



Ansible for DevOps

Server and configuration management for humans

Jeff Geerling

Ansible for DevOps

Server and configuration management for humans

Jeff Geerling

This book is for sale at <http://leanpub.com/ansible-for-devops>

This version was published on 2015-07-24

ISBN 978-0-9863934-0-2



This is a [Leanpub](#) book. Leanpub empowers authors and publishers with the Lean Publishing process. [Lean Publishing](#) is the act of publishing an in-progress ebook using lightweight tools and many iterations to get reader feedback, pivot until you have the right book and build traction once you do.

©2014 - 2015 Jeff Geerling

Tweet This Book!

Please help Jeff Geerling by spreading the word about this book on [Twitter](#)!

The suggested tweet for this book is:

I just purchased @Ansible4DevOps by @geerlingguy on @leanpub -
<https://leanpub.com/ansible-for-devops> #ansible

The suggested hashtag for this book is [#ansible](#).

Find out what other people are saying about the book by clicking on this link to search for this hashtag on Twitter:

<https://twitter.com/search?q=#ansible>

To my wife and children, and to the many readers who have helped make this book a reality.

Cover photograph and illustration © 2011 Jeff Geerling

Ansible is a software product distributed under the GNU GPLv3 open source license

Editing by Margie Newman and Katherine Geerling

Contents

Preface	i
Who is this book for?	i
Typographic conventions	ii
Please help improve this book!	iii
About the Author	iii
Introduction	iv
In the beginning, there were sysadmins	iv
Modern infrastructure management	iv
Ansible and Ansible, Inc.	v
Ansible Examples	vi
Other resources	vi
Chapter 1 - Getting Started with Ansible	1
Ansible and Infrastructure Management	1
On snowflakes and shell scripts	1
Configuration management	1
Installing Ansible	2
Creating a basic inventory file	4
Running your first Ad-Hoc Ansible command	5
Summary	6
Chapter 2 - Local Infrastructure Development: Ansible and Vagrant	7
Prototyping and testing with local virtual machines	7
Your first local server: Setting up Vagrant	8
Using Ansible with Vagrant	8
Your first Ansible playbook	9
Summary	12
Chapter 3 - Ad-Hoc Commands	13
Conducting an orchestra	13
Build infrastructure with Vagrant for testing	14
Inventory file for multiple servers	16
Your first ad-hoc commands	17

CONTENTS

Discover Ansible's parallel nature	17
Learning about your environment	19
Make changes using Ansible modules	21
Configure groups of servers, or individual servers	22
Configure the Application servers	22
Configure the Database servers	23
Make changes to just one server	24
Manage users and groups	25
Manage files and directories	26
Get information about a file	26
Copy a file to the servers	26
Retrieve a file from the servers	27
Create directories and files	27
Delete directories and files	27
Run operations in the background	28
Update servers asynchronously, monitoring progress	28
Fire-and-forget tasks	29
Check log files	30
Manage cron jobs	31
Deploy a version-controlled application	32
Ansible's SSH connection history	32
Paramiko	33
OpenSSH (default)	33
Accelerated Mode	33
Faster OpenSSH in Ansible 1.5+	34
Summary	35
Chapter 4 - Ansible Playbooks	36
Power plays	36
Running Playbooks with <code>ansible-playbook</code>	40
Limiting playbooks to particular hosts and groups	40
Setting user and sudo options with <code>ansible-playbook</code>	41
Other options for <code>ansible-playbook</code>	42
Real-world playbook: CentOS Node.js app server	42
Add extra repositories	43
Deploy a Node.js app	46
Launch a Node.js app	47
Node.js app server summary	48
Real-world playbook: Ubuntu LAMP server with Drupal	49
Include a variables file, and discover <code>pre_tasks</code> and <code>handlers</code>	49
Basic LAMP server setup	51
Configure Apache	52
Configure PHP with <code>lineinfile</code>	54

CONTENTS

Configure MySQL	55
Install Composer and Drush	55
Install Drupal with Git and Drush	57
Drupal LAMP server summary	59
Real-world playbook: Ubuntu Apache Tomcat server with Solr	59
Include a variables file, and discover <code>pre_tasks</code> and <code>handlers</code>	60
Install Apache Tomcat 7	60
Install Apache Solr	61
Apache Solr server summary	64
Summary	65
Chapter 5 - Ansible Playbooks - Beyond the Basics	66
Handlers	66
Environment variables	67
Per-play environment variables	68
Variables	70
Playbook Variables	70
Inventory variables	72
Registered Variables	73
Accessing Variables	73
Host and Group variables	75
<code>group_vars</code> and <code>host_vars</code>	76
Magic variables with host and group variables and information	76
Facts (Variables derived from system information)	77
Local Facts (<code>Facts.d</code>)	78
Variable Precedence	79
If/then/when - Conditionals	80
Jinja2 Expressions, Python built-ins, and Logic	81
<code>register</code>	82
<code>when</code>	82
<code>changed_when</code> and <code>failed_when</code>	84
<code>ignore_errors</code>	85
Delegation, Local Actions, and Pauses	85
Pausing playbook execution with <code>wait_for</code>	86
Running an entire playbook locally	87
Prompts	87
Tags	88
Summary	90
Chapter 6 - Playbook Organization - Roles and Includes	91
Includes	91
Handler includes	93
Playbook includes	93

