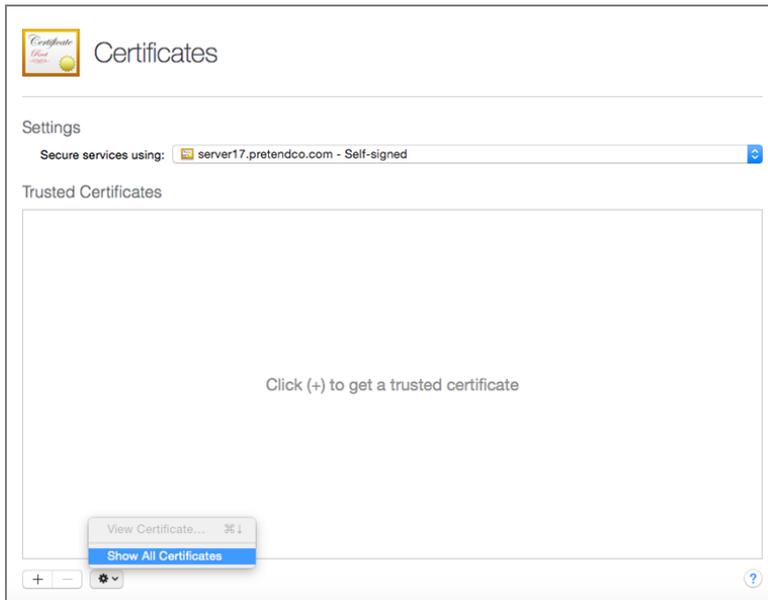
The CA's process of using your CSR and signing your SSL certificate with its own private key includes verifying your identity (otherwise, why would anyone trust the CA if it signed certificates from unverified entities?) and optionally charging you money.

To finish the story, computers and devices can now use your server's services without getting a warning that your SSL certificate is not verified (as long as those computers and devices trust the CA you've chosen to sign your certificate). Additionally, your server and the users of its services can use your server's SSL certificate in the process of encrypting communications for services that use that SSL certificate.

Before you start creating new certificates, take a moment to inspect what you already have.

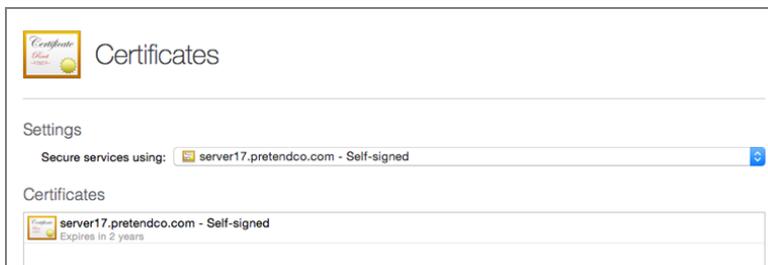
### **Viewing Your Server's Default Certificate**

You can use the Server app to display certificates (if you're logged in at the server, you can also use the Keychain Access app). By default, the Server app doesn't display the default certificate. To display all certificates, select Certificates in the Server app sidebar, and then from the Action (gear icon) pop-up menu, choose Show All Certificates.

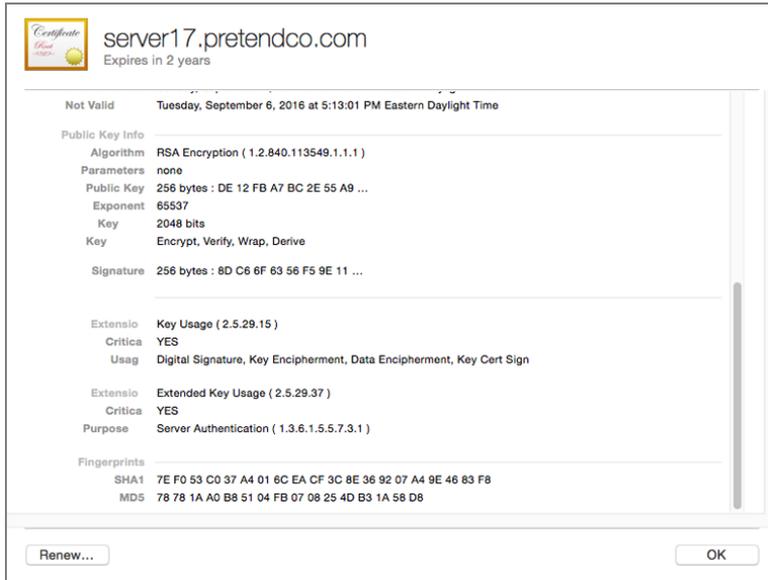


Once Show All Certificates is selected, you see your default certificate. In the following figure, the certificate has the server's host name and expires in two years.

**MORE INFO** ► When you use the Server app Change Host Name Assistant to change your server's host name, it automatically creates a new self-signed certificate for the new host name.

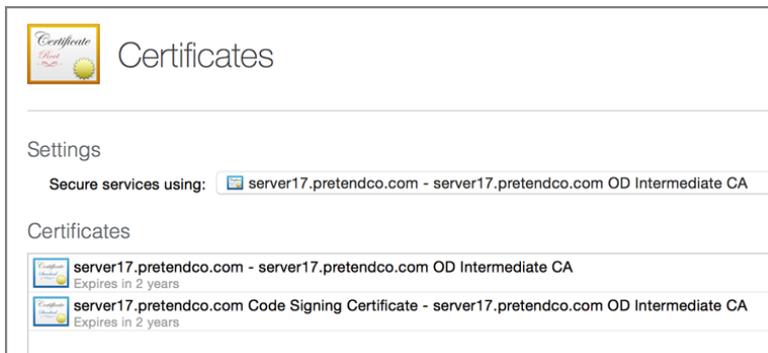


To get more details, double-click the certificate; alternatively, select it, click the Action (gear icon) pop-up menu, and choose View Certificate. When you choose View Certificate, the details of the certificate appear. You'll need to scroll to inspect all of the certificate's information.



Click OK to return to the Certificates pane.

The following figure illustrates what you'd see after you configure your server as an Open Directory master or replica. At first glance, it looks like there is just one additional certificate, the code signing certificate, but the certificate with the server's host name is no longer a self-signed certificate but a certificate signed by your Open Directory CA; that certificate icon is blue, whereas the original self-signed certificate was bronze.



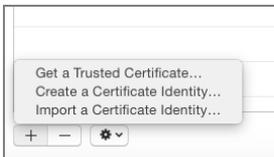
### Explaining Options for Adding New Certificates

In the Server app Certificates pane, if Show All Certificates is not selected in the Action (gear icon) pop-up menu, then the text in the Trusted Certificates field instructs you to “Click (+) to get a trusted certificate.” This is the path to getting a CA to sign a certificate for you.

**NOTE** ► To reveal the menu choice to create a new self-signed certificate, you must first click the Action (gear icon) pop-up menu and choose Show All Certificates.

After Show All Certificates has been selected, click Add (+) to reveal three menu commands:

- Get a Trusted Certificate has the same effect as clicking Add (+) if Show All Certificates is not selected; it allows you to quickly generate a certificate signing request.
- Create a Certificate Identity is the command to choose to create a new self-signed certificate.
- Import a Certificate Identity allows you to import a signed certificate or a certificate and private key that you’ve archived.



### Obtaining a Trusted Certificate

You can choose to get a CA to sign a certificate for you so that users around the world can use your server’s services without being notified that your server’s identity is not verified.

**NOTE** ► In versions of OS X Server previous to 2.2, you need to first create a self-signed certificate and then create a CSR from that certificate. This process has been streamlined as of OS X Server version 2.2. However, be aware that when you use the following procedure to generate a CSR, the Server app generates a public and private key pair, but it doesn’t generate a self-signed certificate.

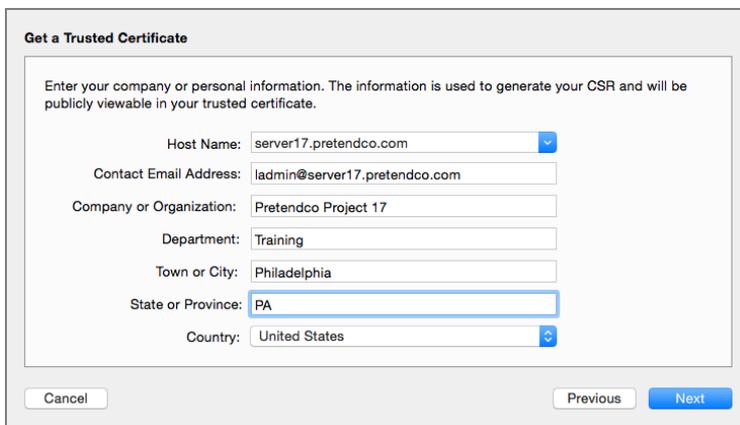
The path to generating a self-signed certificate depends on whether Show All Certificates is selected in the Action (gear icon) pop-up menu:

- ▶ If Show All Certificates is not selected, simply click Add (+) in the Certificates pane.
- ▶ If Show All Certificates is selected, click Add (+), and then choose Get a Trusted Certificate.

After that, you'll see the Get a Trusted Certificate wizard.

In the next pane you can enter all the information that is necessary to establish an identity. A CA uses these details to verify your identity.

In the Host Name field, enter the host name you'll use for the services that will use this certificate. Use your organization's full legal name for the Company or Organization field, or if it's for personal use, just use your full name. The Department field is flexible; you can enter information such as your department name, but you should enter some value. To be fully compliant with standards, do not abbreviate your state or province. The following figure illustrates all of the fields completed.

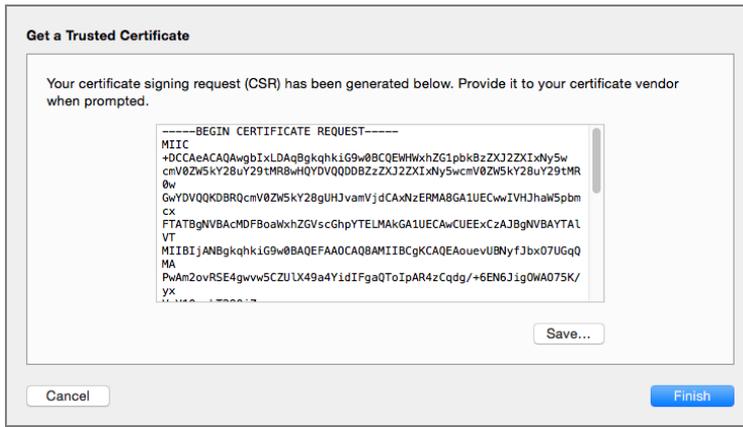


The screenshot shows a window titled "Get a Trusted Certificate". Inside the window, there is a text box with the instruction: "Enter your company or personal information. The information is used to generate your CSR and will be publicly viewable in your trusted certificate." Below this instruction are several input fields:

- Host Name: server17.pretendco.com (dropdown menu)
- Contact Email Address: ladmin@server17.pretendco.com (text field)
- Company or Organization: Pretendco Project 17 (text field)
- Department: Training (text field)
- Town or City: Philadelphia (text field)
- State or Province: PA (text field)
- Country: United States (dropdown menu)

At the bottom of the window, there are three buttons: "Cancel", "Previous", and "Next".

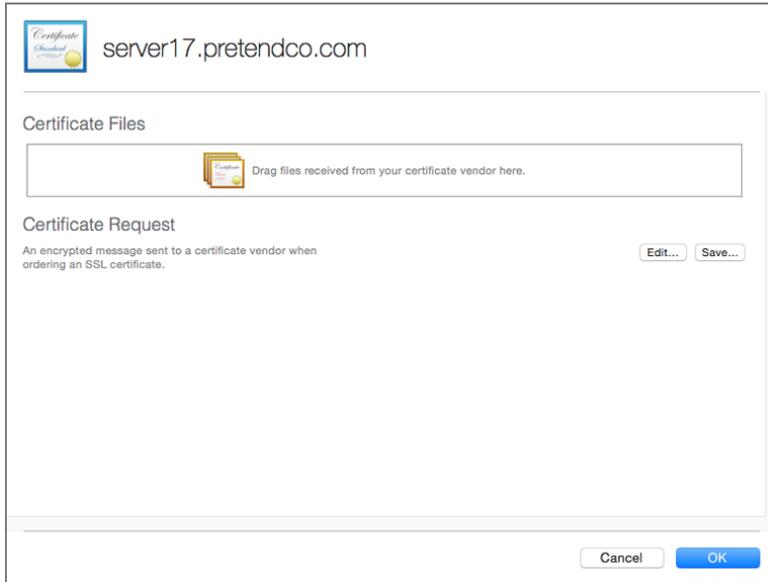
The next pane displays the text of your CSR, which you will submit to the CA of your choice. You can wait and access this text later, or you can select and copy this text, or click Save, now.



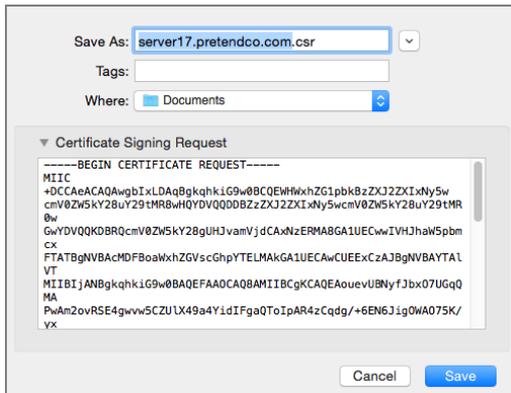
After you click Finish, the Server app displays the pending request.



If you didn't copy the text of your CSR earlier, you can access it again: Select the certificate that's marked "Pending," click the Action (gear icon) pop-up menu, and choose View Certificate Signing Request (or just double-click the pending certificate item).



Your course of action depends on how your CA accepts CSRs. If your CA allows you to upload a text file, then use the Save dialog to save the CSR as a text file. If your CA requires you to paste the text of the CA into a web form, click the disclosure triangle, and then copy the text of the CSR.



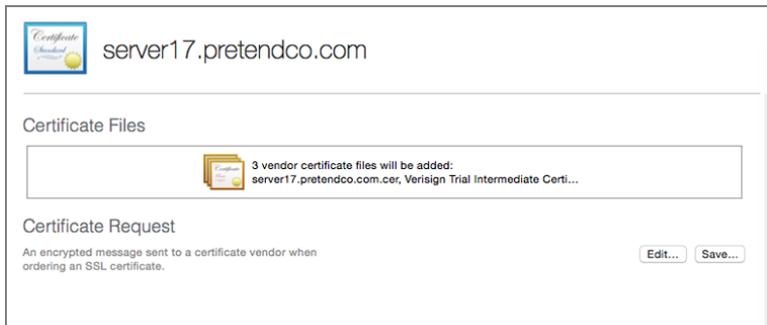
You need to choose an appropriate CA for your organization's needs (choosing a CA is outside the scope of this guide), send the CSR to the CA, and prove your identity to the CA. After some period of time, you will receive a signed certificate from the CA.

## Importing a Signed Certificate

Once you receive the signed certificate from the CA, it's time to import it with the Server app. If you are still at the list of certificates, double-click your pending certificate to reveal the field into which you can drag your signed certificate.

**NOTE** ► If the CA provides you with the certificate in text form rather than in a separate file, you'll need to convert that text into a file. A quick way to do this is to select and copy the text, open TextEdit, press Command-N to create a new file, and choose Format > Make Plain Text (if that is an available command). Paste the text into the text file, and save it with a .cer extension.

Double-click the pending CSR, and drag the file containing a signed certificate, as well as any ancillary files provided by the CA, into the Certificate Files field (this is also where you could import a certificate and private key that you've exported with Keychain Access). Once the certificate is in the Certificate Files field, its color will be blue, as long as the top of the certificate chain is a root CA that your server trusts.



**NOTE** ► If you click Edit next to Certificate Request and then click Edit in the confirming dialog, a new public and private key pair and a new CSR will be generated, and you'll lose the original CSR.

Click OK to save your changes.

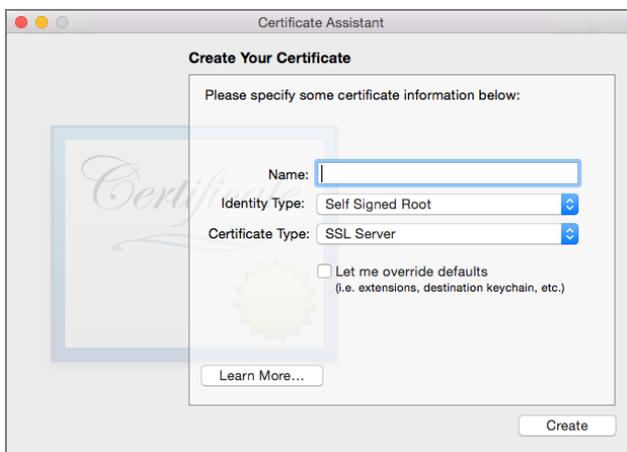
## Generating a Self-Signed Certificate

In addition to generating a CSR, you can also use the Server app to generate a new self-signed certificate. This is useful if your server offers services at an alternative host name that corresponds to your server's Internet Protocol version 4 (IPv4) address or another IPv4 address that your server is configured to use and if you have the ability to configure computers and iOS devices to trust the self-signed certificate.

**MORE INFO** ► In versions of the Server app prior to version 2.2, the workflow was to create a self-signed certificate, then generate a CSR, and finally replace the self-signed certificate with the signed certificate. In version 2.2 and later, the Server app does not offer a way to replace a self-signed certificate with a signed certificate.

In the Certificates pane, when you click Add (+) and choose Create a Certificate Identity, you see a blank Name field.

**NOTE** ► The Show All Certificates option must be selected in the Action (gear icon) pop-up menu for the Create a Certificate Identity command to be available from the Add (+) button.



Enter the host name for the self-signed certificate, and then click Create.

**NOTE** ► You can select the “Let me override defaults” checkbox if you have more specific needs, but for most purposes, the defaults will suffice.

