Setting Solid Foundations

MacTech In Depth - OS X Server

Thursday, April 19, 2012

Max Buxton

max@callandy.com

Call Andy!

MACINTOSH CONSULTING

The Installation Sandwich

- Before Installation
- Data collection
- Internet DNS
- Routing

Call Andy!

The Installation Sandwich

Install... (ho hum)

The Installation Sandwich

- After Installation
- More DNS
- Certificates
- Open Directory

Call Andy!

Before: Data Collection

- Services
- Users & Groups
- Permissions
- Types of computers
- Share Points
- Amount of data to store
- Backup Plan
- Load Balance
- Machine Name(s)

Call Andy!

Internet DNS

- Get friendly with your ISP
  - Get a static IP address
    - Always a better solution than DDNS
      (not good for SMTP)

Call Andy!

DNS Settings at the Registrar

- Be able to log in to registrar account
- Probably web host account as well
- Get listed as one of the contacts
- Create record for static IP address
- At least one record for the machine

Call Andy!

Hosting Your Own Mail: Prep MX Records

- FQDN for the mail server must match the host name of the server
- External forward and reverse DNS translations & your external MX Record must also all match (“Hello, ISP?”)
- Don't forget a backup server MX Record

Call Andy!

SRV Records: Why and How?

- Type of DNS record: “Service Record”
- Used for “specified services”
  - Address Book (carddav)
  - iCal (caldav)
  - iChat (XMPP aka "Jabber")

Call Andy!

SRV Record Examples:

- iCal with SSL (port 8443):

  _caldavs._tcp 86400 IN SRV 0 1 8443 server.example.com

- iCal without SSL (port 80008):

  _caldav._tcp 86400 IN SRV 0 1 80008 server.example.com

Call Andy!

SPF

- Not suntan lotion
- “Sender Policy Framework”
- Open standard created to stop forgery of FROM addresses.
- Some ISPs will handle it for you

Call Andy!

Routing to your server

- Get familiar with your router
- Get a better router
  - Don’t rely on the ISP
  - Put ISP router in Bridge Mode
- DON’T DOUBLE NAT!

Call Andy!

How to Use Port Forwarding

- Every router interface is different
- Sometimes the terminology is different
  - Port Mapping
  - NAT Traversal
- To SSL or not to SLL

Call Andy!

Using a DMZ

- "Split horizon" or perimeter networking
- Allows external access to services
- Protects the LAN
- Be sure to lock it down

Stupid Router Tricks

- DMZ the ISP Router and use your own behind it
- Consider using dedicated WAPs instead of your primary router
- If your router is handing out DHCP, what DNS server is it handing to clients?

Call Andy!

Installation

Next Steps

- Please sir, may I have some more?
- Custom PDF
- Server.app

Call Andy!

Next Steps: PDF

Next Steps.

Congratulations! You've successfully set up Mac OS X Server, the world's easiest-to-use server operating system, and you're now ready to use many of the exciting services that it has to offer. To enhance the security, accessibility, and overall usefulness of your new server, there are a few additional changes you should make to your network, and this document will help you get started. These items may require changes to components of your network such as routers and other servers. If you don't have access to these components, contact the person who's responsible for them.

Port Forwarding

Your server is connected to the Internet through a NAT device, such as a network router, which may prevent some users who are outside your immediate network from accessing services. If you don't want to provide access to users outside your immediate network, you can skip this step.

To allow access to all users, including those outside your immediate network, you need to configure port forwarding on your NAT device. To do this, use your device's configuration software, which usually consists of several webpages at an address such as http://192.168.1.1 or http://192.168.1.254. Using Safari, you go to the configuration website, and then navigate to the webpage with settings for "Port Range Forwarding," "Port Mapping," "Firewall Settings," or "Virtual Server." In some cases, you can select standard services such as web or VPN and specify that each be forwarded to your server's IP address. In other cases, you must enter port numbers for services and enter your server's IP address for each one. For specific information about configuring your NAT device, see its documentation.