&RPSOHWH LQFOXGHV H[DPSOH
5ROHV
5ROH VFDIIROGLQJ
%XLOGLQJ \RXU ILUVW UROH
0RUH IOH[LELOLW\ ZLWK UROH YDUV DQG GHIDXOWV
2WKHU UROH SDUWV KDQGOHUV ILOHV DQG WHPSODWHV
+DQGOHUV
)LOHV DQG 7HPSODWHV
2UJDQL]LQJ PRUH FRPSOH[DQG FURVV SODWIRUP UROHV
\$QVLEOH *DOD[\
*HWWLQJ UROHV IURP *DOD[\
8VLQJ UROH UHTXLULPHQWV ILOHV WR PDQDJH GHSHQ
\$ /\$03 VHUYHULQVL[OLQHV RI <\$0/
\$ 6ROU VHUYHULQVL[OLQHV RI <\$0/
+HOSIXO *DOD[\ FRPPDQGV
&RQWULEXWLQJ WR \$QVLEOH *DOD[\
6XPPDU\

&KDSWHU , QYHQWRULHV
\$ UHDO ZRUOG ZHE DSSOLF DWLRQ VHUYHULQYHQWRU\
1RQ SURG HQYLURQPHQWV VHSDUDWH LQYHQWRU\ ILOHV
, QYHQWRU\ YDULDEOHV
IPTU@WBST
HSPVQ@WBST
(SKHPHUDO LQIUDVWUXFWXUH '\QDPLF LQYHQWRU\
\QDPLF LQYHQWRU\ ZLWK 'LJLWD02FHDQ
'LJLWD02FHDQ DFFRXQW SUHUHTXLVLWHV
&RQQHFWLQJ WR \RXU 'LJLWD02FHDQ DFFRXQW
&UHDWLQJ D GURSOHW ZLWK \$QVLEOH
'LJLWD02FHDQ G\QDPEWFLQYHQWRU\ QZ WK
\QDPLF LQYHQWRU\ ZLWK \$:6
, QYHQWRU\ RE @ C1H0P\ VQ @ CZ
0XOWL SOH LQYHQWRU\ VRXUFHV PL[LQJ VWDWLF DQG G\
&UHDWLQJ FXVWRP G\QDPLF LQYHQWRULHV
%XLOGLQJ D &XVWRP '\QDPLF , QYHQWRU\ LQ 3\WKRQ
%XLOGLQJ D &XVWRP '\QDPLF , QYHQWRU\ LQ 3+3
0DQDJLQJ D 3DD6 ZLWK D &XVWRP '\QDPLF , QYHQWRU\
6XPPDU\

&KDSWHU \$QVLEOH &RRNERRNV
+LJKO\ \$YDLODEOH , QIUDVWUXFWXUH ZLWK \$QVLEOH
'LUHFWRU\ 6WUXFWXUH
, QGLYLGXDO 6HUYHU 3OD\ERRNV

CONTENTS

Main Playbook for Configuring All Servers	145
Getting the required roles	145
Vagrantfile for Local Infrastructure via VirtualBox	146
Provisioner Configuration: DigitalOcean	150
Provisioner Configuration: Amazon Web Services (EC2)	154
Summary	160
ELK Logging with Ansible	161
ELK Playbook	161
Forwarding Logs from Other Servers	165
Summary	170
GlusterFS Distributed File System Configuration with Ansible	170
Configuring Gluster - Basic Overview	172
Configuring Gluster with Ansible	172
Summary	178
Mac Provisioning with Ansible and Homebrew	178
Running Ansible playbooks locally	179
Automating Homebrew package and app management	179
Configuring Mac OS X through dotfiles	181
Summary	182
Docker-based Infrastructure with Ansible	182
A brief introduction to Docker containers	183
Using Ansible to build and manage containers	184
Building a Flask app with Ansible and Docker	186
Data storage container	190
Flask container	191
MySQL container	195
Ship it!	197
Summary	198
Chapter 9 - Deployments with Ansible	199
Deployment strategies	199
Simple single-server deployments	200
Provisioning a simple Ruby on Rails server	200
Deploying a Rails app to the server	202
Provisioning and Deploying the Rails App	206
Deploying application updates	208
Zero-downtime multi-server deployments	210
Ensuring zero downtime with serial and integration tests	217
Deploying to app servers behind a load balancer	219
Capistrano-style and blue-green deployments	225
Additional Deployment Features	226
Summary	227

CONTENTS

Chapter 10 - Server Security and Ansible	228
A brief history of SSH and remote access	228
Telnet	229
rlogin, rsh and rcp	230
SSH	230
The evolution of SSH and the future of remote access	232
Use secure and encrypted communication	233
Disable root login and use sudo	234
Remove unused software, open only required ports	235
Use the principle of least privilege	236
User account configuration	236
File permissions	237
Update the OS and installed software	238
Automating updates	238
Automating updates for RedHat-based systems	239
Automating updates for Debian-based systems	239
Use a properly-configured firewall	240
Configuring a firewall with ufw on Debian or Ubuntu	240
Configuring a firewall with firewalld on RedHat, Fedora, or CentOS	241
Make sure log files are populated and rotated	243
Monitor logins and block suspect IP addresses	244
Use SELinux (Security-Enhanced Linux) or AppArmor	244
Summary and further reading	246
Chapter 11 - Automating Your Automation - Ansible Tower and CI/CD	247
Ansible Tower	247
Getting and Installing Ansible Tower	248
Using Ansible Tower	249
Other Tower Features of Note	251
Tower Alternatives	252
Jenkins CI	252
Build a local Jenkins server with Ansible	253
Create an Ansible playbook on the Jenkins server	254
Create a Jenkins job to run an Ansible Playbook	255
Unit, Integration, and Functional Testing	256
Debugging and Asserting	257
The debug module	257
The fail and assert modules	259
Checking syntax and performing dry runs	260
Automated testing on GitHub using Travis CI	261
Setting up a role for testing	261
Testing the role's syntax	263
Role success - first run	263