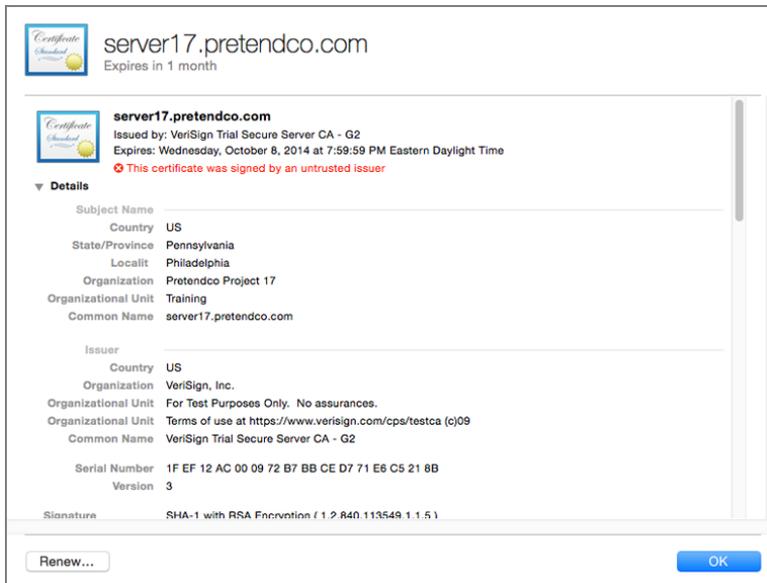
At the warning that you are about to create a self-signed certificate, click Continue.

At the Conclusion window, click Done. Finally, click either Always Allow or Allow to allow the Server app to copy the public and private key pair and the certificate from your login keychain to the System keychain and to `/private/etc/certificates/`.

You’ll see the certificate in the Certificates field, as long as the Show All Certificates option is selected in the Action (gear icon) pop-up menu.

## Inspecting a Certificate

You can inspect your certificates with the Server app, as well as with the System keychain of your server computer (the System keychain contains items that are not user specific and that are available to all users of a system). The following figure shows a certificate that's been signed by a CA for test purposes. Note that the OS has not yet been configured to trust the CA that signed this certificate.



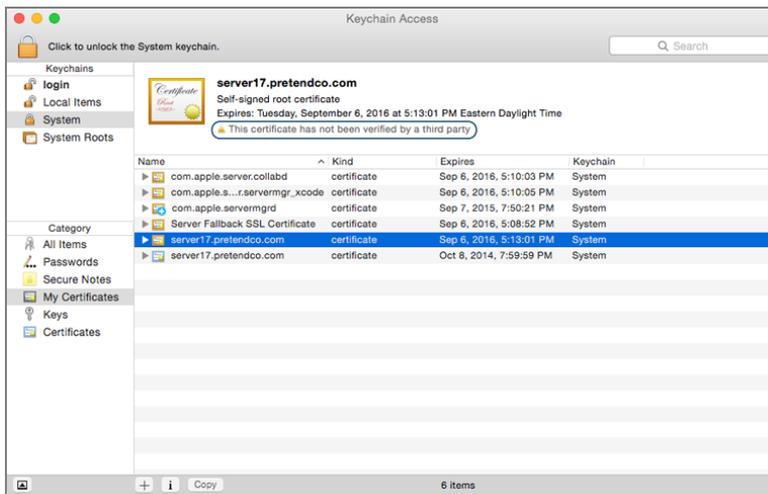
You can also use Keychain Access to inspect a certificate and its associated private key. Because the certificate and private key are stored in the System keychain on the server, you need to log in directly on your server (or use a screen-sharing method to control your server) to use Keychain Access to access the private key.

Keychain Access is in the /Applications/Utilities/ folder on your startup volume; you can use Spotlight or Launchpad to search for it (in Launchpad, it is in the folder named Other). Select the My Certificates category to filter the items that Keychain Access displays. If necessary, toggle the show/hide button in the lower-left corner of the Keychain Access window until you can see all keychains. Select the System keychain to show items that are for the entire system, not just for the user who is currently logged in.

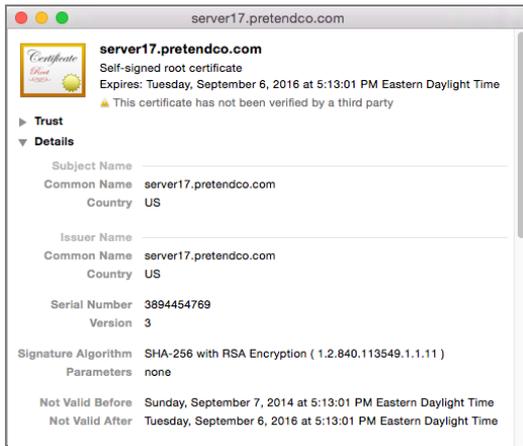
At least three items are listed (if you provided an Apple ID for push notifications, you will see more items):

- ▶ `com.apple.servermgrd`, which is used for remote administration with the Server app
- ▶ A certificate named Server Fallback SSL Certificate, which the Server app automatically uses if the default SSL certificate is removed
- ▶ An SSL certificate with the host name of your server

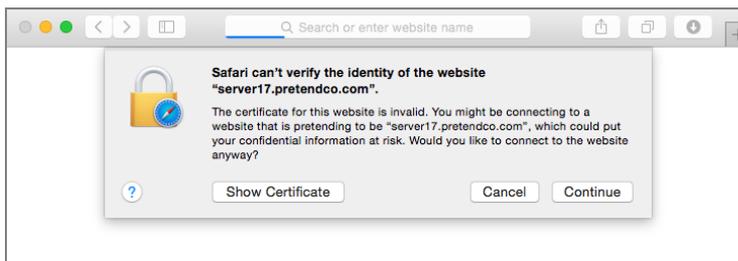
When you select a certificate that is not signed by a trusted CA, Keychain Access displays a warning icon, along with the text that explains the issue. In the following figure, the warning for the self-signed certificate is “This certificate has not been verified by a third party.”



If you double-click your default self-signed SSL certificate to open it, you’ll see a warning icon and the text “This certificate has not been verified by a third party.”



If a service on your server uses this self-signed certificate, when users attempt to use services that use that SSL certificate, they may be warned that your SSL certificate is not trusted, as shown in the following figure.



It's recommended to train your users that when they see an SSL warning, they should *not* continue using the service that uses the unverified SSL certificate.

### Archiving Your Certificate

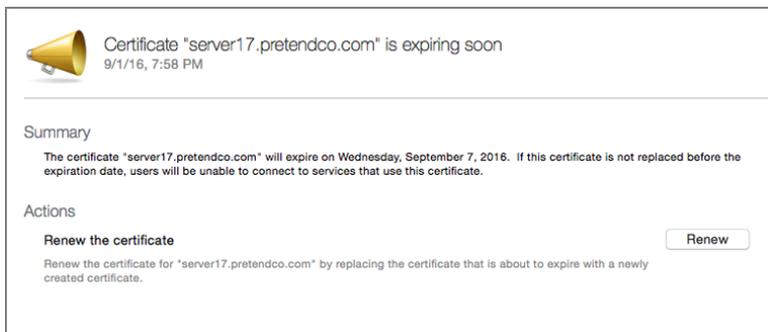
Whether you have a self-signed certificate or a certificate signed by a CA, you should take steps to archive your certificate and its private key. You may need to reinstall your server in the future, or an administrator might accidentally remove your certificate and its private key; if you have an archive of your certificate and private key, you can easily use the Server app to re-import your certificate and its private key.

You use the Keychain Access app to export your certificate and private key. Keychain Access prompts you to specify a password to protect your private key; it is recommended that you use a strong password.

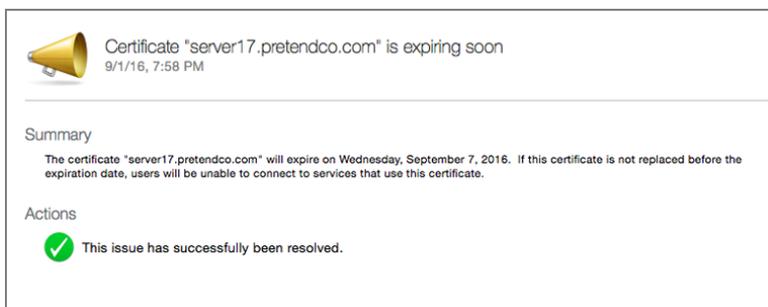
You use the Server app to import the certificate and private key. You need to provide the password that was entered when the certificate was exported in the first place; otherwise, you will not be able to import.

### Renewing Your Certificate

SSL certificates do not last forever. Luckily, it is simple to renew SSL certificates. The Server app issues an alert when an SSL certificate expiration date approaches. To renew a self-signed SSL certificate, simply click Renew when viewing the certificate in the Certificates pane or when viewing the alert.

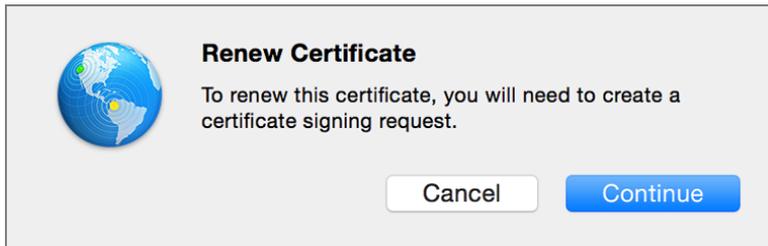


Once you click Renew, the Server app takes care of renewing the certificate, and the alert displays that the issue has been resolved.



**NOTE** ► Do not click Renew for an Open Directory CA because this causes changes to the CA properties, and your Open Directory intermediate CA will no longer be signed by a trusted authority.

If you have a certificate signed by a widely trusted CA, when you click Renew, you will see the message that you need to generate a new CSR. See the earlier section “Obtaining a Trusted Certificate” on page 131 for more details.



### Configuring OS X Server Services to Use a Certificate

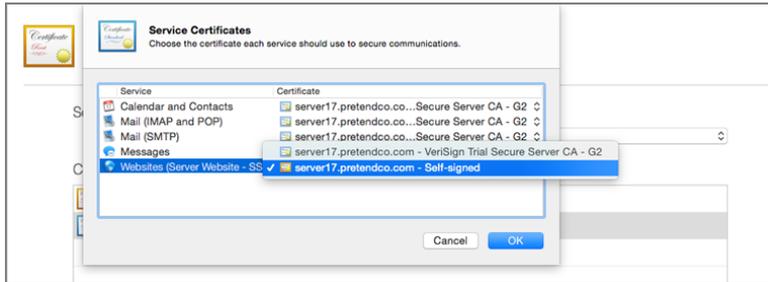
Once you have taken steps to obtain a signed certificate or create a new self-signed certificate or have configured your server as an Open Directory server, you should use the Server app to configure services to use that certificate. You start in the Certificates pane of the Server app.

With the pop-up menu, you can do either of the following:

- ▶ Choose one certificate to specify that all services use that certificate.
- ▶ Choose Custom to configure each service separately to use or not use a certificate.



The following figure shows an example of choosing Custom and then editing the value for the default secure site of the Websites service. Note that there are some extra certificates in the figure. This illustrates that you can configure your server to respond to requests at multiple host names, create a certificate for each host name, and configure each secure site to use the appropriate certificate.



You can use the Server app to configure the following OS X Server services to use SSL:

- ▶ Calendar and Contacts
- ▶ Mail (IMAP and POP)
- ▶ Mail (SMTP)
- ▶ Messages
- ▶ Open Directory (appears only after starting Open Directory services)
- ▶ Websites

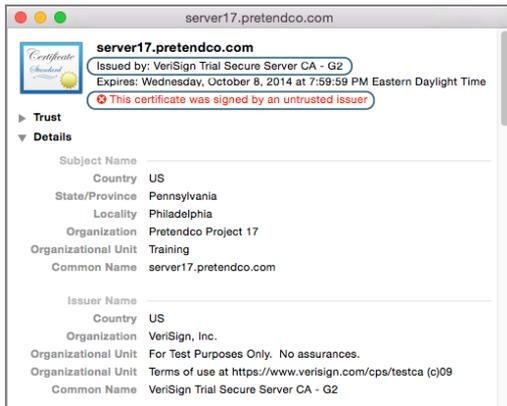
You will see in Lesson 20 “Hosting Websites” that you can granularly specify an SSL certificate for each website you host, and you can use the Profile Manager pane to specify the SSL certificate to use for the Profile Manager service.

A few other services use SSL but do not appear in the Server app:

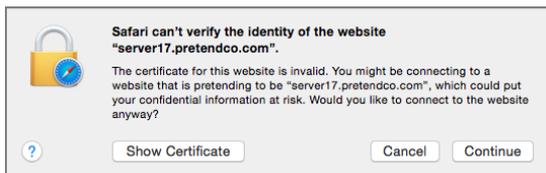
- ▶ `com.apple.servermgrd` (for remote administration with the Server app)
- ▶ VPN
- ▶ Xcode

### Following the Certificate Chain

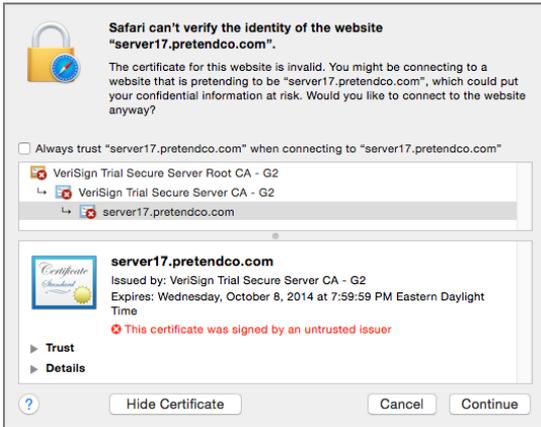
When choosing a CA to use, make sure that it’s a root CA that most computers and devices are configured to trust. It’s not useful for you to have a CA sign your certificate if not many computers or devices will trust that certificate. As an example, the following figure shows how an SSL certificate signed by a trial CA appears in Keychain Access.



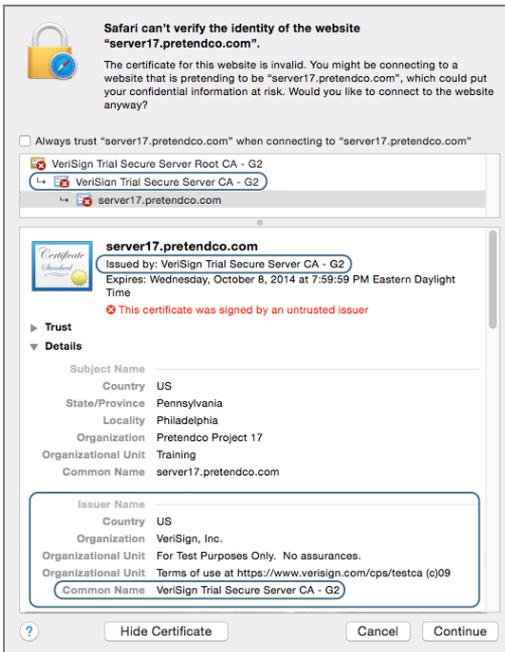
You can see that the “Issued by” field near the top of the window shows VeriSign Trial Secure Server CA – G2. Note the red X icon and the text “This certificate was signed by an untrusted issuer.” This is a CA that is by default not trusted by computers and devices, so even if you used this signed certificate for OS X Server services, the people who access your services would experience trouble. In some cases, the service might silently fail, or the user may be alerted that the identity of the service cannot be verified. The following figure illustrates that on a client Mac Safari notifies the user that Safari can’t verify the identity of the website.



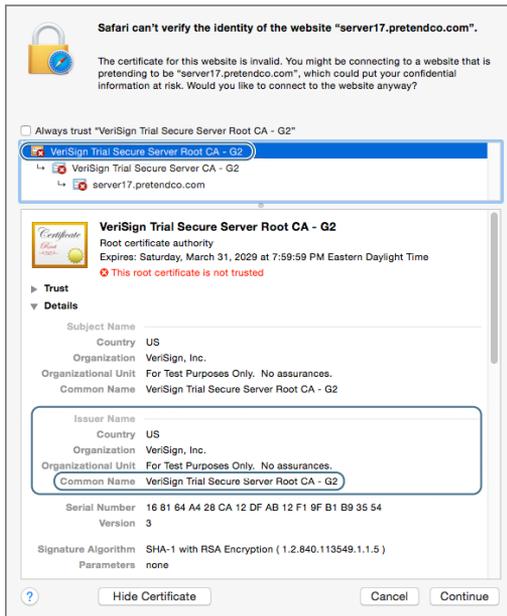
If you click Show Certificate, Safari displays the certificate chain. The following figure shows what you see when you select the server’s certificate at the bottom of the certificate chain: that the certificate was signed by an untrusted issuer.



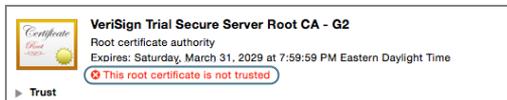
The following figure illustrates that if you click the Details disclosure triangle, you'll see information about the identity of the certificate holder, as well as information about the issuer (the entity that signed the certificate). In this case, the issuer's common name is VeriSign Trial Secure Server CA – G2.



When you select the certificate in the middle of the certificate chain, you see that this is an intermediate CA; the window states “Intermediate certificate authority,” and the Issuer Name information shows you that the common name of the issuer (or signer) is VeriSign Trial Secure Server Root CA – G2.



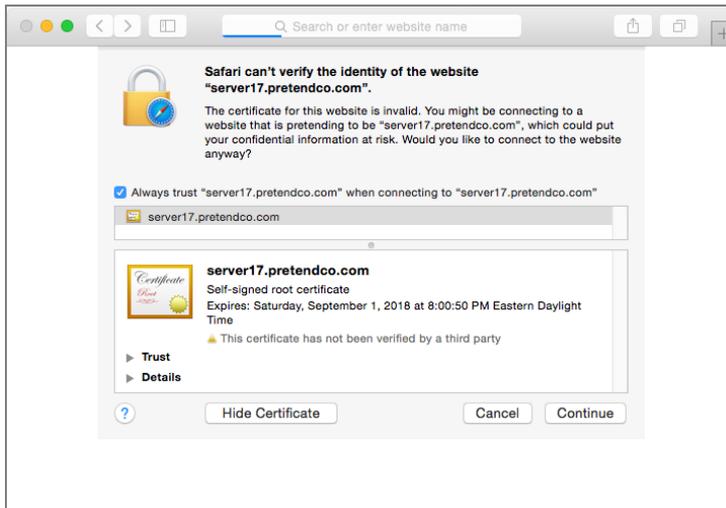
Finally, when you select the certificate at the top of the certificate chain, you see that this is a root CA; the window states “This root certificate is not trusted.” This root CA is not in this computer’s System Root keychain, so Safari doesn’t trust the intermediate CA, and it doesn’t trust the server17.pretendco.com certificate either.



Since that example root CA is for trial use only, it is not recommended to configure your Mac to always trust it outside of a learning or testing environment.