The ports to forward for many of your services are listed below. Some NAT devices may ask you to specify TCP or UDP for each port, while other devices don't. For a list of ports for additional services, search Server Admin help for "TCP and UDP port reference," or see http://support.apple.com/kb/TS1629

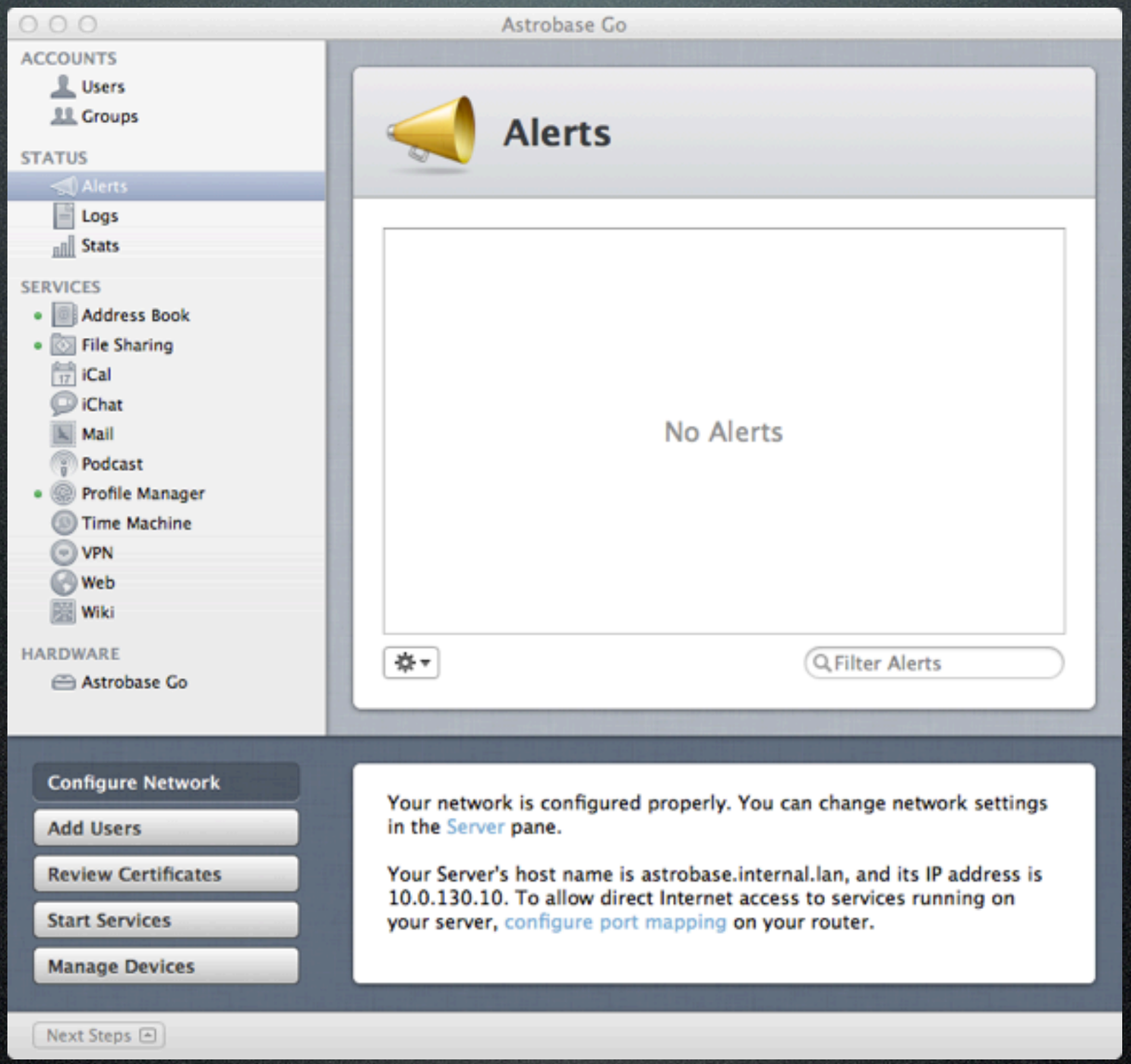
Description	Ports	Protocols
Apple File Service (AFP)	548	TCP

Next Steps: PDF

- Port Forwarding
- Configure DNS
- Create a Signed SSL Certificate

Call Andy!