CONTENTS

Role idempotence	263
Role success - final result	264
Some notes about Travis CI	264
Real-world examples	265
Functional testing using serverspec	265
Summary	266
Appendix A - Using Ansible on Windows workstations	267
Prerequisites	267
Set up an Ubuntu Linux Virtual Machine	268
Log into the Virtual Machine	268
Install Ansible	270
Summary	271
Appendix B - Ansible Best Practices and Conventions	272
Playbook Organization	272
Write comments and use name liberally	272
Include related variables and tasks	273
Use Roles to bundle logical groupings of configuration	274
Use role defaults and vars correctly	274
YAML Conventions and Best Practices	274
YAML for Ansible tasks	275
Three ways to format Ansible tasks	276
Shorthand/one-line (<code>key=value</code>)	276
Structured map/multi-line (<code>key:value</code>)	276
Folded scalars/multi-line (<code>></code>)	277
Using <code> </code> to format multiline variables	278
Using <code>ansible-playbook</code>	279
Use Ansible Tower	279
Specify <code>--forks</code> for playbooks running on > 5 servers	279
Use Ansible's Configuration file	279
Summary	280
Changelog	281
Current version	281
Version 0.99 (2015-07-19)	281
Version 0.97 (2015-06-10)	281
Version 0.95 (2015-05-26)	282
Version 0.94 (2015-05-16)	282
Version 0.92 (2015-04-09)	282
Version 0.90 (2015-03-16)	282
Version 0.89 (2015-02-26)	283
Version 0.88 (2015-02-13)	283

CONTENTS

Version 0.87 (2015-02-01)	283
Version 0.84 (2015-01-27)	283
Version 0.81 (2015-01-11)	284
Version 0.75 (2014-12-23)	284
Version 0.73 (2014-12-09)	284
Version 0.71 (2014-11-27)	284
Version 0.70 (2014-11-16)	284
Version 0.64 (2014-10-24)	285
Version 0.62 (2014-10-07)	285
Version 0.60 (2014-09-30)	285
Version 0.58 (2014-08-01)	285
Version 0.56 (2014-07-20)	286
Version 0.54 (2014-07-02)	286
Version 0.53 (2014-06-28)	286
Version 0.52 (2014-06-14)	286
Version 0.50 (2014-05-05)	286
Version 0.49 (2014-04-24)	287
Version 0.47 (2014-04-13)	287
Version 0.44 (2014-04-04)	287
Version 0.42 (2014-03-25)	287
Version 0.38 (2014-03-11)	288
Version 0.35 (2014-02-25)	288
Version 0.33 (2014-02-20)	288

Preface

Growing up, I had access to a world that not many kids ever get to enter. At the local radio stations where my dad was chief engineer, I was fortunate to get to see networks and IT infrastructure up close: Novell servers and old Mac and Windows workstations in the '90s; Microsoft and Linux-based servers; and everything in between. Best of all, he brought home decommissioned servers and copies of Linux burned to CD.

I began working with Linux and small-scale infrastructures before I started high school, and my passion for infrastructure grew as I built a Cat5 wired network and a small rack of networking equipment for a local grade school. When I started developing full-time, what was once a hobby became a necessary part of my job, so I invested more time in managing infrastructure efficiently. Over the past ten years, I've gone from manually booting and configuring physical and virtual servers; to using relatively complex shell scripts to provision and configure servers; to using configuration management tools to manage many cloud-based servers.

When I began converting my infrastructure to code, some of the best tools for testing, provisioning, and managing my servers were still in their infancy, but they have since matured into fully-featured, robust tools that I use every day. Vagrant is an excellent tool for managing local virtual machines to mimic real-world infrastructure locally (or in the cloud), and Ansible — the subject of this book — is an excellent tool for provisioning servers, managing their configuration, and deploying applications, even on my local workstation!

These tools are still improving rapidly, and I'm excited for what the future holds. New tools like Docker that are nearing production-ready status also excite me, and I know the time I invest in learning to use these tools well will be helpful for years to come. (Ansible, Docker, and Vagrant seem a potent combination for both local and production infrastructure, but that's a little outside of *this* book's scope.)

In these pages, I'll share with you all I've learned about provisioning and configuration! I'll also show you how to apply those concepts to your own projects. This book is for you if you're new to Ansible or looking for a refresher on its features and capabilities. Whether you're a sysadmin, developer, or anyone else involved in managing infrastructure, this book will help you get started with Ansible and make the most of its power.

tools like Jenkins, Capistrano, or Fabric. I am writing this book for these friends who, I think, are representative of most people who have heard of and/or are beginning to use Ansible.

If you are interested in both development and operations, and have at least a passing familiarity with managing a server via the command line, this book should provide you with an intermediate-to expert-level understanding of Ansible and how you can use it to manage your infrastructure.