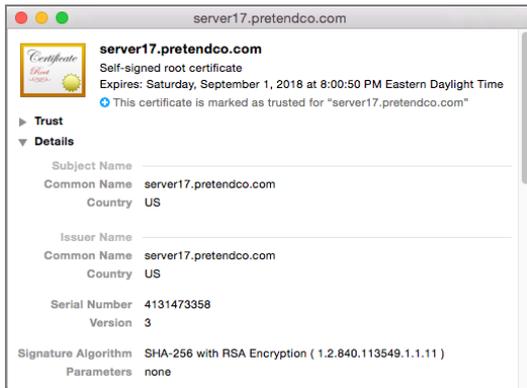
## Configuring Trust

You can configure your Mac to always trust a certificate for the currently logged-in user. Returning to the previous example of your server using its self-signed SSL certificate for a website, you can click Show Certificate and then select the “Always trust...” checkbox.

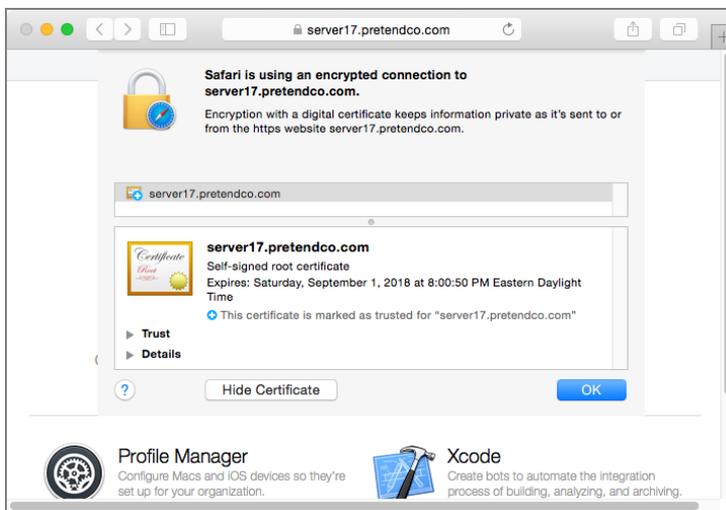


After you select “Always trust...” OS X asks for your login credentials. After you successfully authenticate, OS X adds the certificate to your personal login keychain and configures your system to always trust the certificate for SSL purposes so that your Mac trusts it when you are logged in with the account that you were logged in as when you clicked the “Always trust...” checkbox. This will not affect any other computers or devices or any other users who log in to that Mac.

In Keychain Access, you can open and inspect the self-signed certificate you just added. Note the blue plus (+) icon with the text that states the certificate is marked as trusted for server17.pretendco.com.

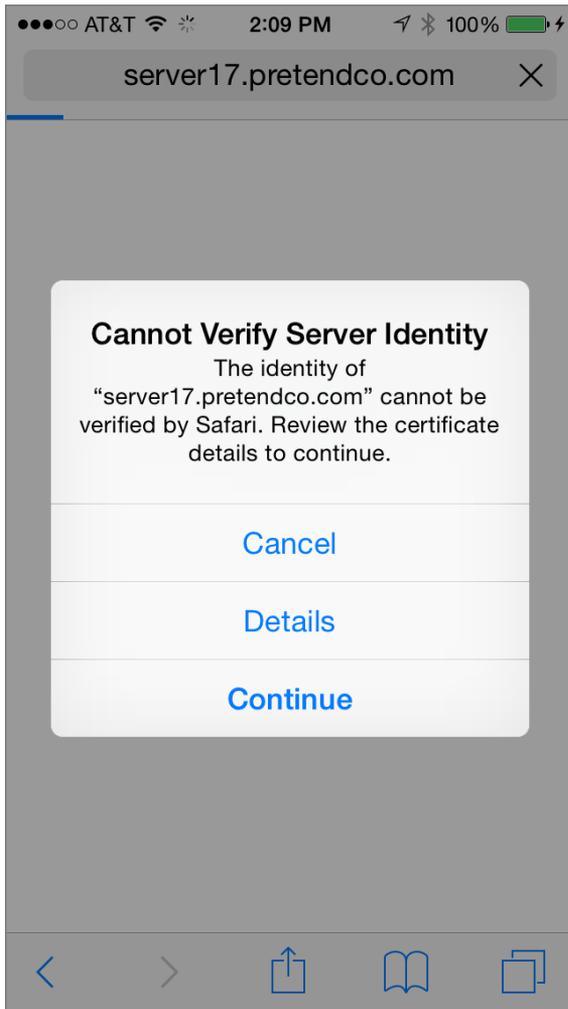


After you visit the site again in Safari, if you click the encryption icon in the Address and Search field and then click Show Certificate, you see similar information.

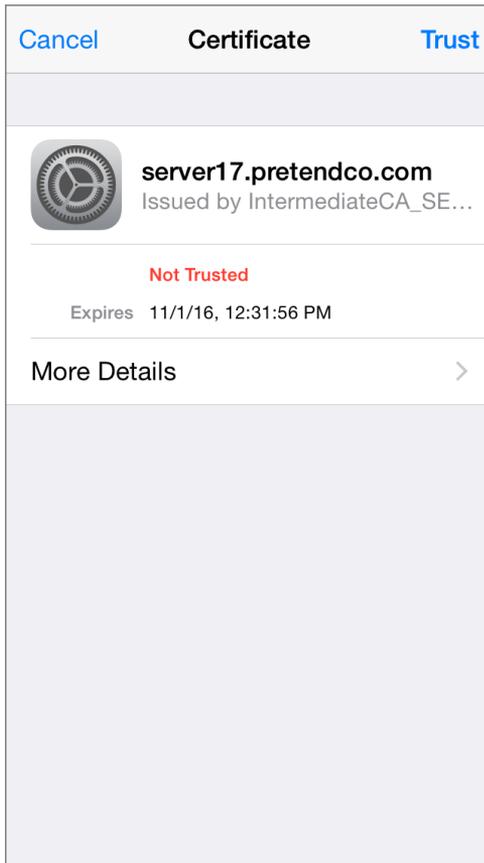


A further option for Mac computers is to download and install the certificate in the System keychain, with the "Always trust..." checkbox selected for SSL. Keep in mind that you would need to do this for *every* Mac that uses SSL-enabled services from your server.

For an iOS device, when you open Safari to a page protected by the server's self-signed certificate, you can tap Details.



Then tap Trust.



Now your iOS device is configured to trust that certificate.

Note that you can use a configuration profile to distribute a certificate to Mac computers and iOS devices. This automatically configures the device to trust the certificate. See Lesson 11 “Managing with Profile Manager” for more information about profiles.

See “Exercise 4.3 Configure Your Administrator Computer to Trust an SSL Certificate” on page 159 for complete instructions.

## Reference 4.3 Troubleshooting

Certificate Assistant uses the IPv4 address of the Mac from which you run the Server app, so if you’re using an administrator computer to configure a remote server and generate a

new self-signed certificate, be sure to use the server's host name and IP address where appropriate.

When you configure your server as an Open Directory server, if you have a self-signed certificate with your server's host name in the certificate's Common Name field, the Server app replaces the original self-signed SSL certificate with a new certificate. This new certificate will be signed by a newly created intermediate CA associated with your server's Open Directory service.

However, if you have a certificate with your server's host name in the certificate's Common Name field and the certificate is signed by a CA or an intermediate CA (that is not associated with your Open Directory service), then the Server app doesn't replace it with a new one signed by the Open Directory intermediate CA (however, the Server app still creates the Open Directory CA and intermediate CA).

Each certificate has an expiration date; if the current date is later than a certificate's expiration date, the certificate is not valid.

**MORE INFO** ► Some files associated with certificates are stored in `/private/etc/certificates/`, and possibly `/private/var/root/Library/Application Support/Certificate Authority/`, on your server.

## Exercise 4.1

### Examine the Default SSL Certificate

#### ► Prerequisites

- All exercises in Lesson 1 “Installing OS X Server”
- “Exercise 2.1 Create DNS Zones and Records” on page 71

In this exercise, you will examine the default self-signed certificate.

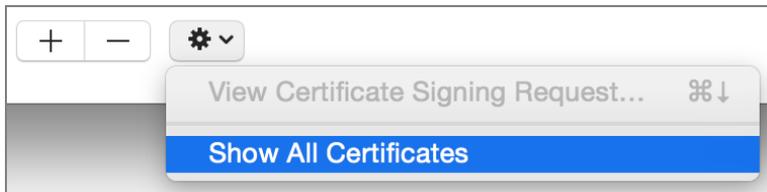
- 1 Perform these exercises on your administrator computer. If you do not already have a connection to your server computer with the Server app on your administrator computer, then connect to it with the following steps: Open the Server app on your administrator computer, choose `Manage > Connect to Server`, select your server, click `Continue`, provide administrator credentials (Administrator Name: `ladmin` Adminis-

trator Password: **ladminpw**), deselect the “Remember this password” checkbox, and then click Connect.

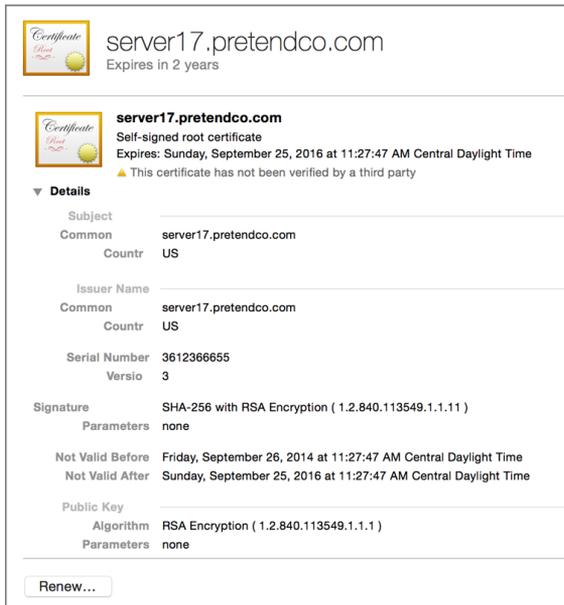
- 2 In the Server app sidebar, select Certificates.
- 3 Note that by default your server’s services use a certificate that is self-signed.



- 4 Click the Action (gear icon) menu, and choose Show All Certificates.



- 5 Select the self-signed certificate.
- 6 View the details of the certificate. Double-click the self-signed certificate, or click the Action menu and choose View Certificate.



## 7 Click OK return to the Certificates pane.

Note that there is little identifying information associated with this certificate. For example, there is no email address, organization name, department, or city. By default, no other computer or device trusts this self-signed certificate. To use this self-signed certificate to secure your server's services, you could configure your client computers and devices to trust this certificate.

Alternatively, you could click the Add (+) button and choose Get a Trusted Certificate, send the resulting certificate signing request to a widely trusted certificate authority to sign, and then import the signed certificate. However, this is outside the scope of this guide, so the next exercise is a compromise between using a self-signed certificate with little information and using a certificate signed by a widely trusted CA.

## Exercise 4.2 Configure an Open Directory Certificate Authority

When you configure your server as an Open Directory (OD) master, the Server app automatically creates an OD CA, an intermediate CA, a signed certificate, and a code signing certificate that you can use with the Profile Manager service. When you enroll your Mac

computer or your iOS device with your server’s Profile Manager service, your computer automatically trusts your server’s OD CA. Additionally, if you bind your Mac to your OD server, it automatically trusts your server’s OD CA. This guide has not yet covered binding or enrolling, so in “Exercise 4.3 Configure Your Administrator Computer to Trust an SSL Certificate” on page 159 you will use Safari to configure your administrator computer to trust your server’s OD CA.

In this exercise, you will configure your OD CA. You will examine the new CA, the intermediate CA, and two new certificates and verify that the Server app automatically removes your server’s old default self-signed certificate, updates services to use the certificate signed by the intermediate CA, and configures your server to trust the new certificates.

### Configure Open Directory

Because the Server app creates keychain entries on your server, perform the following steps on your server.

Correct DNS records are crucial to the proper functioning of Open Directory services, so double-check DNS before starting the Open Directory service.

- 1 On your administrator computer, quit the Server app if it is open.
- 2 On your server computer, open Network Utility (use Spotlight if necessary).
- 3 Click the Lookup tab.
- 4 Enter your server’s host name in the field, and then click Lookup.
- 5 Confirm that your server’s IPv4 address is returned.
- 6 Enter your server’s primary IPv4 address in the field, and then click Lookup.
- 7 Confirm that your server’s host name is returned.

Once you’ve confirmed your DNS records, configure your server as an Open Directory master.

- 1 On your server, open the Server app, select your server, click Continue, provide administrator credentials (Administrator Name: **admin**, Administrator Password: **adminpw**), deselect the “Remember this password” checkbox, and then click Connect.
- 2 If the Server app does not display the list of advanced services, hover the pointer above the word “Advanced” in the sidebar, and then click Show.

- 3 Select Open Directory.
- 4 Click On to turn on the Open Directory service (or in the Server app sidebar, Control-click Open Directory, and choose Start Open Directory Service).
- 5 Select “Create a new Open Directory domain,” and click Next.
- 6 In the Directory Administrator pane, deselect the checkbox “Remember this password in my keychain.”

The screenshot shows a form with the following fields and options:

- Name: Directory Administrator
- Account Name: diradmin
- Password: (empty field with a blue border)
- Verify: (empty field)
- Remember this password in my keychain

- 7 Configure a password.

If your server is not accessible from the Internet, in the Directory Administrator pane, enter **diradminpw** in the Password and Verify fields.

Of course, in a production environment, you should use a secure password and consider using an account name different from the default “diradmin” so that it is more difficult for unauthorized people to guess the username and password combination.

- 8 Click Next.
- 9 In the Organization Information pane, enter the appropriate information.

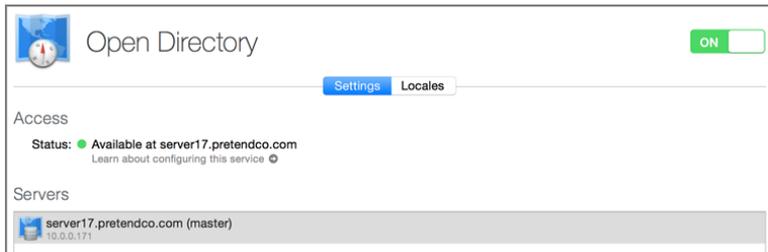
If the following fields do not already contain the information shown, enter it, and click Next.

- ▶ Organization Name: **Pretendco Project *n*** (where *n* is your student number)
- ▶ Admin Email Address: **ladmin@servern.pretendco.com** (where *n* is your student number)

- 10 View the Confirm Settings pane, and click Set Up.

The Server app displays its progress in the lower-left corner of the Confirm Settings pane.

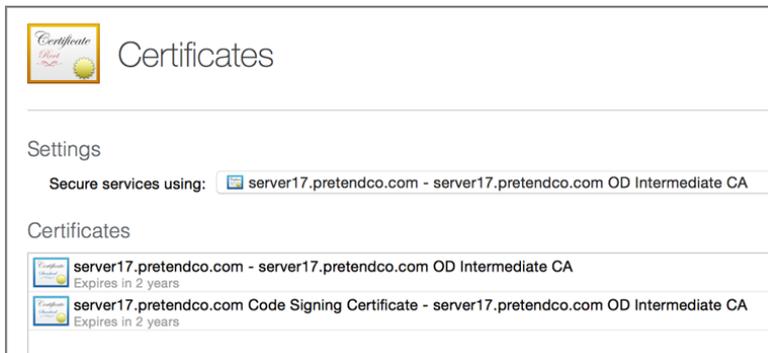
When it has completed the configuration, the Server app displays the Settings tab of the Open Directory pane, with your server listed as the master in the Servers list.



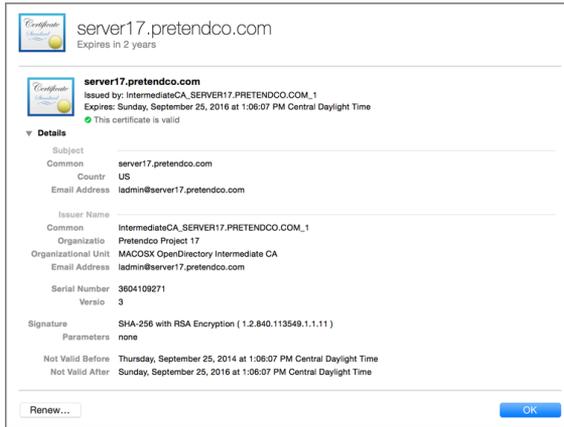
### Inspect the OD Certificates

Inspect the certificates that the Server app automatically created.

- 1 In the Server app sidebar, select Certificates.
- 2 Click the Action (gear icon) pop-up menu, and choose Show All Certificates.
- 3 Confirm that the “Secure services using” pop-up menu is no longer set to a self-signed certificate but rather a certificate signed by your server’s OD intermediate CA.



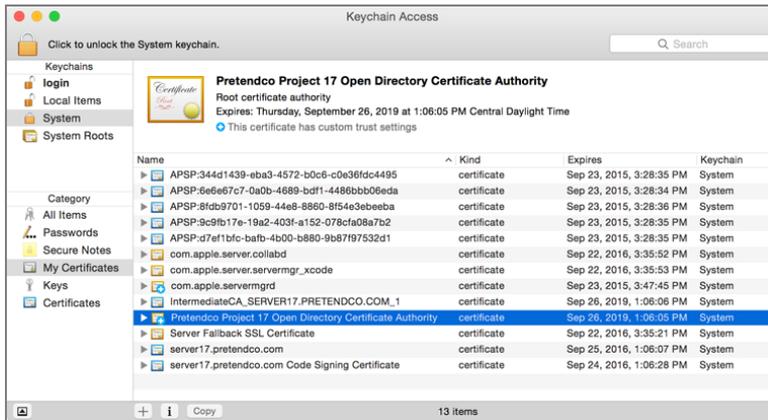
- 4 Confirm that the self-signed certificate is no longer listed in the Certificates field.
- 5 Double-click the certificate with your server’s host name, signed by your OD intermediate CA (the first entry in the Certificates field).