Next Steps: Server.app



Certificates

- What is this and why do I need it?
- All SSL connections need it
- iCal won’t work without it
- Teaches your users to trust
- It’s the right thing to do

Call Andy!

Certificates: Different Kinds

- Self-signed
- Quick & Easy
- Not trusted
- Establishes bad user habits

Call Andy!

Certificates: Different Kinds

- CA-Signed
- You are “Official”
- Generate a CSR from your Self-signed cert
- Need to pay a Certificate Authority

Call Andy!

Certificates: Different Kinds

- Apple Push Notification Service
- APNS
- Enables delivery of push notifications

Call Andy!

Certificates: Final Tips

- Need to update if any of the other foundations change
- Trust Server.app

Call Andy!

Open Directory:
The King is Dead!

What is open directory?

“An extensible directory-services architecture
built into
OS X Lion & OS X Lion Server.”

Call Andy!

What Does It Do?

- Securely store and validate passwords
- Enforce policies
- Manage preferences (MCX)

Call Andy!

When did you need Open Directory?

- NetBoot
- Network Homes
- Managed Preferences (MCX)

Call Andy!

Open Directory:

Long live the king!

Why Use OD Today?

- NetBoot
- Network Homes
- Managed Preferences (MCX)
- Profile Management

Call Andy!

Why profiles deserve your attention

- Features beyond MCX:
  - Restrict resources
  - VPN & WiFi settings
  - Self Service
  - Manage iOS devices!

Call Andy!

Using Profiles: supplant or supplement MCX

- MCX is still in Work Group Manager
- Old tricks still apply
- Plenty of new tricks with Profile Manager

Call Andy!

HELP!
I'm still dealing with Active Directory!

Don’t Panic

- Golden Triangle to the rescue
  - AKA “Magic Triangle”
- What worked in 10.6 still (mostly) applies

Call Andy!

The Sandwich Summary

Before Installation	• Data collection • Internet DNS • Routing
Install	Zzzzzzz…
After Installation	• More DNS • Certificates • Open Directory

Call Andy!

Link List:
Apple Resources

www.apple.com/support/lionserver/	Apple - Support - Lion Server
help.apple.com/advancedserveradmin/mac/10.7/	Lion Server: Advanced Administration
docs.info.apple.com/article.html?path=Server/10.7/en/r_DNSrecords.html	OS X Lion Server Help: DNS records for your server
support.apple.com/kb/ts1629	Well known TCP and UDP ports used by Apple software products
docs.info.apple.com/article.html?path=ServerAdmin/10.6/en/odfd7c23d9.html	Server Admin 10.6 Help: Magic Triangle General Setup Overview

Link List:
Other Resources*

labs.hoffmanlabs.com/node/1436	DNS Tips: Establishing a DNS Server on Mac OS X Server 10.7 or 10.6 | HoffmanLabs
www.zytrax.com/books/dns/	DNS for Rocket Scientists - Contents
www.wowtutorial.org/node/84	How To Setup SPF Record | Wowtutorial
www.anandtech.com/show/4547/mac-os-x-lion-server-review	AnandTech - In-Depth with Mac OS X Lion Server
macs.about.com/od/OSXLion107/ss/Installing-Mac-Os-X-Lion-Server.htm	Installing Mac OS X Lion Server
discussions.apple.com/thread/3565475	How To Install An (Almost) Working Lion Server With Profile Management/SSL/OD/Mail/iCal/Address Book/VNC/Web/etc.
macs.about.com/od/OSXLion107/ss/Using-Server-App-Introduction-To-Administrating-Your-Os-X-Lion-Server.htm	Using Server App - Introduction to Administrating Your OS X Lion Server
portforward.com/	PortForward.com
community.spiceworks.com/how_to/show/237	Binding OS X to an Active Directory Domain for User Authentication - Spiceworks

* Use at your own risk. No endorsement implied. Void where prohibited by law. May cause headaches, nausea and irritable bowel syndrome. If symptoms persist, consult a professional. Not applicable in North Dakota. RAID is not backup.

Q & A

Max Buxton
max@callandy.com