Typographic conventions

Ansible uses a simple syntax (YAML) and simple command-line tools (using common POSIX conventions) for all its powerful abilities. Code samples and commands will be highlighted throughout the book either inline (for example: `ansible [command]`), or in a code block (with or without line numbers) like:

```
1 ---  
2 # This is the beginning of a YAML file.
```

Some lines of YAML and other code examples require more than 80 characters per line, resulting in the code wrapping to a new line. Wrapping code is indicated by a \ at the end of the line of code. For example:

```
1 # The line of code wraps due to the extremely long URL.  
2 wget http://www.example.com/really/really/really/long/path/in/the/url/causes/the\  
3 /line/to/wrap
```

When using the code, don't copy the \ character, and make sure you don't use a newline between the first line with the trailing \ and the next line.

Links to pertinent resources and websites are added inline, like the following link to [Ansible¹](#), and can be viewed directly by clicking on them in eBook formats, or by following the URL in the footnotes.

Sometimes, asides are added to highlight further information about a specific topic:



Informational asides will provide extra information.



Warning asides will warn about common pitfalls and how to avoid them.

¹<http://www.ansible.com/>



Tip asides will give tips for deepening your understanding or optimizing your use of Ansible.

When displaying commands run in a terminal session, if the commands are run under your normal/non-root user account, the commands will be prefixed by the dollar sign (\$). If the commands are run as the root user, they will be prefixed with the pound sign (#).

Please help improve this book!

This book is a work in progress, and is being expanded and updated on LeanPub at a rather rapid clip. If you think a particular section needs improvement or find something missing, please contact me via Twitter ([@geerlingguy²](#)), [Google+³](#), a comment on [this book's Feedback page on LeanPub⁴](#), or whatever method is convenient for you.

Please note that, since the book is still being written and proofread, the book contains certain imperfections and oddities. I've tried to ensure every line of code, at least, works perfectly, but I may have an occasional typo. You've been warned!

About the Author

[Jeff Geerling⁵](#) is a developer who has worked in programming and devops for companies with anywhere between one to thousands of servers. He also manages many virtual servers for services offered by [Midwestern Mac, LLC⁶](#) and has been using Ansible to manage infrastructure since early 2013.

²<https://twitter.com/geerlingguy>

³<https://plus.google.com/+JeffGeerling>

⁴<https://leanpub.com/ansible-for-devops/feedback>

⁵<http://jeffgeerling.com/>

⁶<http://www.midwesternmac.com/>

Introduction

In the beginning, there were sysadmins

Since the beginning of networked computing, deploying and managing servers reliably and efficiently has been a challenge. Historically, system administrators have typically been walled off from the developers and users who interact with the systems they administer, and so they have had to manage servers by hand, installing software, changing configurations, and administering services on individual servers.

As data centers grew, and hosted applications became more complex, administrators realized they couldn't scale their manual systems management as fast as the applications they were enabling. That's why server provisioning and configuration management tools came to flourish.

Server virtualization brought large-scale infrastructure management to the fore, and the number of servers managed by one admin (or by a small team of admins), has grown by an order of magnitude. Instead of deploying, patching, and destroying every server by hand, admins now are expected to bring up new servers, either automatically or with minimal intervention. Large-scale IT deployments now may involve hundreds or thousands of servers; in many of the largest environments, server provisioning, configuration, and decommissioning are all entirely automated.

Modern infrastructure management

As the systems that run applications become an ever more complex and integral part of the software they run, application developers themselves have begun to integrate their work more fully with operations personnel. In many companies, development and operations work is almost fully integrated. Indeed, this integration is a requirement for modern test-driven application design.

As a software developer by trade, and a sysadmin by necessity, I have seen the power in uniting development and operations—more commonly referred to now as DevOps. When developers begin to think of infrastructure as *part of their application*, stability and performance become normative. When sysadmins (most of whom have intermediate to advanced knowledge of the applications and languages being used on servers they manage) work tightly with developers, development velocity is improved, and more time is spent doing ‘fun’ activities like performance tuning, experimentation, and getting things done, and less time putting out fires.



Ansible is a loaded word; some people argue that using the word to identify both the **movement** of development and operations working more closely to automate infrastructure-related processes, and the **personnel** who skewed slightly more towards the system administration side of the equation, dilutes the word's meaning. I think the word has come to be a rallying cry for the employees who are dragging their startups, small businesses, and enterprises into a new era of infrastructure growth and stability. I'm not too concerned that the term has become more of a catch-all for modern infrastructure management. My advice: spend less time arguing over the definition of the word, and more time making it mean something *to you*

Ansible and Ansible, Inc.

Ansible was released in 2012 by Michael DeHaan ([@laserllama⁷](#) on Twitter), a developer who has been working with configuration management and infrastructure orchestration in one form or another for many years. Through his work with Puppet Labs and RedHat (where he worked on [Cobbler⁸](#), a configuration management tool and [Func⁹](#), a tool for communicating commands to remote servers), and [some other projects¹⁰](#), he experienced the trials and tribulations of many different organizations and individual sysadmins on their quest to simplify and automate their infrastructure management operations.