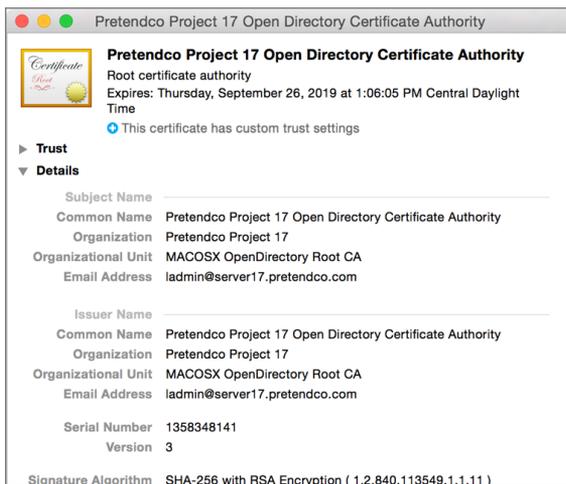
- 6 Confirm that in the Issuer Name section, the first field (which is the common name) has a value made up of the following strings:
  - ▶ “IntermediateCA\_”
  - ▶ Your server’s host name in all capital letters
  - ▶ “\_1”
- 7 Click OK to close the certificate information pane.
- 8 Double-click the code signing certificate (the second entry in the Certificates field).
- 9 Confirm that this is also issued by your OD intermediate CA.

Use Keychain Access to inspect your OD CA, your OD intermediate CA, and the two signed certificates.

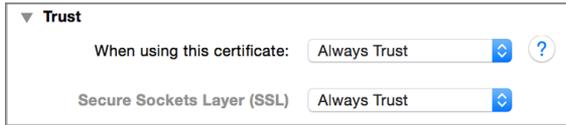
- 1 On your server, use a Spotlight search to open Keychain Access.
- 2 In the Keychains column, select System.
- 3 In the Category column, select My Certificates.
- 4 Select your OD CA. Its name is Pretendco Project *n* Open Directory Certificate Authority (where *n* is your student number).



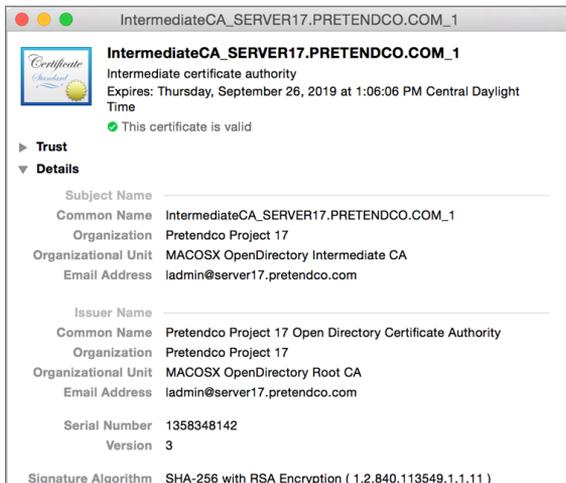
- 5 Double-click your OD CA to examine it.
- 6 Confirm that the second line of text identifies it as “Root certificate authority” and that the Subject Name information matches the Issuer Name information.



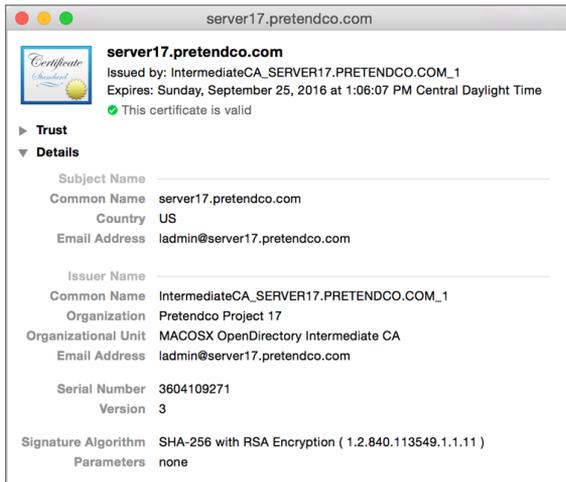
- 7 Note that the certificate’s color is bronze, which signifies that it is a root certificate.
- 8 Click the Trust disclosure triangle to display more details.
- 9 Confirm that your server is set to always trust this certificate.



- 10 Close your OD CA.
- 11 Double-click your OD intermediate CA.
- 12 Confirm that its second line of text identifies it as “Intermediate certificate authority.” Because your server trusts your OD CA and your OD CA signed this intermediate CA, this certificate is marked as valid with a green checkmark.  
Note that the color of the certificate is blue, which signifies that it is an intermediate or leaf certificate.



- 13 Close your OD intermediate CA.
- 14 Double-click the certificate with your server’s host name.
- 15 Confirm that the second line of text indicates that it is signed by your OD intermediate CA. Your server is configured to trust your OD CA, which signed your OD intermediate CA, which signed this certificate, so it is marked as valid with a green checkmark.



**16** Double-click your code signing certificate, inspect it, and close it.

**17** Quit Keychain Access.

In this exercise, you configured your server to be an Open Directory master. The Server app automatically configured a new OD CA, intermediate CA, and two new certificates; it removed your server's old default self-signed certificate, and it updated services to use the certificate signed by the intermediate CA. It automatically configured your server to trust its own OD CA, which means that your server also trusts the OD intermediate CA and the two other certificates that are signed by the OD intermediate CA.

## Exercise 4.3

### Configure Your Administrator Computer to Trust an SSL Certificate

#### ► Prerequisite

- “Exercise 4.2 Configure an Open Directory Certificate Authority” on page 152

**NOTE** ► If you obtained a certificate from a widely trusted CA, you do not need to perform this exercise.

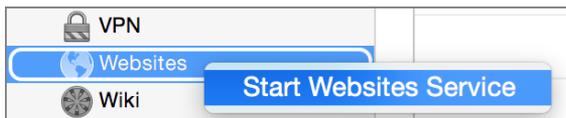
In a production environment, it is best to use a valid SSL certificate that's been signed by a trusted CA. If that isn't possible, you should configure your users' computers and devices to trust your server's certificate so that your users do not get into the habit of configuring their devices to trust unverified SSL certificates.

This lesson shows you how to configure an individual computer to trust your server's OD CA; it is beyond the scope of this exercise to show you how to replicate the end result on multiple computers and devices.

### Turn On the Web Service Temporarily

Turn on your server's Websites service so you can quickly access the SSL certificate your server's services use.

- 1 In the Server app sidebar, Control-click Websites, and then choose Start Websites Service.



### Visit Your Server's Website Protected by SSL

In this exercise, you will use your administrator computer and confirm that you are using your server's DNS service; otherwise, you will not be able to connect to its web service using its host name. Then you'll open Safari to your server's default HTTPS website. Finally, you'll configure your administrator computer to trust the SSL certificate.

- 1 On your administrator computer, open System Preferences.
- 2 Open the Network pane.
- 3 Select the active network service, and confirm that your server's IP address is listed for the DNS Service value.

If you are using Wi-Fi, you need to click Advanced and then click the DNS tab to view the DNS Service value.

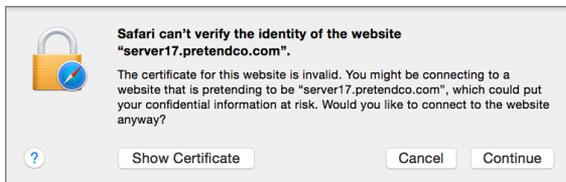
- 4 Quit System Preferences.

- 5 On your administrator computer, open Safari, and in the Address and Search field, enter <https://servern.pretendco.com> (where *n* is your student number).



- 6 Press Return to open the page.

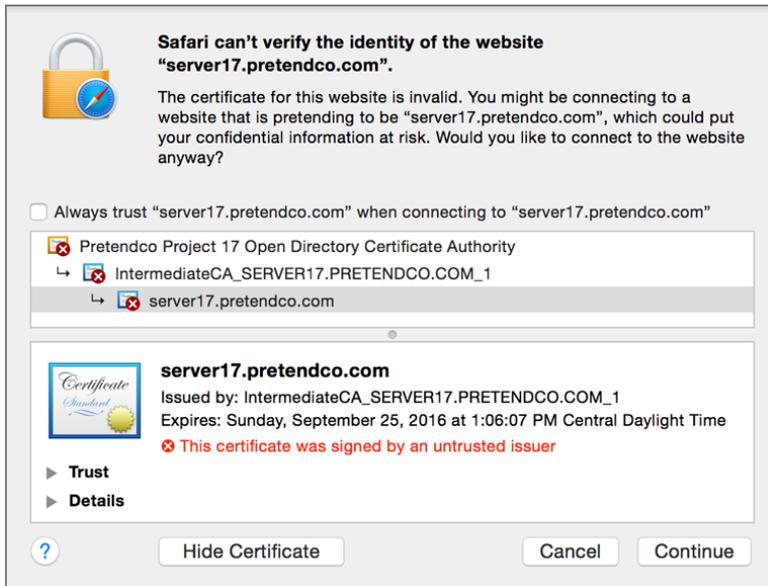
Your certificate is not signed by a CA that your administrator computer is configured to trust, so you'll see the message that Safari can't verify the identity of the website.



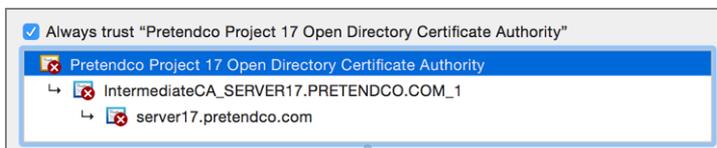
### Configure Your Administrator Computer to Trust This SSL Certificate

Once you see the dialog that Safari can't verify the identity of the website, you can click Show Certificate and configure the currently logged-in user to trust the SSL certificate used by the website.

- 1 Click Show Certificate.
- 2 Note that the certificate with your server's host name is marked in red, "This certificate was signed by an untrusted issuer."



- 3 In the certificate chain, select your OD CA.
- 4 Click the Details disclosure triangle, and inspect the details.
- 5 Select the checkbox “Always trust ‘Pretendo Project *n* Open Directory Certificate Authority” (where *n* is your student number).



- 6 Click Continue.
- 7 Provide your login credentials, and click Update Settings.  
This updates the settings for the currently logged-in user; this does not affect any other user on this computer.
- 8 Confirm the Safari Address and Search field displays a lock icon, which indicates that the page was opened using SSL.

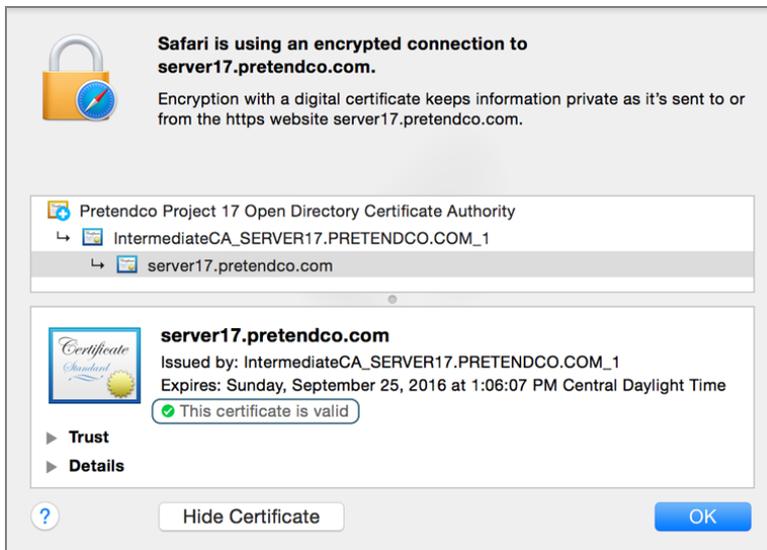


- 9 Keep Safari open for the next section of this exercise.

### Confirm That Your Mac Trusts the SSL Certificate

To view the SSL certificate the Websites service is using, perform the following steps.

- 1 In the Safari Address and Search field, click the lock icon.
- 2 In the pane that informs you that Safari is using an encrypted connection, click Show Certificate.
- 3 Confirm that the certificate is listed as valid with a green checkmark.



- 4 Press Command-Q to quit Safari.

You confirmed that the Websites service uses the SSL certificate you configured in the previous exercise. You confirmed that by trusting a CA, you trust a certificate that was signed by an intermediate CA that was signed by the CA (at least for the currently logged-in user).

## Exercise 4.4 Clean Up

To ensure that the rest of the exercises are consistent, turn off the Websites service.

- 1 In the Server app sidebar, select the Websites service, and click Off to turn the service off.
- 2 Confirm that no green status indicators appear next to the Websites service. This indicates that the service is off.

You are ready to complete the tasks of any other lesson's exercises.

*This page intentionally left blank*

# Index

## A

- About This Mac window
  - confirming computer capability to run OS X Server, 26
- Access control, 589
  - (see also Permissions)
  - configuring for sharing, 429
  - for messages federation, 662
  - for services, 242
  - for users of Messages services, 660
  - for websites, 578
  - for wikis, 612
  - groups used to manage access to files and services, 217
  - inspecting access to services, 244-247
  - managing access to services, 241
  - managing access to services manually, 216
  - managing website access, 578
  - removing custom access rules for Messages service, 661
  - testing access restrictions for Messages service, 660
  - troubleshooting service access, 219
  - viewing website access log, 581
- Access control entries (see ACEs (access control entries))
- Access control lists (see ACLs (access control lists))
- Access control, DNS services
  - cleaning up permissions, 90
  - configuring permissions, 87
  - configuring recursive lookup restrictions, 85-87
  - confirming restrictions, 89
  - inspecting, 88
  - overview of, 84
- Access pane, Server app
  - adding custom access rules, 102
  - confirming access rules are in effect, 119
  - confirming custom access rules, 121
  - inspecting DNS access permissions, 88
  - modifying custom access rules, 120
  - overview of, 100, 116
  - restoring default access rules, 121
  - specifying access for users and groups, 216
- Access tab, Server app
  - modifying default access rules, 117-119
- Account name (short name)
  - user accounts, 205
- Accounts
  - adding CalDAV accounts, 634, 637
  - administrator (see Administrator account)
  - creating Local Admin account, 24
  - creating new administrator account, 25
  - group accounts (see Groups)
  - managing with Profile Manager, 327
  - network users (see Local network accounts)
  - setting up email account, 602, 603
  - user (see User accounts)
- Accounts section
  - Server app, 105
- ACEs (access control entries)
  - adding for share point, 416
  - allowing read-only access, 433
  - configuring complex permissions for, 419
  - configuring file access with Sharing pane of Server app, 408
  - configuring shared folders for groups, 386
  - creating, 418
  - inheritance of, 421-423
  - order of entries in ACLs, 416
  - sorting canonically in ACLs, 423
  - Storage pane permissions and, 412
  - use of GUID for group or user identification, 425
  - what is included in, 415
- ACK
  - types of DHCP events, 543
- ACLs (access control lists)
  - comparing POSIX permissions and ACLs, 413
  - comparing views of permissions, 443-447
  - configuring with Sharing pane, 408, 416
  - configuring with Storage pane, 418
  - describing how they work, 416
  - editing from Server app Storage pane, 100
  - file sharing across multiple platforms and, 389
  - group membership and, 426
  - inheritance, 421-423
  - overview of, 414
  - portability of, 424
  - POSIX compare with, 425
  - propagating permissions, 424
  - protecting backup files, 189
  - protecting Time Machine files, 505
  - rules of precedence in POSIX and ACLs, 427
  - share points and, 369
  - sorting canonically, 423

- updating with Sharing pane, 441
  - user and group identification, 425
- Action menu
  - deleting wikis, 621
  - editing user attributes, 222
  - Storage pane options, 412
  - viewing alerts, 168
  - viewing certificate details, 129
  - wiki settings, 620
- Activity Monitor
  - confirming basic operation of
    - Caching service, 493
- AD (Active Directory)
  - externally provided DNS and, 66
- Address Book
  - compatibility with Contacts service, 639
- Administration set, of permissions, 420
- Administrator account
  - access control for wikis, 612
  - configuring and starting VPN service, 524
  - creating Local Admin account, 24
  - creating new account, 25
  - creating user templates, 225
  - creating with Profile Manager, 355
  - giving local users administrative rights, 209
  - global password policy impacting, 285
- Administrators
  - configuring administrator computer, 48
  - configuring administrator computer on existing computer, 51
  - configuring Messages service on administrator computer, 656
  - configuring OS X on administrator computer, 49
  - configuring use of DNS service, 53
  - confirming access to DNS records, 56
  - confirming administrator computer is enrolled, 360
  - enrolling administrator computer for remote management, 356-360
  - setting up contact access to CalDAV on administrator computer, 643
  - setting up email account on administrator computer, 602-603
- Advanced Options
  - Users pane, 206
- Advanced services
  - Server app, 107
- AFP (Apple Filing Protocol)
  - accessing Kerberized services, 288
  - comparing file-sharing protocols, 374
  - configuring file sharing service, 376
  - configuring password policy and, 299
  - confirming password policy and, 300
  - connecting to network file services, 202
  - file-sharing services, 371
  - guest access, 384, 411
  - inheritance of ACLs and, 566
  - inspecting access log, 404
  - inspecting AFP error log, 405
  - inspecting file sharing services, 477
  - making shared folders available for home directories, 385
  - monitoring file sharing performance, 180
  - multiple platform support, 389
  - POSIX ownership and permissions, 414
  - protocols for file sharing, 105
  - reviewing AFP Error log, 378
  - securing, 515
  - viewing connected users, 387
- AirDrop
  - downloading student materials, 59
- AirPort
  - making VPN service available to AirPort devices, 518
  - managing AirPort devices, 102
- Alerts
  - adding recipients of push alerts, 175
  - configuring, 166-168, 173
  - configuring email recipients to receive, 174
  - confirming alert operation, 177-179
  - in Server app, 46, 165
  - inspecting list of alerts to be sent, 176
  - inspecting/configuring recipients of push alerts, 174
  - monitoring disk space, 179
  - sending test alert, 176
  - turning on push notifications, 173
- Alerts pane
  - tabs of, 166
- Aliases
  - accessing multiple URLs, 561
  - assigning to user accounts, 208
- Allow permission
  - how ACLs work, 416
- Amavis virus-scanner, 591
- Anonymous user
  - blogging on wiki as, 621
- Apache
  - logs for monitoring web services, 558
  - OS X Server web service based on, 552
  - web service configuration files, 552
- APM (Apple Partition Map), 8
- APN (see Apple push notification)
- App Store
  - downloading OS X Server, 15
  - installing OS X Server from, 39-40
  - preferences, 57
  - update preferences, 36
  - updating OS X Server, 19
- Apple Configurator
  - for streamlining profile enrollment, 341
- Apple IDs
  - for push notifications, 167
  - obtaining in preparing for Profile Manager, 307
  - resetting passwords and, 52
  - sign in and, 23
- Apple Partition Map (APM), 8
- Apple push notification, 175