Additionally, Michael found [many shops were using separate tools¹¹](#) for configuration management (Puppet, Chef, cfengine), server deployment (Capistrano, Fabric), and ad-hoc task execution (Func, plain SSH), and wanted to see if there was a better way. Ansible wraps up all three of these features into one tool, and does it in a way that's actually *simpler* and more consistent than any of the other task-specific tools!

Ansible aims to be:

1. **Clear** - Ansible uses a simple syntax (YAML) and is easy for anyone (developers, sysadmins, managers) to understand. APIs are simple and sensible.
2. **Fast** - Fast to learn, fast to set up—especially considering you don't need to install a

5. **Secure** - Ansible uses SSH, and requires no extra open ports or potentially-vulnerable daemons on your servers.

Ansible also has a lighter side that gives the project a little personality. As an example, Ansible's major releases are named after Van Halen songs (e.g. 1.4 was named after 1980's "Could This Be Magic", and 1.5 after 1986's "Love Walks In"). Additionally, Ansible will use `cowsay`, if installed, to wrap output in an ASCII cow's speech bubble (this behavior can be disabled in Ansible's configuration).

[Ansible, Inc.](#)¹² was founded by Saïd Ziouani ([@SaidZiouani](#)¹³ on Twitter) and Michael DeHaan, and oversees core Ansible development and provides support (such as [Ansible Guru](#)¹⁴) and extra tooling (such as [Ansible Tower](#)¹⁵) to organizations using Ansible. Hundreds of individual developers have contributed patches to Ansible, and Ansible is the most starred infrastructure management tool on GitHub (with over 10,000 stars as of this writing). Ansible, Inc. has proven itself to be a good steward and promoter of Ansible so far, and I see no indication of this changing in the future.

Ansible Examples

There are many Ansible examples (playbooks, roles, infrastructure, configuration, etc.) throughout this book. Most of the examples are in the [Ansible for DevOps GitHub repository](#)¹⁶, so you can browse the code in its final state while you're reading the book. Some of the line numbering may not match the book *exactly* (especially if you're reading an older version of the book!), but I will try my best to keep everything synchronized over time.

Other resources

We'll explore all aspects of using Ansible to provision and manage your infrastructure in this book, but there's no substitute for the wealth of documentation and community interaction that make Ansible great. Check out the links below to find out more about Ansible and discover the community:

- [Ansible Documentation](#)¹⁷ - Covers all Ansible options in depth. There are few open source projects with documentation as clear and thorough.
- [Ansible Glossary](#)¹⁸ - If there's ever a term in this book you don't seem to fully understand, check the glossary.

¹²<http://www.ansible.com/>

¹³<https://twitter.com/SaidZiouani>

¹⁴<http://www.ansible.com/guru>

¹⁵<http://www.ansible.com/tower>

¹⁶<https://github.com/geerlingguy/ansible-for-devops>

¹⁷<http://docs.ansible.com/>

¹⁸<http://docs.ansible.com/glossary.html>

- [Ansible Mailing List¹⁹](#) - Discuss Ansible and submit questions with Ansible's community via this Google group.
- [Ansible on GitHub²⁰](#) - The official Ansible code repository, where the magic happens.
- [Ansible Example Playbooks on GitHub²¹](#) - Many examples for common server configurations.
- [Getting Started with Ansible²²](#) - A simple guide to Ansible's community and resources.
- [Ansible Blog²³](#)
- [Ansible Weekly²⁴](#) - A newsletter about Ansible, including notable cowsay quotes!

I'd like to especially highlight Ansible's documentation (the first resource listed above); one of Ansible's greatest strengths is its well-written and extremely relevant documentation, containing a large number of relevant examples and continuously-updated guides. Very few projects—open source or not—have documentation as thorough, yet easy-to-read. This book is meant as a supplement to, not a replacement for, Ansible's documentation!

¹⁹<https://groups.google.com/forum/#!forum/ansible-project>

²⁰<https://github.com/ansible/ansible>

²¹<https://github.com/ansible/ansible-examples>

²²<http://www.ansible.com/get-started>

²³<http://www.ansible.com/blog>

²⁴<http://devopsu.com/newsletters/ansible-weekly-newsletter.html>

Chapter 1 - Getting Started with Ansible

Ansible and Infrastructure Management

On snowflakes and shell scripts

Many developers and system administrators manage servers by logging into them via SSH, making changes, and logging off. Some of these changes would be documented, some would not. If an admin needed to make the same change to many servers (for example, changing one value in a config file), the admin would manually log into *each* server and repeatedly make this change.

If there were only one or two changes in the course of a server's lifetime, and if the server were extremely simple (running only one process, with one configuration, and a very simple firewall), *and* if every change were thoroughly documented, this process wouldn't be a problem.

But for almost every company in existence, servers are more complex—most run tens, sometimes hundreds of different applications. Most servers have complicated firewalls and dozens of tweaked configuration files. And even with change documentation, the manual process usually results in some servers or some steps being forgotten.

If the admins at these companies wanted to set up a new server *exactly* like one that is currently running, they would need to spend a good deal of time going through all of the installed packages, documenting configurations, versions, and settings; and they would spend a lot of unnecessary time manually reinstalling, updating, and tweaking everything to get the new server to run close to how the old server did.

Some admins may use shell scripts to try to reach some level of sanity, but I've yet to see a complex shell script that handles all edge cases correctly while synchronizing multiple servers' configuration and deploying new code.