- (see also Push notifications)
  - profile delivery options, 330
  - push notification of email, 586
  - pushing profiles, 340
  - turning on, 166, 173
  - Apple Remote Desktop (ARD)
    - image creation and deployment, 451
    - turning on remote management, 29
  - Apple Software Restore (ASR)
    - image creation and deployment, 451
    - multicast streams as disk image source, 459
  - Apple Software Update
    - mirroring updates on Apple servers, 497
  - Apps
    - managing with Profile Manager, 329
  - Archives
    - certificate archive, 139
    - creating Open Directory archive, 265
    - logging messages, 652
    - of Open Directory content, 187
    - turning on message archiving, 655
    - viewing message archive, 664
  - ARD (Apple Remote Desktop)
    - image creation and deployment, 451
    - turning on remote management, 29
  - ASR (Apple Software Restore)
    - image creation and deployment, 451
    - multicast streams as disk image source, 459
  - Attributes
    - user account, 207
  - Audio conferencing
    - functions of Messages service, 649
  - Authentication
    - centralized repository, 254
    - configuring Mail services for, 589
    - configuring on OS X Server, 282
    - configuring VPN service, 519
    - defined, 201
    - inspecting email options for, 596
    - inspecting email relay options, 596
    - Kerberos services, 286
    - managing AirPort devices and, 102
    - of users, 202
    - Open Directory service providing, 254
    - troubleshooting Calendar service, 628
    - troubleshooting Contacts service, 640
    - troubleshooting Kerberos, 291
    - troubleshooting Messages service, 654
    - troubleshooting service access, 219
    - troubleshooting Wiki service, 614
    - two-factor, 311
  - Authorization
    - defined, 201
    - for access to directory service, 261
    - removing right to access services, 216
    - requesting for Messages service users, 659
    - to access services, 203
    - troubleshooting service access, 219
    - verifying for file sharing, 247, 249
  - Automatic redirect settings
    - websites and, 562
- B**
- Backing up OS X Server, 503
    - (see also Time Machine)
    - backup concepts, 183
    - configuring Time Machine, 191
    - diversity in approach to, 184
    - external disk as back up destination, 188-189
    - Finder used for examining backup files, 193-196
    - inspecting backup files, 192
    - internal volume as back up destination, 189-191
    - overview of, 183
    - viewing backup logs, 197
    - what Time Machine will back up, 186
    - what Time Machine will not back up, 186
  - Backup disks
    - selecting, 510
  - Blacklists
    - enabling filtering, 596
    - filtering email, 591
  - Blogs
    - adding for wikis, 620
    - compared with wikis, 613
    - view wiki blogs and add comments, 621
    - wiki settings, 620
  - Bonjour
    - advertising shared folders for Time Machine service, 503
    - clients computers connecting with DNS servers, 66
    - server advertising services via, 12
  - Boot disk
    - creating with NetInstall, 453
  - Boot Service Discovery Protocol (BSDP), 455
  - BOOTP (Bootstrap Protocol)
    - DHCP relying on, 543
    - DHCP using, 534
  - Bound server
    - binding server to directory service of another server, 261
  - BSDP (Boot Service Discovery Protocol), 455
  - Buddy lists
    - adding buddy to, 659
    - checking availability status of buddies, 658
- C**
- CA (certificate authority)
    - configuring Open Directory CA, 152
    - defined, 124
    - following certificate chain, 142
    - Get a Trusted Certificate wizard, 152
    - getting signed certificate from, 128
    - importing signed certificates, 135
    - inspecting Open Directory CA, 156-159

- obtaining trusted certificates, 131
- SSL certificate from, 62
- trusting, 125
- Caching service
  - basic OS X Server services, 106
  - configuring and maintaining, 486-490
  - confirming basic operation, 492
  - describing, 483-486
  - logs, 493
  - moving data volume of, 495
  - performance bottlenecks, 494
  - Software Update compared with, 490
  - testing by deleting items, 492
  - troubleshooting, 492
  - updating software, 35, 57
- Caching, Bytes Served
  - performance monitoring, 180
  - performance stats, 171
- CalDAV (Calendar Server Extensions for WebDAV)
  - adding CalDAV accounts, 634, 637
  - Calendar service based on, 624
  - Contacts service use of open source technologies, 640
  - setting up contact access to, 643
- Calendar application
  - basic OS X Server services, 106
  - wiki calendar feature and, 613
- Calendar Server Extensions for WebDAV (see CalDAV (Calendar Server Extensions for WebDAV))
- Calendar service
  - adding CalDAV accounts, 634-635, 637
  - creating locations, 632
  - creating resources, 632
  - data locations, 623
  - features, 624
  - inspecting email invitation settings, 630-631
  - overview of, 623
  - replying to invitations, 638
  - reviewing certificates, 629
  - sending invitations, 635-637
  - starting, 631
  - starting and configuring, 629
  - troubleshooting, 628
  - using, 625-628
- CardDAV
  - accessing contacts from applications that use, 645
- CDP (continuous data protection)
  - backup styles, 184
- Certificate Assistant
  - troubleshooting certificates, 149
- Certificate signing request (see CSR (certificate signing request))
- Certificates
  - configuring Open Directory certificate, 153-154
  - configuring SSL certificates, 97
  - confirming protection in Calendar service, 629
  - confirming protection of Contacts service, 641
  - confirming protection of Mail services, 595
  - confirming protection of Messages service, 654
  - creating new websites, 574
  - inspecting Open Directory certificates, 155
  - inspecting service certificates, 574
  - issuing new SSL certificate, 571-573
  - protecting websites, 556
- Certificates pane, Server app
  - configuring services for certificate use, 141
  - options for adding new certificates, 131
- Change Host Name Assistant
  - configuring network interfaces, 31
  - creating default zones, 69
  - starting from Server app, 14
- Chat services, 649
  - (see also Messages service)
  - joining Messages federation, 653
  - persistent chat or chat rooms, 649
  - viewing archives, 664
  - viewing logs, 663
- ClamAV virus protection, 591
- Clients
  - advanced VPN configuration, 520
  - assigning range of client addresses, 524
  - configuring backup limits, 504
  - configuring VPN service, 523
  - monitoring DHCP service, 539
  - NetInstall client startup process, 455
- Cloud
  - backup diversity and, 184
  - media options for backups, 184
- Collaboration
  - with Calendar service (see Calendar service)
  - with Messages service (see Messages service)
  - with Wiki service (see Wiki service)
- Comma-separated value files (see CSV (comma-separated value) files)
- Comments
  - accepting comments to wikis, 621
  - adding to wiki blog, 621
- Computers
  - changing names, 13
  - confirming computer qualified to run OS X Server, 26
  - managing with NetInstall, 452
  - setting computer name, 28, 52
  - understanding computer names, 11
- Confidentiality
  - configuring VPN service, 519
- Configuration files
  - Calendar service, 623
  - for web services, 552
- Configuration profiles, 327
  - (see also Profile Manager)
  - configuring Messages service, 651
  - creating for device groups, 344-347
  - distributing VPN configuration profile, 519
  - overview of, 306
  - saving VPN profile, 521
  - testing, 347-350
- Configuring server computer before installing OS X server
  - establish student number, 21
  - on existing OS X system, 25-26
  - options, 21
  - overview of, 21
  - using Setup Assistant, 22-24
- Connect to Server on a Mac, 109

- Connected Users pane
  - File Sharing, 387
  - viewing/disconnecting from file sharing users, 403
- Console utility
  - inspecting logs from, 20
  - logs available from, 170
  - logs for troubleshooting Caching service, 493
  - reviewing file sharing logs, 378
  - troubleshooting account import, 240
  - troubleshooting directory services, 273
  - troubleshooting user import, 218
  - viewing import log, 295
  - viewing web service logs, 558
- Contacts application
  - basic OS X Server services, 106
  - compatible with Contacts service, 639
  - configuring access to Contacts service, 643
- Contacts service
  - configuring, 641, 642
  - configuring Contacts app for accessing, 643
  - configuring OS X to use, 642
  - confirming contacts accessible on multiple devices, 645
  - confirming directory searches, 646
  - confirming SSL protection, 641
  - creating local network accounts, 647-648
  - creating new contacts, 644
  - overview of, 639-640
  - searching for local network users, 648
  - setting up access to CalDAV on administrator computer, 643-643
  - setting up contacts on second Mac, 645
  - troubleshooting, 640
- Continuous data protection (CDP), 184
- Coordinated Universal Time (UTC), 197
- Core Storage
  - startup volume in, 190
- Credentials
  - authentication and, 201
  - providing for imported users, 298
- CSR (certificate signing request)
  - generating and submitting to CA, 128
  - importing signed certificates, 135
  - obtaining trusted certificates, 127, 131-134
- CSV (comma-separated value) file
  - for importing devices into Profile Manager, 329
  - importing and assigning placeholders to device group, 342
- D**
- Data
  - describing Calendar service data locations, 623
- Date & Time preferences, 257
- Delegation
  - functions of, 627
- Deny permission
  - how ACLs work, 416
- DEP (Device Enrollment Program)
  - enabling, 311
  - turning on Profile Manager with DEP active, 316-321
- Deployment solutions
  - caching content from Apple (see Caching service)
  - NetInstall (see NetInstall)
  - Software Update service (see SUS (Software Update service))
- Device Enrollment Program (see DEP (Device Enrollment Program))
- Device groups
  - creating configuration profile for, 344-347
  - importing and assigning placeholders to, 342-343
  - layering and multiple profile considerations, 338
  - levels of management with Profile Manager, 328
  - managing, 329
- Device Management
  - mobile devices (see MDM (Mobile Device Management))
  - with Profile Manager (see Profile Manager)
- Devices
  - confirming contact availability on multiple, 645
  - confirming operation of Caching service in iOS devices, 493
  - layering and multiple profile considerations, 338
  - levels of management with Profile Manager, 328
  - locking or wiping remotely, 331
  - preparing Profile Manager for one-to-one devices, 352
  - preparing Profile Manager for shared devices, 341
  - problems enrolling in profile management, 340
- DHCP (Dynamic Host Configuration Protocol)
  - advanced OS X Server services, 108
  - assigning static addresses, 540
  - configuring, 531
  - configuring DHCP service, 544, 550
  - configuring DHCP service with Server app, 535
  - configuring server's network interface, 535
  - configuring VPN service, 517
  - DNS requests and, 63
  - editing subnets, 536-538
  - examining DHCP logs, 542
  - how it works, 532
  - leases, 533
  - manually assigning static IPv4 addresses vs., 11
  - monitoring and configuring DHCP service, 539
  - NetInstall client startup process, 455
  - serving multiple subnets, 534
  - specifying information for DHCP network, 537
  - starting DHCP service, 539
  - static and dynamic addresses, 534
  - troubleshooting, 541
  - turning off DHCP service, 550
  - understanding DHCP networks, 532

- DHCP pane
  - Server app, 536
- Diagnostics & Usage
  - sending diagnostic reports to Apple, 24
- Digital identity
  - defined, 124
- Digital signatures
  - defined, 124
- Directory services
  - allowing access to services from another directory node, 280
  - binding OS X server to directory service of another server, 268-270
  - concepts, 253
  - dealing with variety of, 253
  - managing remotely with Directory Utility, 270
  - Open Directory (see Open Directory)
  - troubleshooting, 272
- Directory Utility
  - binding OS X to Open Directory service, 271
  - managing directory services remotely, 270
  - troubleshooting directory services, 272
- Discover
  - types of DHCP events, 543
- Disk images
  - automating installation of NetInstall images, 458
  - configuring protocol for NetInstall image, 474
  - creating customized NetInstall image, 465, 467
  - creating NetBoot images, 459
  - creating NetInstall images with System Image Utility, 456
  - inspecting customized NetInstall image, 471
  - NetRestore, 460
  - sources of NetInstall images, 458
  - specifying default NetInstall image, 476
  - starting up from NetInstall image, 478
  - types of NetInstall images, 454
- Disk space
  - monitoring, 179
- troubleshooting NetInstall service, 463
- troubleshooting Software Update service, 500
- Disk Utility
  - backing up to external disks, 188
  - creating disk images, 459
  - creating disk images that can be deployed from file server, 461
  - internal volume as backup destination, 189
  - location of, 8
- Disks, 184
  - (see also Hard disks)
  - configuring Time Machine, 191
  - media options for backups, 184
- DNS (Domain Name System)
  - adding nameserver record for reverse zone, 81
  - advanced OS X Server services, 108
  - advanced VPN configuration, 520
  - cleaning up permissions, 90
  - collecting configuration data, 72
  - collecting information for setting up in OS X Server, 68
  - components, 64
  - configuring DNS Servers field, 45
  - configuring for Mail services, 588
  - configuring forwarding servers, 73
  - configuring naming and networking, 10
  - configuring network interfaces, 31
  - configuring permissions, 87
  - configuring recursive lookup restrictions, 85-87
  - configuring VPN service, 517, 525
  - configuring with Server app, 14
  - confirming DNS records, 56
  - confirming new records, 82-84
  - confirming server access to DNS records, 262
  - confirming service access restrictions, 89
  - creating new record, 76
  - creating new record for website, 570
  - creating new record from Show All Records dialog, 78
  - creating new websites, 574
  - creating zones and records, 71
  - flow of DNS request, 63
  - inspecting limited default zones, 75
  - inspecting new zones and records, 77
  - overview of, 63
  - problems related to bad or non-existent DNS, 64
  - removing redundant zones, 80
  - restricting access to DNS service, 84
  - reviewing access permission, 88
  - role of MX server in email, 586
  - setting up, 44
  - split DNS for dealing with external and internal DNS, 67
  - starting DNS service, 42-45
  - troubleshooting Calendar service, 628
  - troubleshooting Contacts service, 640
  - troubleshooting in OS X Server, 70
  - troubleshooting Kerberos, 291
  - troubleshooting Mail services, 594
  - troubleshooting Messages service, 654
  - troubleshooting Wiki service, 614
  - typical scenarios for DNS services, 66
  - understanding host names, 13
  - workaround for access issues, 112
- DNS servers
  - clients connecting with via Bonjour, 66
  - components of DNS service, 65
  - configuring DNS Servers field, 45
  - configuring forwarding servers, 73
  - flow of setting up, 69
  - split DNS and, 68
  - troubleshooting, 70
- Documents

- copying student materials to, 58
    - uploading to wikis, 619
  - Domain Name System (see DNS (Domain Name System))
  - Domains
    - adding email domain, 598
    - assigning to email accounts, 592
    - blacklisting junk mail hosts, 592
    - configuring an additional email domain, 600
    - configuring DNS service, 68
  - Dovecot
    - email packages Mail services is based on, 585
  - Downloads
    - OS X Server, 15
    - OS X Server from App Store, 40
    - student materials, 36-38, 58
    - Trust Profile, 466
    - virus definitions, 594
  - Dynamic addresses
    - comparing DHCP static and dynamic address assignment, 534
  - Dynamic Host Configuration Protocol (see DHCP (Dynamic Host Configuration Protocol))
- E**
- EFI (Extensible Firmware Interface), 331
  - Email, 585
    - (see also Mail services)
    - configuring email recipients to receive alerts, 174
    - inspecting Calendar service invitation settings, 630
    - profile delivery options, 330
  - Emergency boot disk
    - creating with NetInstall, 453
  - Encryption
    - cryptographic keys, 123
    - file sharing protocols and, 392
    - full disk encryption, 10
    - of Messages federation, 653
    - VPNs used to encrypt network traffic, 515
  - Energy Saver preferences
    - availability of OS X Server and, 7
  - Ethernet
    - Caching service requirements, 487
    - configuring OS X on server, 22
    - hardware requirements for NetInstall, 453
    - network interface speed and, 6
    - preparing NetInstall service, 464
  - Events, Calendar service
    - replying to invitations, 638
    - sending invitations, 635-637
  - Exclusions
    - configuring Time Machine to exclude most files, 509-510
    - managing quantity of data backed up, 504
  - Extensible Firmware Interface (EFI), 331
  - Extensible Markup Language (XML), 305
  - Extensible Messaging and Presence Protocol (XMPP), 650
  - External disks
    - as back up destination, 188-189
- F**
- Federation of messages
    - configuring, 653
    - restricting, 662
  - File servers
    - deploying disk images, 461
    - monitoring, 377
    - share points and, 370
  - File Sharing
    - ACLs in, 414
    - adding/removing share points, 381-383
    - basic OS X Server services, 106
    - challenges of, 369
    - clients browsing to services, 10
    - comparing POSIX permissions and ACLs, 413
    - comparing protocols, 374
    - comparing uses of UID, GID, and GUID, 425
    - comparing views of permissions, 443-447
    - configuring access control, 429
    - configuring access to share points and folders, 407
    - configuring access with Sharing pane of Server app, 408-410
    - configuring access with Storage pane of Server app, 411
    - configuring ACLs from Sharing pane, 416
    - configuring ACLs from Storage pane, 418
    - configuring complex permissions for ACEs, 419
    - configuring group folder, 386
    - configuring groups and shared folders, 430
    - configuring share points, 383
    - configuring users and groups, 375
    - confirming permission are allowing desired access, 434-440
    - confirming permissions, 442
    - creating group and adding users, 430
    - creating group and updating permissions, 441
    - creating new location for shared folders, 396-398
    - creating new shared folder, 398-400
    - creating share points, 378
    - creating/configuring shared folders, 431
    - default share points, 380
    - defining file access, 407
    - defining methods or protocols for, 371-374
    - describing how ACLs work, 416
    - enabling services for, 371
    - exercise using, 392-394
    - exploring how it works, 379
    - features common to POSIX and ACLs, 425
    - giving groups access to shared folders, 400-403
    - groups membership and ACLs and, 426
    - guest access, 410
    - inheritance of ACLs and, 421-423
    - inspecting access to services, 244
    - inspecting AFP access log, 404
    - inspecting AFP error log, 405
    - inspecting shared folders related to NetInstall service, 476
    - maintaining regularly, 377
    - making shared folders available for home directories, 385
    - managing, 243
    - monitoring file server, 377