Configuration management

Lucky for you, there are tools to help you avoid having these *snowflake servers*—servers that are uniquely configured and impossible to recreate from scratch because they were hand-configured without documentation. Tools like CFEngine²⁵, Puppet²⁶ and Chef²⁷ became very popular in the mid-to-late 2000s.

²⁵<http://cfengine.com/>

²⁶<http://puppetlabs.com/>

²⁷<http://www.getchef.com/chef/>

But there's a reason why many developers and sysadmins stick to shell scripting and command-line configuration: it's simple and easy-to-use, and they've had years of experience using bash and command-line tools. Why throw all that out the window and learn a new configuration language and methodology?

Enter Ansible. Ansible was built (and continues to be improved) by developers and sysadmins who know the command line—and want to make a tool that helps them manage their servers exactly the same as they have in the past, but in a repeatable and centrally managed way. Ansible also has other tricks up its sleeve, making it a true Swiss Army knife for people involved in DevOps (not just the operations side).

One of Ansible's greatest strengths is its ability to run regular shell commands verbatim, so you can take existing scripts and commands and work on converting them into idempotent playbooks as time allows. For someone (like me) who was comfortable with the command line, but never became proficient in more complicated tools like Puppet or Chef (which both required at least a *slight* understanding of Ruby and/or a custom language just to get started), Ansible was a breath of fresh air.

Ansible works by pushing changes out to all your servers (by default), and requires no extra software to be installed on your servers (thus no extra memory footprint, and no extra daemon to manage), unlike most other configuration management tools.



Idempotence is the ability to run an operation which produces the same result whether run once or multiple times ([source²⁸](#)).

An important feature of a configuration management tool is its ability to ensure the same configuration is maintained whether you run it once or a thousand times. Many shell scripts have unintended consequences if run more than once, but Ansible deploys the same configuration to a server over and over again without making any changes after the first deployment.

In fact, almost every aspect of Ansible modules and commands is idempotent, and for those that aren't, Ansible allows you to define when the given command should be run, and what constitutes a changed or failed command, so you can easily maintain an idempotent configuration on all your servers.

Installing Ansible

Ansible's only real dependency is Python. Once Python is installed, the simplest way to get Ansible running is to use pip, a simple package manager for Python.

If you're on a Mac, installing Ansible is a piece of cake:

²⁸http://en.wikipedia.org/wiki/Idempotence#Computer_science_meaning

1. Install [Homebrew²⁹](#) (get the installation command from the Homebrew website).
2. Install Python 2.7.x (`brew install python`).
3. Install Ansible (`sudo pip install ansible`).

You could also install Ansible via Homebrew with `brew install ansible`. Either way (`pip` or `brew`) is fine, but make sure you update Ansible using the same system with which it was installed!

If you're running Windows (i.e. you work for a large company that forces you to use Windows), it will take a little extra work to everything set up. There are two ways you can go about using Ansible if you use Windows:

1. The easiest solution would be to use a Linux virtual machine (with something like VirtualBox) to do your work. For detailed instructions, see [Appendix A - Using Ansible on Windows workstations](#).
2. Ansible runs (somewhat) within an appropriately-configured [Cygwin³⁰](#) environment. For setup instructions, please see my blog post [Running Ansible within Windows³¹](#), and note that *running Ansible directly within Windows is unsupported and prone to breaking*

If you're running Linux, chances are you already have Ansible's dependencies installed, but we'll cover the most common installation methods.

If you have `python-pip` and `python-devel` (`python-dev` on Debian/Ubuntu) installed, use `pip` to install Ansible (this assumes you also have the 'Development Tools' package installed, so you have `gcc`, `make`, etc. available):

```
$ sudo pip install ansible
```

Using `pip` allows you to upgrade Ansible with `pip install --upgrade ansible`.

Fedora/RHEL/CentOS:

The easiest way to install Ansible on a Fedora-like system is to use the official yum package. If you're running RedHat or CentOS, you need to install EPEL's RPM before you install Ansible (see the info section below for instructions):

```
$ yum -y install ansible
```

²⁹<http://brew.sh/>

³⁰<http://cygwin.com/>

³¹<https://servercheck.in/blog/running-ansible-within-windows>



On RedHat/CentOS systems, `python-pip` and `ansible` are available via the [EPEL repository](#)³². If you run the command `yum repolist | grep epel` (to see if the EPEL repo is already available) and there are no results, you need to install it with the following commands:

```
# If you're on RedHat/CentOS 6:  
$ rpm -ivh http://dl.fedoraproject.org/pub/epel/6/x86_64/\  
epel-release-6-8.noarch.rpm  
# If you're on RedHat/CentOS 7:  
$ rpm -ivh http://dl.fedoraproject.org/pub/epel/7/x86_64/\  
e/epel-release-7-5.noarch.rpm
```

Debian/Ubuntu

The easiest way to install Ansible on a Debian or Ubuntu system is to use the official apt package.

```
$ sudo apt-add-repository -y ppa:ansible/ansible  
$ sudo apt-get update  
$ sudo apt-get install -y ansible
```



If you get an error like “`sudo: add-apt-repository: command not found`”, you’re probably missing the `python-software-properties` package. Install it with the command:

```
$ sudo apt-get install python-software-properties
```

Once Ansible is installed, make sure it’s working properly by entering `ansible --version` on the command line. You should see the currently-installed version:

```
$ ansible --version  
ansible 1.9.2
```

Creating a basic inventory file

Ansible uses an inventory file (basically, a list of servers) to communicate with your servers. Like a hosts file (at `/etc/hosts`) that matches IP addresses to domain names, an Ansible inventory file matches servers (IP addresses or domain names) to groups. Inventory files can do a lot more, but for now, we’ll just create a simple file with one server. Create a file at `/etc/ansible/hosts` (the default location for Ansible’s inventory file), and add one server to it:

³²<https://fedoraproject.org/wiki/EPEL>

```
$ sudo mkdir /etc/ansible  
$ sudo touch /etc/ansible/hosts
```

Edit this hosts file with nano, vim, or whatever editor you'd like, but note you'll need to edit it with sudo as root. Put the following into the file:

```
1 [example]  
2 www.example.com
```

...where `example` is the group of servers you're managing and `www.example.com` is the domain name (or IP address) of a server in that group. If you're not using port 22 for SSH on this server, you will need to add it to the address, like `www.example.com:2222`, since Ansible defaults to port 22 and won't get this value from your ssh config file.



This first example assumes you have a server set up that you can test with; if you don't already have a spare server somewhere that you can connect to, you might want to create a small VM using DigitalOcean, Amazon Web Services, Linode, or some other service that bills by the hour. That way you have a full server environment to work with when learning Ansible—and when you're finished testing, delete the server and you'll only be billed a few pennies!

Replace the `www.example.com` in the above example with the name or IP address of your server.

Running your first Ad-Hoc Ansible command

Now that you've installed Ansible and created an inventory file, it's time to run a command to see if everything works! Enter the following in the terminal (we'll do something safe so it doesn't make any changes on the server):

```
$ ansible example -m ping -u [username]
```

...where `[username]` is the user you use to log into the server. If everything worked, you should see a message that shows `www.example.com | success >>`, then the result of your ping. If it didn't work, run the command again with `-vvvv` on the end to see verbose output. Chances are you don't have SSH keys configured properly—if you login with `ssh username@www.example.com` and that works, the above Ansible command should work, too.



Ansible assumes you're using passwordless (key-based) login for SSH (e.g. you login by entering `ssh username@example.com` and don't have to type a password). If you're still logging into your remote servers with a username and password, or if you need a primer on Linux remote authentication and security best practices, please read [Chapter 10 - Server Security and Ansible](#). If you insist on using passwords, add the `--ask-pass (-k)` flag to Ansible commands, but this entire book is written assuming passwordless authentication, so you'll need to keep this in mind every time you run a command or playbook.

Let's run a more useful command:

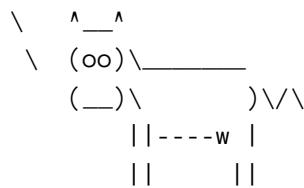
```
$ ansible example -a "free -m" -u [username]
```

In this example, we quickly see memory usage (in a human readable format) on all the servers (for now, just one) in the `example` group. Commands like this are helpful for quickly finding a server that has a value out of a normal range. I often use commands like `free -m` (to see memory statistics), `df -h` (to see disk usage statistics), and the like to make sure none of my servers is behaving erratically. While it's good to track these details in an external tool like [Nagios³³](#), [Munin³⁴](#), or [Cacti³⁵](#), it's also nice to check these stats on all your servers with one simple command and one terminal window!

Summary

That's it! You've just learned about configuration management and Ansible, installed it, told it about your server, and ran a couple commands on that server through Ansible. If you're not impressed yet, that's okay—you've only seen the *tip* of the iceberg.

```
/ A doctor can bury his mistakes but an \
| architect can only advise his clients |
\ to plant vines. (Frank Lloyd Wright) /
```



³³<http://www.nagios.org/>

³⁴<http://munin-monitoring.org/>

³⁵<http://www.cacti.net/>

Chapter 2 - Local Infrastructure Development: Ansible and Vagrant

Prototyping and testing with local virtual machines

Ansible works well with any server to which you can connect—remote *or* local. For speedier testing and development of Ansible playbooks, and for testing in general, it’s a very good idea to work locally. Local development and testing of infrastructure is both safer and faster than doing it on remote/live machines—especially in production environments!



In the past decade, test-driven development (TDD), in one form or another, has become the norm for much of the software industry. Infrastructure development hasn’t been as organized until recently, and best practices dictate that infrastructure (which is becoming more and more important to the software that runs on it) should be thoroughly tested as well.

Changes to software are tested either manually or in some automated fashion; there are now systems that integrate both with Ansible and with other deployment and configuration management tools, to allow some amount of infrastructure testing as well. Even if it’s just testing a configuration change locally before applying it to production, that approach is a thousand times better than what, in the software development world, would be called ‘cowboy coding’—working directly in a production environment, not documenting or encapsulating changes in code, and not having a way to roll back to a previous version.

The past decade has seen the growth of many virtualization tools that allow for flexible and very powerful infrastructure emulation, all from your local workstation! It’s empowering to be able to play around with a config file, or to tweak the order of a server update to perfection, over and over again, with no fear of breaking an important server. If you use a local virtual machine, there’s no downtime for a server rebuild; just re-run the provisioning on a new VM, and you’re back up and running in minutes—with no one the wiser.

Vagrant³⁶, a server provisioning tool, and VirtualBox³⁷, a local virtualization environment, make a potent combination for testing infrastructure and individual server configurations locally. Both applications are free and open source, and work well on Mac, Linux, or Windows hosts.