- multiple groups impacting, 427
  - nested groups impacting, 427
  - overview of, 369
  - planning file server requirements, 375
  - portability of ACLs and, 424
  - POSIX ownership and permissions, 413
  - propagating permissions, 424
  - protocols, 105
  - providing FTP service, 389-392
  - reviewing logs, 378
  - rules of precedence in POSIX and ACLs, 427
  - sharing website folder, 566-567
  - sorting ACLs canonically, 423
  - starting and configuring service with Server app, 376
  - stopping, 251
  - stopping sharing of website content, 569
  - stopping/starting service, 394-396
  - troubleshooting, 388
  - turning on and verifying
    - authorization, 247-249
  - turning on when using Time Machine, 504
  - turning on with Server app, 218
  - updating permissions, 440
  - verifying imported users can connect to, 297
  - viewing and disconnecting connected users, 403
  - viewing connected users, 387
  - with Permissions dialog of Storage pane, 412
- File Sharing pane, Server app
- allowing guest access for file sharing, 410
  - comparing views of permissions, 443-447
  - configuring ACLs, 416
  - configuring file access, 408-410
  - inspecting shared folders related to NetInstall service, 476
  - propagating permissions, 424
  - updating ACLs, 441
  - viewing backup details, 511
- File Sharing, Connected Users
- monitoring performance with, 180
  - performance stats, 171
- Files
- allowing local user access, 209
  - confirming existence of files for
    - removed website, 576
  - examining backup files with Finder, 193-196
  - groups used to manage access to, 217
  - Import Accounts from File, 280
  - importing user accounts from text delimited file, 230-232
  - importing users from exported formatted file, 232
  - inspecting backup files, 192
  - locations of website files, 553
- FileVault
- full disk encryption, 10
- Filtering
- Filter Users menu options, 206
- Filters
- troubleshooting NetInstall service, 463
- Filters, email
- blacklists, greylists, junk mail, 591
  - configuring options for, 596
  - testing spam filter, 607
  - troubleshooting Mail services, 594
- Finder
- changing name of startup volume, 27
  - connecting to File Sharing service, 297
  - copy operations, 94
  - examining backup files, 193-196
- Firewalls
- troubleshooting NetInstall service, 463
  - VPNs compared with, 515
- FireWire
- downloading student materials using removable disk, 59
- Folders
- changing folder used by default secure website, 565
  - changing folder used by default website, 564
  - copy content to new website folder, 567
  - location of website folders, 553
  - sharing (see File Sharing) (see Shared folders)
    - sharing website folder, 566-567
- Formatting
- hard disks, 7-10
- Forwarding servers, DNS
- collecting DNS configuration data, 72
  - components of DNS service, 65
  - configuring, 73
  - requests and, 64
- FQDN (fully qualified domain names)
- for websites, 556
- FTP (File Transfer Protocol)
- advanced OS X Server services, 108
  - file sharing service, 389-392
  - file-sharing services, 371
- Full file-level copy
- backup styles, 183
- Full image backup, 183
- Full name
- user accounts, 205
- ## G
- GID (group ID), 425
- Gigabit Ethernet, 6
- (see also Ethernet)
- Globally unique ID (GUID), 425
- Graphs
- Caching service-related, 488
  - monitoring performance with, 180
  - performance stats, 171
- Greylists
- enabling filtering, 596
  - filtering email, 591
- Group ID (GID), 425
- Groups
- access control for wikis, 612
  - ACLs and group membership, 426
  - adding group membership to user account, 238
  - adding groups to groups, 239
  - adding users to, 237
  - assigning local groups to local group, 213
  - assigning local groups to local users, 211
  - assigning local users to, 210
  - configuring, 430
  - configuring file sharing for, 375

- configuring group folder for file sharing, 386
  - controlling access to Time Machine service, 506
  - creating and adding users, 430
  - creating local, 210, 235
  - creating new group and updating permissions, 441
  - creating templates, 208
  - default access rules, 101
  - deleting, 251
  - importing, 236
  - importing local network groups into server's shared directory node, 296
  - inspecting email accounts, 601
  - inspecting group workgroup, 273
  - inspecting user membership in, 244
  - layering and multiple profile considerations, 338
  - levels of management with Profile Manager, 328
  - managing access to files and services, 217
  - managing preferences for users in, 328
  - multiple groups impacting POSIX and ACLs, 427
  - nested, 427
  - panes in Account section of Server app, 105
  - primary and secondary, 208
  - providing shared folder for, 400-403
  - sending email to, 604
  - Time Machine access, 512
  - Guest accounts
    - allowing access to file sharing, 410
  - GUID (globally unique ID), 425
    - in ACEs, 415
  - GUID Partition Table (GPT)
    - selecting partition scheme, 8
- H**
- Hard disks, 189
    - (see also Volumes)
    - disk space requirements for OS X Server hardware, 6
    - external disk as back up destination, 188, 189
    - formatting/partitioning, 7-10
    - monitoring disk space, 179
  - Hardware
    - disk space requirements for OS X Server hardware, 6
    - minimum requirements for OS X Server, 4
    - NetInstall requirements, 453
    - network interface requirements, 6
    - upgrading to OS X Server and, 18
    - verifying system requirements, 4
  - Help menu, Server app
    - Server Tutorials, 110
  - Home directory
    - making shared folder available for, 385
  - host command
    - confirming new DNS records, 82
    - looking up MX records, 83
  - Host configuration, DNS
    - adding nameserver record for reverse zone, 81
    - confirming new records, 82-84
    - creating new records, 76, 78
    - inspecting new zones and records, 77
    - overview of, 76
    - removing redundant zones, 80
  - Host names
    - configuring DNS service, 68
    - configuring VPN service, 517
    - how DNS works, 63
    - updating server host name, 42-45
    - viewing host name change alert, 46
  - HTTP (Hypertext Transfer Protocol)
    - Calendar service using, 624
    - configuring protocol for NetInstall image, 474
    - Contacts service use of open source technologies, 640
    - default website responding to HTTP requests, 562
    - in NetInstall client startup process, 455
  - HTTPS (HTTP Secure)
    - Calendar service using, 624
  - Contacts service use of open source technologies, 640
  - default website responding to HTTPS requests, 562
- I**
- iChat (see Messages service)
  - Identification
    - Kerberos services, 286
    - of users and groups, 425
    - Open Directory using LDAP for, 255
  - Image pane
    - Server app, 476
  - IMAP (Internet Message Access Protocol)
    - email retrieval protocol, 587
    - examining Mail Service logs, 609
    - setting up email accounts, 604
  - Importing local network accounts
    - adding groups to server's shared directory node, 296
    - adding network users to server's shared directory node, 293-296
    - creating accounts and, 292
    - overview of, 280
    - verifying users can connect to File Sharing service, 297
  - Importing user accounts
    - from delimited text file, 230-232
    - from exported formatted file, 232
    - groups, 236
    - troubleshooting, 218, 240
    - updating passwords for imported users, 233
  - Incremental backups
    - backup styles, 184
  - Index files
    - default website and, 561
  - Inheritance
    - ACLs and, 421-423
    - of ACLs during file sharing, 566
  - Installing OS X Server
    - administering server with Server app, 60-62
    - changing names and addresses, 13
    - changing startup volume name, 27
    - computer name, 11

- configuring administrator computer, 48
  - configuring administrator computer on existing computer, 51
  - configuring administrator computer on new computer, 49
  - configuring computer before installation, 21
  - configuring DNS Servers field, 45
  - configuring existing computer, 25-26
  - configuring naming and networking, 10
  - configuring network interfaces, 31-35
  - configuring networking, 53-56
  - configuring new computer with Setup Assistant, 22-24
  - configuring server for remote administration, 47
  - confirming computer qualified to run OS X Server, 26
  - confirming DNS records, 56
  - disk space requirements, 6
  - downloading OS X Server, 15
  - downloading student materials, 36-38, 58
  - Energy Saver preferences, 7
  - formatting/partitioning disks, 7-10
  - full disk encryption, 10
  - hardware requirements, 4
  - host name, 12-13
  - inspecting logs, 20
  - installing latest server version from App Store, 39-40
  - installing Server app, 60
  - network interface speed and, 6
  - opening installed server, 40-41
  - overview of, 3, 16
  - preparing for, 7
  - RAID volumes and, 10
  - RAM requirements, 6
  - setting up computer name, 28
  - setting up computer name and turning on remote management, 52
  - troubleshooting, 20
  - turning on remote management, 29
  - updates and, 19
  - updating host name and starting DNS service, 42-45
  - updating software, 35-36, 57
  - upgrading or migrating to, 18
  - verifying system requirements, 4
  - viewing host name change alert, 46
  - Integrity
    - configuring VPN service, 519
  - Intermediate CAs
    - defined, 124
    - in Open Directory, 126, 152
    - trust and, 145
  - Internet Accounts preferences
    - adding CalDAV accounts, 637
    - configuring Mail services, 602
    - configuring Messages service, 651
  - Internet Message Access Protocol (see IMAP (Internet Message Access Protocol))
  - Invitations, Calendar service
    - inspecting settings for, 630-631
    - overview of, 626
    - replying to, 638
    - sending, 635-637
  - IP addresses
    - advanced VPN configuration, 520
    - blacklisting junk mail hosts, 592
    - changing, 13
    - configuring DNS service, 69
    - configuring VPN service, 518
    - creating new websites, 574
    - how DHCP works, 532
    - how DNS works, 63
    - managing websites, 556
    - requested by NetInstall clients, 455
    - whitelists, 167
  - IPv4, 63
    - (see also IP addresses)
    - checking DNS service, 153
    - configuring DNS service, 69
    - configuring server to use additional IPv4 addresses, 570
    - DHCP leases and, 533
    - DNS hosting requirements, 65
    - DNS service and, 63
    - how DHCP works, 532
    - removing additional addresses from website, 577
  - troubleshooting DHCP service issues, 542
  - ISPs (Internet service providers)
    - SMTTP servers and, 590
  - iTunes
    - confirming operation of Caching service, 493
  - iWork
    - turning on WebDAV for use with, 616
- J**
- Jabber accounts
    - configuring Messages service, 651
    - selecting account type, 657
  - Journalled formats, 8, 415
  - Junk mail
    - confirming test message was flagged as junk, 608
    - enabling filtering, 596
    - filtering email, 591
    - sending test message, 607
    - testing spam filter, 607
- K**
- KDC (Kerberos Key Distribution Center)
    - functions of, 286
    - Open Directory master role and, 257
    - Open Directory replicas and, 257
    - single sign-on, 282
  - Kerberos
    - basics, 286-288
    - examining tickets, 288
    - Open Directory using, 255
    - password policies and, 284
  - Key Distribution Center (see KDC (Kerberos Key Distribution Center))
  - Keychain Access utility
    - archiving certificates and, 139
    - inspecting Open Directory CA, 156-159
    - inspecting SSL certificates, 137
    - viewing SSL certificates, 128
    - viewing trusted CAs, 125
  - Keychains
    - inspecting SSL certificates with System keychain, 137

- storing passwords in, 61
  - storing trusted CAs in, 125
  - Ticket Viewer and, 289
- Keys
  - cryptographic, 123
- Keywords
  - organizing users by, 206
- L**
- L2TP (Layer 2 Tunneling Protocol), 517
- Launchpad
  - opening Server app, 40
- Layer 2 Tunneling Protocol (L2TP), 517
- LDAP (Lightweight Directory Access Protocol)
  - accessing Open Directory log files, 271
  - authentication using hashed password in LDAP database, 282
  - Calendar service integration with, 625
  - Open Directory using for identification, 255
  - populating shared directory, 277
- Leases
  - defining DHCP leases, 533
- Lightweight Directory Access Protocol (see LDAP (Lightweight Directory Access Protocol))
- Links
  - profile delivery options, 330
- Local accounts
  - connecting to server via different account, 223-225
  - differentiated from local network accounts, 256
  - importing, 229
- Local Admin accounts
  - accessing read only permissions, 196
  - creating, 24
  - credentials, 40
  - passwords, 52
- Local groups
  - adding users to, 237
  - assigning local groups to local group, 213
  - assigning local users to, 210
  - assigning to local users, 211
  - creating, 210, 235
  - importing, 236, 296
- Local hostname
  - understanding, 12
- Local network accounts
  - accessing account services from another directory node, 280
  - cleaning up password policy, 302
  - configuring authentication, 282
  - configuring password policy, 299-300
  - confirming password policy, 300-302
  - creating new, 647-648
  - defining Kerberos basics, 286-288
  - differentiated from local accounts, 257
  - disabling accounts, 283
  - examining Kerberos tickets, 288
  - importing, 280, 292
  - importing groups into server's shared directory node, 296
  - importing users into server's shared directory node, 293-296
  - managing with Server app, 277-280
  - overview of, 277
  - searching for users, 648
  - setting global password policies, 284-286
  - specifying email addresses for, 598-599
  - troubleshooting, 291
  - troubleshooting Kerberos, 291
  - verifying user ability to connect to File Sharing service, 297
- Local users
  - allowing access to services and files, 209
  - assigning local groups to, 211
  - assigning to local groups, 210
  - configuring, 208-210
  - creating new user, 220-221
  - editing user attributes, 221
  - granting administrative rights, 209
- Locales
  - Open Directory, 259
- Locations, Calendar service
  - creating, 632
  - sending invitations and, 635
- Locking device
  - remotely, 331
- Logging
  - illustrating message logging, 652
  - turning on Messages service logging, 655
- Login
  - authentication and, 202
  - preventing, 283
- Logs
  - accessing Open Directory log files, 271
  - examining DHCP logs, 542
  - examining Mail Service logs, 609
  - examining VPN service logs, 528
  - in Server app, 165
  - inspecting AFP access log, 404
  - inspecting AFP error log, 405
  - monitoring DHCP service, 549
  - monitoring NetInstall service, 480
  - monitoring OS X Server, 169-170
  - monitoring web services, 558
  - reviewing file sharing logs, 378
  - troubleshooting account import, 240
  - troubleshooting Caching service, 493
  - troubleshooting Mail services, 594
  - troubleshooting NetInstall service, 463
  - troubleshooting Open Directory, 275
  - troubleshooting OS X Server installation, 20
  - troubleshooting profiles, 340
  - troubleshooting Software Update service, 500
  - troubleshooting user import, 218
  - troubleshooting VPN service, 522
  - viewing backup logs, 197
  - viewing import log, 295
  - viewing message and chat logs, 663
  - viewing website access log, 581
- Logs pane
  - viewing backup logs, 197

- Lookups, DNS
  - checking DNS service, 153
  - configuring recursive lookup restrictions, 85-87
  - how DNS works, 63
  - range of IPv4 addresses, 69
- M**
- MAC (Media Access Control)
  - addresses, 534
- Mac App Store (see App Store)
- Mac computers
  - adding certificates to System keychain, 147
  - capable of running Yosemite, 4
  - configuring certificate trust, 146
  - confirming basic operation of Caching service, 493
  - Connect to Server on a Mac, 109
  - displaying information regarding, 360
  - obtaining Kerberos tickets, 288
  - sending messages between, 658
  - setting up contacts on second Mac, 645
  - verifying system requirements for OS X Server installation, 4
- Mac OS Extended
  - applying ACLs on, 415
  - types of journaled volumes, 8
- Mail services
  - adding domains, 598
  - checking reply to sent message, 606
  - compatibility with Contacts service, 639
  - configuring an additional email domain, 600
  - configuring filtering options, 596
  - configuring using Internet Accounts preferences, 602
  - confirming incoming message scanned for viruses, 605
  - confirming service is running, 601
  - confirming SSL certificate, 595
  - confirming test message was flagged as junk, 608
  - description of, 106
  - DNS settings, 588
  - domains, 592
  - downloading virus definitions, 594
  - examining logs, 609
  - hosting, 585
  - inspecting authentication methods, 596
  - inspecting group accounts, 601
  - inspecting relay options, 596
  - inspecting user accounts, 600
  - outgoing mail, 589
  - overview of, 585
  - permissions and authentication methods, 589
  - protocols in, 586
  - replying to message received, 605
  - sending mail to group from user account, 604
  - sending test of junk message, 607
  - setting storage quotas, 597
  - setting up email account on administrator computer, 602-603
  - setting up email account on server computer, 603-604
  - specifying email address for local network accounts, 598-599
  - testing spam filter, 607
  - troubleshooting, 593
  - turning on, 594
  - user storage quotas, 590
  - virus scanning, blacklist, grey-lists, and junk filtering, 591
- Mainserver
  - downloading student materials, 58
- Maintenance
  - of Caching service, 486
  - of file sharing, 377
- Manage menu
  - Server app, 108
- Master role
  - configuring Open Directory as, 262-264
  - describing server roles, 256
  - inspecting Open Directory master, 273
  - preparing for Profile Manager, 307
- MDM (Mobile Device Management)
  - automatic enrollment in, 350
  - configuring and turning on, 306
  - Device Enrollment Program and, 311
  - identifying Open Directory server to, 263
  - Profile Manager functionality options, 305
- Media Access Control (MAC)
  - addresses, 534
- Member server
  - binding server to directory service of another server, 261
- Memory
  - Caching service requirements, 487
  - confirming computer qualified to run OS X Server, 26
  - hardware requirements for NetInstall, 453
  - RAM and system performance, 6
  - setting email storage quotas, 597
- Memory Pressure
  - monitoring performance with, 180
  - performance stats, 171
- Memory Usage
  - monitoring performance, 180
  - performance stats, 171
- Messages service
  - compatibility with Contacts service, 639
  - configuring federation of, 653
  - configuring messaging on administrator computer, 656
  - configuring messaging on server computer, 657
  - configuring users, 650
  - confirming SSL protection, 654
  - defining network ports, 651
  - description of, 106
  - logs, 652
  - managing, 649
  - overview of, 649
  - removing custom access rules, 661
  - requesting user authorization, 659
  - restricting federation of messages, 662
  - restricting user access, 660

- sending messages between Mac computers, 658
  - setting up, 654
  - starting, 655
  - testing access restrictions, 660
  - troubleshooting, 654
  - turning on archiving, 655
  - viewing archives, 664
  - viewing logs, 663
- Mobile computers
  - comparing Caching service and Software Update service for mobile clients, 491
  - DHCP leases and, 533
- Mobile Device Management (see MDM (Mobile Device Management))
- Monitoring
  - adding recipients of push alerts, 175
  - configuring alerts, 166-168, 173
  - configuring email recipients to receive alerts, 174
  - confirming alert operation, 177-179
  - DHCP service, 539, 549
  - disk space, 179
  - file server, 377
  - graphs for, 180
  - inspecting list of alerts to be sent, 176
  - inspecting/configuring recipients of push alerts, 174
  - logs for, 169-170
  - NetInstall service, 480
  - overview of, 165
  - sending test alert, 176
  - Server app sections for, 165
  - server with Server app, 173
  - stats for, 171-172
  - turning on push notifications, 173
  - viewing storage space, 172
  - web services, 558, 580
- MX (Mail eXchange) records
  - configuring DNS for Mail services, 588
  - looking up destination for email, 586
- N**
- Names
  - computer, 28
  - user account, 205
- Nameserver record
  - adding for reverse zone, 81
- NAT (Network Address Translation)
  - configuring VPN service, 517
  - modifying NAT rules on AirPort devices, 103
- Nested groups, 213
- Nested replicas, 257
- NetBIOS (Network Basic Input/Output System), 372
- NetBook
  - types of NetInstall images, 454
- NetBoot
  - comparing with NetInstall and NetRestore, 451, 452
  - customizing with System Image Utility, 457
  - operating system compatibility and, 459
- NetInstall service
  - advanced OS X Server services, 108
  - client startup process, 455
  - configuring protocol for, 474-476
  - creating customized image, 465, 467-471
  - creating images, 456
  - dedicated NetInstall subnets, 531
  - describing shadow files, 461
  - downloading trust profile for, 466
  - features and operating system compatibility, 459
  - hardware requirements, 453
  - image types, 454
  - inspecting customized image, 471
  - inspecting shared folders related to, 476
  - managing computers with, 452
  - monitoring, 480
  - monitoring log for, 480
  - NetInstall Connections tab, 480
  - NetRestore, 460
  - overview of, 451
  - preparing for use, 463
  - sources of images, 458
  - specifying default image, 476
  - starting, 473
  - starting up from NetInstall image, 478, 480
  - troubleshooting, 463
  - turning off, 481
  - uses of, 458
- NetRestore
  - comparing with NetInstall and NetBoot, 452
  - customizing with, 457
  - types of NetInstall images, 454
  - using, 460
- Network Address Translation (see NAT (Network Address Translation))
- Network Basic Input/Output System (NetBIOS), 372
- Network File System (see NFS (Network File System))
- Network Install
  - types of NetInstall images, 454
- Network interfaces
  - configuring, 31-35, 43
  - configuring server's interface, 535
  - speed requirements for hardware support, 6
- Network preferences
  - troubleshooting directory services, 272
- Network shares
  - as source for disk image, 459
- Network Time Protocol (see NTP (Network Time Protocol))
- Network Traffic
  - monitoring performance, 180
  - performance stats, 171
- Network users (see Local network accounts)
- Network Utility
  - checking DNS service, 153
  - confirming access to DNS records, 56
  - confirming new DNS records, 82
  - looking up DNS records, 85
  - troubleshooting directory services, 272
- Networks
  - configuring networking, 53-56
  - defining network ranges, 101
  - understanding DHCP networks, 532
- NFS (Network File System)

- configuring protocol for NetInstall image, 474
  - file-sharing services provided by, 373
  - in NetInstall client startup process, 455
  - inspecting file sharing services, 477
- Notes
- adding to user accounts, 206
- Notification Center
- alerts appearing in, 167
  - preferences, 178
- Notifications
- adding recipients of push alerts, 175
  - inspecting/configuring push notification recipients, 174
  - overview of, 165
  - replying to Calendar service invitations, 638
- NTP (Network Time Protocol)
- specifying time servers, 257
  - time-sensitivity of Kerberos and, 288
- O**
- OD (see Open Directory)
- Offer
- types of DHCP events, 543
- Open Directory
- accessing log files, 271
  - advanced OS X Server services, 108
  - archiving content of, 187
  - backing up, 197
  - binding OS X to, 270
  - Calendar service integration with, 625
  - CAs and, 126
  - configuring, 153-154
  - configuring server as master, 262, 264
  - configuring server as replica, 266-268
  - configuring to use another directory service, 268
  - creating archive for, 265
  - creating master role in preparing for Profile Manager, 307
  - describing roles of multiple servers, 261
  - describing service access, 261
  - directory service concepts, 253
  - global password policies, 283, 284
  - inspecting certificates, 155
  - inspecting certificates with Keychain Access, 156-159
  - inspecting group workgroup, 273
  - inspecting master, 273
  - Kerberos as component of, 288
  - locales, 259
  - master role, 256
  - overview of, 253
  - remote use of Directory Utility, 270
  - replica role, 257
  - service components, 255
  - single sign-on, 286
  - standalone server role, 256
  - static IPv4 addresses and, 11
  - troubleshooting, 271
  - troubleshooting certificates, 150
  - troubleshooting directory services, 272
  - troubleshooting using logs, 275
  - what it is, 254
- OpenLDAP, 255
- OS X Lion
- upgrading server to OS X Yosemite, 18
- OS X Mavericks
- Server Tutorials feature new in, 110
  - upgrading server to OS X Yosemite, 18
- OS X Mountain Lion
- upgrading server to OS X Yosemite, 18
- OS X Recovery
- creating external recovery system, 10
- OS X Server
- administering with Server app, 60-62
  - configuring server computer before installing (see Configuring server computer before installing OS X server)
  - configuring services for certificate use, 141
  - describing server roles, 256-258
  - importing groups into shared directory, 296
  - importing users into shared directory node, 293-296
  - installation (see Installing OS X Server)
  - installing from App Store, 39-40
  - mirroring updates on Apple servers, 497
  - Open Directory states, 255
  - opening installed server, 40-41
  - Provide Server Feedback option, 112
  - updating host name and starting DNS service, 42-45
  - viewing default certificate, 128-130
- OTA (over-the-air), Profile Manager function, 305
- Overview pane
- Server app, 97
- Ownership
- editing file ownership from Server app Storage pane, 100
- P**
- Parameter random-access memory), 479
- Partition Layout menu, 9
- Partitions
- hard disks, 7-10
  - Partition Layout menu, 9
- Password Assistant
- creating secure passwords, 278
- Password Server
- database supporting authentication protocols, 288
  - password policies and, 284
- Passwords
- archiving certificates and, 139
  - authentication methods and, 282
  - cleaning up policy for, 302
  - configuring Open Directory, 154
  - configuring policy for, 299-300
  - confirming policy for, 300-302
  - creating secure, 278
  - enforcing password policies, 254
  - entering wrong password at login, 203
  - for Local Admin accounts, 52

- setting global policy for, 284-286
  - storing in keychain, 61
  - updating for imported users, 233
- Performance bottlenecks
  - troubleshooting Caching service, 494
- Permissions
  - authorization to create wikis, 616
  - Calendar service, 625
  - changing to allow inspection of backup files, 195
  - cleaning up DNS access permissions, 90
  - comparing views of, 443-447
  - configuring complex permissions for ACEs, 419
  - configuring Mail services for, 589
  - confirming, 442
  - confirming permission are allowing desired access, 434-440
  - controlling access to Time Machine service, 506
  - creating wikis and, 617
  - editing from Server app Storage pane, 100
  - granting, 204
  - modifying manually, 414
  - Permissions dialog of Storage pane, 412
  - POSIX, 413
  - propagating, 424
  - protecting websites, 557
  - restricting access to DNS service, 87
  - restricting access to Messages service, 660
  - Time Machine access, 512
  - updating for new group, 441
  - updating to meet evolving needs, 440
- Ping tool
  - troubleshooting DHCP service, 542
- PKI (public key infrastructure), 123
- Placeholders
  - importing and assigning to device group, 342-343
- Point-to-Point Tunneling Protocol (PPTP), 517
- POP (Post Office Protocol), 587
- Portable Operating System Interface (see POSIX (Portable Operating System Interface))
- Ports
  - creating new websites, 574
  - defining for websites, 556
  - defining network ports for messages, 651
  - troubleshooting Calendar service, 628
  - troubleshooting Contacts service, 640
  - troubleshooting Messages service, 654
  - troubleshooting Wiki service, 614
- POSIX (Portable Operating System Interface)
  - ACL permissions and, 416
  - ACLs compared with, 425
  - comparing POSIX permissions and ACLs, 413
  - configuring file access with Sharing pane of Server app, 408
  - configuring ownership and permissions from Storage pane, 418
  - rules of precedence in POSIX and ACLs, 427
  - scalability of permissions, 427
  - share point access based on, 369
  - UNIX-style permission, 413
  - user and group ownership, 425
- Post Office Protocol (POP), 587
- Postfix
  - email packages Mail services is based on, 585
- PPTP (Point-to-Point Tunneling Protocol), 517
- PRAM (parameter random-access memory), 479
- Private keys
  - in PKI, 123
- Processor Usage
  - monitoring performance with, 180
  - performance stats, 171
- Profile Manager
  - account management, 327
  - administering, 305
  - basic OS X Server services, 106
  - cleaning up configuration, 324
  - confirming administrator computer is enrolled, 360
  - confirming effects of profiles, 361
  - creating configuration profile for device group, 344-347
  - creating enrollment profile, 350
  - creating new administrator account, 355
  - creating/distributing VPN profile, 522
  - Device Enrollment Program, 311
  - distributing certificates via, 149
  - distributing VPN configuration profile, 519
  - downloading trust profile, 466
  - enabling, 308
  - enrolling administrator computer, 356-360
  - enrolling devices using user portal, 354
  - functionality of, 305
  - importing and assigning placeholders to device group, 342-343
  - installing profiles, 340
  - layering and multiple profile considerations, 338
  - levels of management, 328
  - managing apps, 329
  - managing device group accounts, 329
  - managing preferences, 332, 338
  - managing preferences of users in a group, 328
  - Open Directory as requirement for, 253
  - preparing for configuration, 307
  - preparing for one-to-one devices, 352-354
  - preparing for shared devices, 341
  - problems enrolling devices, 340
  - profile delivery options, 330
  - pushing profiles, 340
  - remote management with, 363
  - remotely locking or wiping devices, 331
  - static IPv4 addresses and, 11

- terminology, 306
  - testing configuration profile, 347-350
  - troubleshooting, 340
  - Trust Profile, 466
  - trusted certificates and, 153
  - turning on device management, 312-315
  - turning on MDM, 306
  - turning on with Device Enrollment Program active, 316-321
  - turning on with Volume Purchase Program active, 321, 324
  - unenrolling from, 364
  - unexpected profile behaviors, 341
  - user portal website, 306
  - viewing logs, 340
  - viewing profiles, 340
  - Volume Purchase Program, 309
  - Web app for accessing, 306
- Profiles**
- confirming effects of, 361
  - creating configuration profile for device group, 344-347
  - creating enrollment profile, 350
  - defined, 306
  - delivery options, 330
  - installing, 340
  - installing and using VPN profile, 526
  - layering and multiple profile considerations, 338
  - obtaining from user portal website, 306
  - overview of, 305
  - pushing, 340
  - saving VPN configuration profile, 521
  - testing configuration profile, 347-350
  - viewing, 340
- Public key infrastructure (PKI), 123**
- Public keys**
- in PKI, 123
  - uploading, 318
- Push notification**
- calendar events and, 624
  - confirming alert operation, 177-179
  - email and, 585
  - enabling Profile Manager and, 308
  - inspecting/configuring push notification recipients, 174
  - making available, 166
  - profile delivery options, 330
  - sending test alert, 176
  - turning on Apple push notification service, 173
- Q**
- Quick Look**
- viewing blogs or wikis, 614, 619
- Quotas**
- email storage, 590
- R**
- RAID (Redundant Array of Independent Disks), 10**
- RAM (Random Access Memory)**
- hardware requirements for OS X Server installation, 6
  - understanding hardware requirements, 4
- Read set, of permissions**
- configuring complex permissions for ACEs, 420
- Records, DNS**
- adding nameserver record for reverse zone, 81
  - collecting DNS configuration data, 72
  - components of DNS service, 65
  - confirming new, 82-84
  - creating, 71, 76
  - creating new record from Show All Records dialog, 78
  - inspecting new, 77
  - looking up MX records, 83
  - troubleshooting, 71
  - TTL (time to live), 64
- Redirects**
- inspecting automatic redirect settings, 562
  - to other URLs, 561
- Redundant Array of Independent Disks (RAID), 10**
- Relaying outgoing mail**
- inspecting options for, 596
  - methods for, 589
- Remote Management**
- allowing remote access via Server app, 93-96
  - configuring server to allow remote administration, 47
  - confirming it is turned on, 113
  - demonstrating, 363
  - enabling, 94
  - installing, 358
  - turning on, 29, 52, 113
- Replica role**
- configuring OS X server as Open Directory replica, 266-268
  - describing server roles, 257
- Reply to email**
- checking reply to sent message, 606
  - overview of, 605
  - Reply All option, 606
- Request**
- flow of DNS request, 63
  - types of DHCP events, 543
- Requestor**
- DNS components, 64
- Resources, Calendar service**
- creating, 632
  - overview of, 626
  - sending invitations and, 635
- Restore, 503**
- (see also Time Machine)
- Reverse lookup zones**
- adding nameserver record for, 81
  - configuring recursive lookup restrictions, 85-87
- Root CA**
- defined, 125
  - following certificate chain, 142
  - trust and, 145
- S**
- SACLs (service access controls lists), 218**
- Safari**
- confirming new website is active, 575
  - confirming website is removed, 576
  - displaying information about computer, 360
  - preventing automatic entry of URL, 560

- requesting web page that does not exist, 581
- viewing SSL certificates, 163
- SAS (serial-attached SCSI), 6
- Schedules
  - backup, 187
  - Calendar services and, 625
- Screen sharing
  - confirming ability to connect, 113
  - confirming it is turned on, 113
  - enabling, 94
  - functions of Messages service, 649
  - opening Screen Sharing application, 96
  - turning on, 113
  - turning on remote management, 29
- Secure File Transfer Protocol (SFTP), 375
- Secure Shell (see SSH (Secure Shell))
- Secure Sockets Layer (see SSL (Secure Sockets Layer))
- Self-signed certificates
  - deciding what kind of certificate to use, 127
  - default SSL certificate, 127
  - examining default certificate, 150
  - generating, 135
  - overview of, 124
  - path to generating, 131
- Serial-attached SCSI (SAS), 6
- Server app
  - Access pane, 100, 216
  - accessing as nonadministrative user, 228
  - Accounts section, 105
  - adding group membership to user account, 238
  - adding groups to groups, 239
  - adding recipients of push alerts, 175
  - adding users to groups, 237
  - administering server with, 60-62
  - administrators use of, 209
  - advanced services, 107
  - AirPort pane, 102
  - Alerts, 46
  - allowing access to service from another directory node, 280
  - allowing remote access, 93-96
  - allowing user access to services and files, 209
  - archiving certificates and, 140
  - assigning local users to local groups, 210
  - Certificates pane, 131
  - changing folder used by default website, 564
  - changing service data volume, 115
  - choosing backup destination, 505
  - cleaning up DNS access permissions, 90
  - cleaning up password policy, 302
  - configuring ACLs from Sharing pane, 416
  - configuring ACLs from Storage pane, 418
  - configuring Caching service, 486
  - configuring Contacts service, 641, 642
  - configuring DHCP service, 535
  - configuring email recipients to receive alerts, 174
  - configuring file access with Storage pane, 411
  - configuring global password policies, 285
  - configuring local user accounts, 208
  - configuring Open Directory services, 262
  - configuring password policy, 299
  - configuring remote administration, 47
  - configuring server as Open Directory master, 153, 264
  - configuring server as replica of another Open Directory master, 266
  - configuring services for certificate use, 141
  - configuring user accounts, 204
  - configuring users and groups for file sharing, 375
  - configuring VPN service, 516
  - confirming Caching service is turned on, 493
  - confirming capacity for screen sharing connections, 113
  - confirming custom access rules, 121
  - confirming default website is using new content, 568
  - confirming existence of files for removed site, 576
  - confirming Mail services is running, 601
  - confirming modified access rules, 119
  - confirming screen sharing and remote management are turned on, 113
  - connecting to server via different account, 223-225
  - creating Calendar service locations, 632
  - creating groups, 235
  - creating local groups, 210
  - creating new shared folder, 381
  - creating new user, 220
  - creating new websites, 573
  - creating Open Directory CAs, 152
  - creating share points, 373
  - creating user templates, 225
  - defining Open Directory locales, 259
  - deleting user accounts, 251
  - DHCP pane, 536
  - disabling user accounts, 283
  - editing user attributes, 221
  - examining Mail Service logs, 609
  - examining VPN service logs, 528
  - exploring Access tab, 116
  - functions of Server section, 96
  - generating self-signed certificate, 135
  - Help menu, 110
  - Images pane, 476
  - importing list of users, 213
  - importing local network groups, 296
  - importing local network users, 293
  - importing users from exported formatted file, 230, 232
  - inspecting Calendar service invitation settings, 630

- inspecting groups, 601
- inspecting Open Directory certificates, 155
- inspecting performance graphs, 180
- inspecting SSL certificates, 137
- inspecting status of backups at server level, 511
- inspecting user accounts, 600
- inspecting user membership in groups, 244
- inspecting Workgroup group, 273
- inspecting/configuring push notification recipients, 174
- installing, 60
- installing OS X Server, 16
- Logs pane, 169, 193, 197
- maintaining file sharing, 377
- Manage menu options, 108
- managing network users, 277
- modifying custom access rules, 120
- modifying default access rules, 117-119
- monitoring DHCP service, 549
- monitoring file servers, 378
- monitoring NetInstall service, 480
- monitoring OS X Server, 173
- monitoring sections of, 165
- moving location of service data, 99
- NetInstall pane, 481
- opening administrator computer, 48
- opening/closing, 40, 250
- overview of, 93
- Overview pane, 97
- remotely managing local user and group accounts, 203
- renewing SSL certificates, 140
- restoring default access rules, 121
- restricting access to services, 242
- reviewing Calendar service certificates, 629
- reviewing file sharing logs, 378
- Services section, 106
- Settings pane, 98
- Sharing pane for configuring file access, 408-410
- sidebar options, 96
- starting Change Host Name Assistant, 14
- starting/configuring File Sharing service, 376
- Stats pane, 488
- stopping sharing of website content, 569
- stopping/starting file sharing service, 394-396
- Storage pane, 100
- Tools menu, 109
- troubleshooting Open Directory using logs, 275
- troubleshooting VPN service, 522
- troubleshooting with, 112
- turning file sharing on/off, 218, 247, 297
- turning on Messages service, 654, 655
- turning on screen sharing and remote management, 113
- turning on web services, 562
- turning on/configuring Wiki service, 615
- turning websites on/off, 553
- updating server host name, 42
- viewing SSL certificates, 128
- viewing storage space, 172
- Your Server tabs, 97
- Server Message Block (see SMB (Server Message Block))
- Server section
  - of Server app, 96
- Server Tutorials
  - overview of, 110
- Servers
  - administering with Server app, 60
  - configuring Messages service on server computer, 657
  - configuring OS X Server before installing (see Configuring server computer before installing OS X server)
  - DNS (see DNS servers)
  - federation of Messages service servers, 653
  - installing OS X server (see Installing OS X Server)
  - OS X (see OS X Server)
  - setting up email account on server computer, 603-604
  - upgrading, 18
- Service access control lists (SACLs), 218
- Services, 106
  - (see also by individual service)
  - advanced, 107
  - allowing local user access, 209
  - basic, 106
  - configuring to use SSL, 142
  - describing access to Open Directory service, 261
  - groups used to manage access to, 217
  - inspecting access to, 244-247
  - inspecting options for moving service data to new volume, 115
  - managing access manually, 216
  - managing access to, 241
  - moving location of service data, 99
  - restricting access to, 242
  - troubleshooting access, 219
- Services section
  - Server app, 106
- Settings pane, Server app
  - overview of, 98
  - Shared Folders segment of, 379
- Setup Assistant
  - configuring OS X on administrator computer, 49
  - configuring OS X on server computer, 22-24
- SFTP (Secure File Transfer Protocol), 375
- Shadow files
  - describing, 461
- Shadow password
  - authentication methods and, 282
- Share points, 380
  - (see also File Sharing)
  - access settings, 369
  - adding ACEs for, 416
  - adding/removing, 381-383
  - configuring, 383
  - configuring access to, 407, 432
  - configuring file sharing service, 376
  - confirming permissions are allowing desired access, 434-440
  - creating, 378, 432

- creating with Server app, 373
  - default, 380
  - guest access, 410
  - Time Machine using network-based, 503
  - viewing available, 370
- Shared devices, preparing Profile Manager for, 341
- Shared folders, 369
  - (see also Share points)
  - assigning to groups, 400-403
  - configuring, 430
  - configuring access to, 407
  - creating, 398-400
  - creating and configuring, 431
  - creating new location for, 396-398
  - inspecting folders related to NetInstall service, 476
  - making available for home directories, 385
  - segment of Settings pane, 379
- Shares (see Share points)
- Sharing & Permissions
  - changing file access permissions, 195
- Sharing preferences, 28, 52
- Show All Certificates
  - viewing SSL certificates, 129
- Show All Records
  - creating new DNS record, 76, 78
  - inspecting limited default zones, 75
  - inspecting new zones and records, 77
- Simple Mail Transfer Protocol (see SMTP (Simple Mail Transfer Protocol))
- Single sign-on
  - Kerberos and, 286
  - using KDC, 282
- SMB (Server Message Block)
  - accessing Kerberized services, 288
  - comparing file-sharing protocols, 374
  - configuring file sharing service, 376
  - confirming password policy and, 300
  - connecting to network file services, 202
  - file-sharing with SMB3, 371
  - guest access, 384
  - inheritance of ACLs and, 566
  - making shared folders available for home directories, 385
  - monitoring file sharing performance, 180
  - multiple platform support, 389
  - POSIX ownership and permissions, 414
  - viewing connected users, 387
- SMTP (Simple Mail Transfer Protocol)
  - examining Mail Service logs, 609
  - inspecting email relay options, 596
  - role in delivery of email, 586
  - role in relaying outgoing email, 589
  - sending alert notifications and, 167
  - setting up email accounts, 604
  - setting up SMTP server for email account, 603
- Snapshots
  - Time Machine, 186
- Snow Leopard
  - upgrading server to OS X Yosemite, 18
- Software
  - updating, 35-36, 57
- Software Update service (see SUS (Software Update Service))
- Solid-state disk (SSD), 6
- Spam
  - enabling filtering, 596
  - preventing blacklists, greylists, and junk mail, 592
  - testing spam filter, 607
  - troubleshooting Mail services, 594
- SpamAssassin software package, 592
- Spamhaus Project, 592
- Split DNS
  - dealing with internal and external DNS servers, 67
- Spotlight searches
  - opening Console with, 295
- SSD (solid-state disks), 6
- SSH (Secure Shell)
  - allowing remote login, 95
- Secure FTP using for file transfer, 375
- SSL (Secure Sockets Layer)
  - adding new certificates, 131
  - archiving certificates, 139
  - certificate basics, 123-126
  - changing folder used by default secure website, 565
  - configuring administrator computer to trust SSL certificate, 159, 161
  - configuring certificates, 127
  - configuring Open Directory CA, 152
  - configuring services for certificate use, 141
  - configuring SSL certificates, 97
  - configuring trust, 146-149
  - confirming Mac computer trusts SSL certificate, 163
  - confirming protection in Calendar services, 629
  - confirming protection of Contacts service, 641
  - confirming protection of Mail services, 595
  - confirming protection of Messages service, 654
  - creating new websites, 574
  - deciding what kind of certificate to use, 127
  - default website protected by, 560
  - examining default certificate, 150
  - following certificate chain, 142-145
  - generating self-signed certificate, 135
  - getting SSL certificates from CAs, 62
  - importing signed certificates, 135
  - inspecting certificates, 137-139
  - inspecting service certificates, 574
  - issuing new SSL certificate, 571-573
  - obtaining trusted certificates, 131-134
  - obtaining/installing SSL certificate in preparation for using Profile Manager, 307

- protecting websites, 556
  - protecting wikis, 614
  - renewing certificates, 140
  - restricting access to default website, 579
  - securing services and, 515
  - troubleshooting certificates, 149
  - Trust Profile, 340
  - turning on Web service for temporary access to SSL certificate, 160
  - viewing server's default certificate, 128-130
  - visiting website protected by, 160
  - Standalone server role
    - describing server roles, 256
  - Startup
    - from NetInstall image, 478
  - Startup Disk pane
    - in System Preferences, 478
  - Startup disks
    - not using as backup destination, 507
  - Startup Manager
    - boot options using NetInstall image, 478
  - Startup volume
    - backing up, 9
    - Caching service using, 487
    - changing name of, 27
    - in Core Storage, 190
  - Static addresses
    - assigning, 540
    - comparing DHCP static and dynamic address assignment, 534
    - troubleshooting DHCP service issues, 542
  - Stats
    - exploring performance graphs, 180
    - monitoring performance with, 171, 172
    - monitoring via performance graphs, 180
  - Stats pane
    - Server app, 165, 488
  - Storage
    - confirming computer qualified to run OS X Server, 27
    - monitoring disk space, 179
    - setting email quotas, 597
    - setting quotas for Mail services users, 590
    - startup volume in Core Storage, 190
    - viewing storage space, 172
  - Storage pane, Server app
    - comparing views of permissions, 443
    - configuring ACLs, 418
    - configuring complex permissions for ACEs, 419
    - configuring file sharing, 411
    - overview of, 100, 166
    - Permissions dialog, 412
    - propagating permissions, 424
  - Storage Setting pane
    - preparing NetInstall service, 465
  - Student materials
    - downloading, 36-38, 58
  - Subnets
    - Caching servers and, 487
    - configuring multiple subnet ranges, 538
    - dedicated NetInstall subnets, 531
    - DHCP serving multiple subnets, 534
    - editing, 536-538
  - SUS (Software Update Service)
    - advanced OS X Server services, 108
    - Caching services compared with, 490
    - managing software updates, 497
    - overview of, 497
    - troubleshooting, 499
  - System
    - verifying system requirements for OS X Server installation, 4
  - System Image Utility
    - automating image installation, 458
    - creating NetInstall images, 456
    - customizing NetBoot, NetRestore, or Network Install configurations, 457
    - enrollment profile and, 341
    - tools for image creation and deployment, 451
  - System keychain
    - inspecting SSL certificates, 137
    - installing certificates in, 147
  - System logs
    - examining DHCP logs, 542
  - System Preferences
    - Administrators group unlocking preferences, 209
    - App Store preferences, 57
    - creating new administrator account, 25, 51, 355
    - managing for users in a group, 328
    - managing with Profile Manager, 332-338
    - Network preferences, 31, 48, 54, 570
    - setting computer name, 28
    - Sharing preferences, 48, 52, 380
    - Startup Disk pane, 478
    - Time Machine preferences, 191, 509
    - update preferences, 35
- ## T
- Tape
    - media options for backups, 184
  - TCP (Transmission Control Protocol)
    - configuring VPN service, 518
  - Templates
    - creating for user accounts, 208
    - creating user template, 225
    - using user template, 226
  - Text
    - editing in wikis, 618
  - Text delimited file
    - importing user accounts from, 230-232
  - Text messages
    - functions of Messages service, 649
  - TFTP (Trivial File Transfer Protocol), 455
  - TGT (ticket-granting ticket)
    - KDC providing, 287
    - obtaining using Ticket Viewer, 289
  - Thunderbolt
    - downloading student materials using removable disk, 59
  - Ticket Viewer
    - examining Kerberos tickets, 288
    - troubleshooting Kerberos, 292
  - Ticket-granting ticket (see TGT (ticket-granting ticket))

- Time Machine
    - as network service, 503-506
    - basic OS X Server services, 107
    - clients browsing to services, 10
    - configuring, 191
    - configuring for use with network, 506-509
    - configuring OS X computer to use Time Machine destination, 509
    - creating Open Directory archive, 265
    - excluding most files, 509-510
    - external disk as back up destination, 188, 189
    - for network backup, 503
    - inspecting backup files, 192
    - inspecting backup status at Time Machine server, 511
    - internal volume as back up destination, 189-191
    - overview of, 185
    - recommended for backing up OS X Server, 183
    - turning off at server level, 513
    - using server's network volume for, 510
    - what it will back up, 186
    - what it will not back up, 186
  - Time to live (TTL), DNS records, 64
  - Timestamps
    - displaying in UTC format, 197
  - TLDs (top-level domains)
    - DNS requests and, 64
  - Tools menu
    - administrative applications, 109
  - Trivial File Transfer Protocol (TFTP), 455
  - Troubleshooting
    - access to services, 219
    - Calendar service, 628
    - Contacts service, 640
    - DHCP, 541
    - directory services, 272
    - DNS service, 70
    - Messages service, 654
    - NetInstall, 463
    - SSL certificates, 149
    - SUS (Software Update service), 499
    - user import, 218
    - using Server app, 112
    - VPN service, 522
    - websites, 559
    - Wiki service, 614
  - Troubleshooting Caching service
    - confirming basic operation, 492
    - deleting items in testing, 492
    - logs, 493
    - moving service data volume, 495
    - overview of, 492
    - performance bottlenecks, 494
  - Troubleshooting File Sharing
    - inspecting AFP access log, 404
    - inspecting AFP error log, 405
    - overview of, 388
  - Troubleshooting local network accounts
    - Kerberos-related issues, 291
    - overview of, 291
  - Troubleshooting Mail services
    - examining logs, 609
    - problems and solutions, 593
  - Troubleshooting Open Directory
    - accessing log files, 271
    - logs for, 275
    - overview of, 271
  - Troubleshooting OS X Server Install
    - inspecting logs, 20
    - overview of, 20
  - Troubleshooting profiles
    - installing profiles, 340
    - overview of, 340
    - problems enrolling devices, 340
    - pushing profiles, 340
    - unexpected behavior, 341
    - viewing logs, 340
    - viewing profiles, 340
  - Trust Profile
    - downloading for NetInstall, 466
    - for NetInstall image, 466
    - SSL, 340
  - Trusted certificates
    - configuring administrator computer to trust SSL certificate, 159
    - configuring administrator computer to trust SSL certificates, 161
    - configuring trust, 146-149
    - confirming Mac computer trusts SSL certificate, 163
    - Get a Trusted Certificate wizard, 132
    - obtaining, 127, 131-134
  - TTL (time to live), DNS records, 64
  - Tunneling protocols
    - configuring VPN service, 517
- ## U
- UDP (User Datagram Protocol), 518
  - UID (user ID)
    - comparing POSIX and ACLS, 425
    - for differentiation of users, 208
  - umask
    - controlling POSIX permissions, 414
  - Uninterruptible power supply (UPS), 7
  - Universally Unique ID (UUID), 415
  - Updates, 497
    - (see also SUS (Software Update service))
    - computer update with NetInstall, 453
    - getting updates for OS X Server from App Store, 19
    - software update, 35-36, 57
  - Upgrade installation
    - inheriting Sharing settings, 96
    - to OS X Server for Yosemite, 18
  - UPS (uninterruptible power supply), 7
  - URLs (uniform resource locators)
    - for websites, 556
    - preventing Safari from entering automatically, 560
    - redirects and aliases, 561
  - USB
    - downloading student materials using removable disk, 59
  - User accounts
    - access control for wikis, 612
    - accessing Server app as nonadministrative user, 228
    - adding group membership to, 238
    - adding groups to groups, 239
    - adding users to groups, 237
    - advanced options, 206-208
    - assigning groups to groups, 213
    - assigning groups to users, 211
    - assigning users to groups, 210
    - authentication, 202
    - authorization, 203
    - configuring, 204-205
    - configuring file sharing for, 375

- configuring local users, 208-210
- configuring Message service users, 650
- connecting to server via different account, 223-225
- creating groups, 235
- creating local groups, 210
- creating new user, 220-221
- creating templates, 225
- default access rules, 101
- deleting, 251
- editing users, 221
- importing groups, 236
- importing list of users, 213
- importing local users, 229
- importing users from exported formatted file, 232
- importing using delimited text file, 230-232
- inspecting access to services, 244-247
- inspecting email accounts, 600
- inspecting group membership, 244
- inspecting groups, 601
- keywords and notes added to, 206
- layering and multiple profile considerations, 338
- levels of management and, 328
- managing access to files and services using groups, 217
- managing access to services, 241
- managing access to services manually, 216
- managing local users, 201
- managing preferences of users in a group, 328
- panes in Account section of Server app, 105
- preparing for networking, 250
- restricting access to services, 242
- setting mail quotas, 590
- specifying email address for local network accounts, 598-599
- templates, 208
- troubleshooting service access, 219
- troubleshooting user import, 218, 240
- turning on file sharing, 247-249

- updating passwords for imported users, 233
- using templates, 226
- User Datagram Protocol (UDP), 518
- User ID (see UID (user ID))
- User portal
  - enrolling devices using user portal, 354
  - profile delivery options, 330
  - remotely locking or wiping devices, 332
- Users & Groups
  - binding server to another Open Directory service, 269
  - preferences, 203
  - troubleshooting directory services, 272
- UTC (Coordinated Universal Time), 197
- UUID (universally unique ID), 415

**V**

- vCards
  - Contacts service use of open source technologies, 640
- Video conferencing
  - functions of Messages service, 649
- Virtual local area networks (VLANs), 534
- Virtual Private Networks (see VPNs (Virtual Private Networks))
- Viruses
  - confirming email message scanned for, 605
  - scanning incoming email, 591
  - starting Mail services and downloading virus definitions, 594
- VLANs (virtual LANs), 534
- Volume Purchase Program (see VPP (Volume Purchase Program))
- Volumes, 189
  - (see also Hard disks)
  - as backup target, 186
  - changing name of startup volume, 27
  - configuring Time Machine, 192
  - internal volume as back up destination, 189
  - mounted volumes as source for disk image, 459

- moving location of service data, 99
- moving service data to new volume, 115
- selecting for Caching service, 487
- Time Machine-dedicated, 504
- VPNs (Virtual Private Networks)
  - advanced configuration, 519
  - basic OS X Server services, 107
  - configuring and starting VPN service, 523-528
  - configuring VPN service, 516-519, 523
  - describing, 515
  - examining logs, 528
  - installing and using profile for, 526
  - removing VPN service, 529
  - saving configuration profile, 521
  - security provided by, 515
  - troubleshooting, 522
  - turning on VPN service, 525
- VPP (Volume Purchase Program)
  - enabling, 309
  - managing apps purchased with, 329
  - turning on Profile Manager with VPP active, 321-324

**W**

- Web app
  - accessing Profile Manager, 306
- Web-based Distributed Authoring and Versioning (see WebDAV (Web-based Distributed Authoring and Versioning))
- WebDAV (Web-based Distributed Authoring and Versioning)
  - accessing shared folders, 372
  - comparing file-sharing protocols, 374
  - configuring file sharing service, 376
  - enabling access to wiki files, 616
  - file-sharing services, 371
  - multiple platform support, 389
  - POSIX ownership and permissions, 414
  - reviewing file sharing logs, 378
- Websites
  - basic OS X Server services, 107

- changing folder used by default secure site, 565
  - changing folder used by default site, 564
  - configuring server to use additional IPv4 addresses, 570
  - confirming access restrictions, 579
  - confirming existence of files for removed site, 576
  - confirming operation of new site, 575
  - confirming removed site is no longer available, 576
  - confirming use of new content, 568
  - copying new content to site folder, 567
  - creating and removing, 569
  - creating new DNS record for, 570
  - creating new site, 573
  - customizing content of default websites, 564
  - describing basic structure of, 552
  - exploring default sites, 562
  - exploring response when web service is off, 560
  - hosting, 551
  - identifying Web service software, 551
  - inspecting automatic redirect settings, 562
  - inspecting service certificates, 574
  - issuing SSL certificate, 571-573
  - managing, 556-557
  - managing site access, 578
  - modifying default sites, 563
  - monitoring , 558, 580
  - profile delivery options, 330
  - removing additional IPv4 addresses , 577
  - removing site, 575
  - restricting access to, 578
  - restricting access to default site, 579
  - sharing site folder, 566-567
  - stopping file sharing, 569
  - troubleshooting, 559
  - turning sites on/off, 553
  - turning web services on temporarily, 160
  - turning web services on/off, 559, 562
  - user portal for enrolling devices with Profile Manager, 306
  - viewing access logs, 581
  - viewing default parameters, 560
  - visiting server site when service is off, 560
  - visiting SSL-protected, 160
  - Wi-Fi
    - configuring OS X server, 22
    - NetInstall not recommended over, 453
  - Wiki service
    - accessing wiki and blog as anonymous user, 621
    - adding blogs, 620
    - adding calendar to wikis, 638
    - configuring wiki settings, 620
    - configuring/managing wikis, 611-614
    - creating wikis, 616-618
    - description of, 107
    - editing text, 618
    - editing wikis, 618
    - enabling WebDAV for use with, 616
    - logging in and accepting comments, 621
    - overview of, 611
    - troubleshooting, 614
    - turning on, 615
    - turning on/configuring with Server app, 615
    - uploading documents to wikis, 619
    - who is authorized to create wikis, 616
  - Windows file sharing
    - File Sharing options, 105
  - Wiping devices
    - remotely, 331
  - Workflows
    - saving, 471
  - Workgroups
    - inspecting group workgroup, 273
  - Write set, of permissions
    - configuring complex permissions for ACEs, 420
- X**
- Xcode
    - basic OS X Server services, 107
  - XML (Extensible Markup Language), 305
  - XMPP (Extensible Messaging and Presence Protocol), 650
  - Xsan
    - advanced OS X Server services, 108
- Y**
- Your Server tabs, Server app, 97
- Z**
- Zones, DNS
    - adding nameserver record for reverse zone, 81
    - components of DNS service, 65
    - creating, 71
    - creating default zones, 69
    - in OS X Server-hosting DNS, 67
    - inspecting limited default zones, 75
    - inspecting new, 77
    - removing redundant, 80