We’re going to set up Vagrant and VirtualBox for easy testing with Ansible to provision a new server.

³⁶<http://www.vagrantup.com/>

³⁷<https://www.virtualbox.org/>

Your first local server: Setting up Vagrant

To get started with your first local virtual server, you need to download and install Vagrant and VirtualBox, and set up a simple Vagrantfile, which will describe the virtual server.

1. Download and install Vagrant and VirtualBox (whichever version is appropriate for your OS):
- [Download Vagrant³⁸](#) - [Download VirtualBox³⁹](#) (when installing, make sure the command line tools are installed, so Vagrant works with it)
2. Create a new folder somewhere on your hard drive where you will keep your Vagrantfile and provisioning instructions.
3. Open a Terminal or PowerShell window, then navigate to the folder you just created.
4. Add a CentOS 7.x 64-bit ‘box’ using the `vagrant box add40` command: `vagrant box add geerlingguy/centos7` (note: HashiCorp’s [Atlas⁴¹](#) has a comprehensive list of different pre-made Linux boxes. Also, check out the ‘official’ Vagrant Ubuntu boxes on the [Vagrant wiki⁴²](#)).
5. Create a default virtual server configuration using the box you just downloaded: `vagrant init geerlingguy/centos7`
6. Boot your CentOS server: `vagrant up`

Vagrant has downloaded a pre-built 64-bit CentOS 7 virtual machine (you can [build your own⁴³](#) virtual machine ‘boxes’, if you so desire), loaded it into VirtualBox with the configuration defined in the default Vagrantfile (which is now in the folder you created earlier), and booted the virtual machine.

Managing this virtual server is extremely easy: `vagrant halt` will shut down the VM, `vagrant up` will bring it back up, and `vagrant destroy` will completely delete the machine from VirtualBox. A simple `vagrant up` again will re-create it from the base box you originally downloaded.

Now that you have a running server, you can use it just like you would any other server, and you can connect via SSH. To connect, enter `vagrant ssh` from the folder where the Vagrantfile is located. If you want to connect manually, or connect from another application, enter `vagrant ssh-config` to get the required SSH details.

Using Ansible with Vagrant

Vagrant’s ability to bring up preconfigured boxes is convenient on its own, but you could do similar things with the same efficiency using VirtualBox’s (or VMWare’s, or Parallels’) GUI. Vagrant has some other tricks up its sleeve:

³⁸<http://www.vagrantup.com/downloads.html>

³⁹<https://www.virtualbox.org/wiki/Downloads>

⁴⁰<http://docs.vagrantup.com/v2/boxes.html>

⁴¹<https://atlas.hashicorp.com/boxes/search>

⁴²<https://github.com/mitchellh/vagrant/wiki/Available-Vagrant-Boxes>

⁴³<http://docs.vagrantup.com/v2/virtualbox/boxes.html>

- **Network interface management⁴⁴**: You can forward ports to a VM, share the public network connection, or use private networking for inter-VM and host-only communication.
- **Shared folder management⁴⁵**: VirtualBox sets up shares between your host machine and VMs using NFS or (much slower) native folder sharing in VirtualBox.
- **Multi-machine management⁴⁶**: Vagrant is able to configure and control multiple VMs within one Vagrantfile. This is important because, as stated in the documentation, “Historically, running complex environments was done by flattening them onto a single machine. The problem with that is that it is an inaccurate model of the production setup, which behaves far differently.”
- **Provisioning⁴⁷**: When running `vagrant up` the first time, Vagrant automatically ***provisions*** the newly-minted VM using whatever provisioner you have configured in the Vagrantfile. You can also run `vagrant provision` after the VM has been created to explicitly run the provisioner again.

It's this last feature that is most important for us. Ansible is one of many provisioners integrated with Vagrant (others include basic shell scripts, Chef, Docker, Puppet, and Salt). When you call `vagrant provision` (or `vagrant up`) the first time, Vagrant passes off the VM to Ansible, and tells Ansible to run a defined Ansible playbook. We'll get into the details of Ansible playbooks later, but for now, we're going to edit our Vagrantfile to use Ansible to provision our virtual machine.

Open the Vagrantfile that was created when we used the `vagrant init` command earlier. Add the following lines just before the final ‘end’ (Vagrantfiles use Ruby syntax, in case you’re wondering):

```

1 # Provisioning configuration for Ansible.
2 config.vm.provision "ansible" do |ansible|
3   ansible.playbook = "playbook.yml"
4   # Run commands as root.
5   ansible.sudo = true
6 end

```

This is a very basic configuration to get you started using Ansible with Vagrant. There are **many other Ansible options⁴⁸** you can use once we get deeper into using Ansible. For now, we just want to set up a very basic playbook—a simple file you create to tell Ansible how to configure your VM.

Your first Ansible playbook

Let’s create the Ansible `playbook.yml` file now. Create an empty text file in the same folder as your Vagrantfile, and put in the following contents:

⁴⁴<http://docs.vagrantup.com/v2/networking/index.html>

⁴⁵<http://docs.vagrantup.com/v2/synced-folders/index.html>

⁴⁶<http://docs.vagrantup.com/v2/multi-machine/index.html>

⁴⁷<http://docs.vagrantup.com/v2/provisioning/index.html>

⁴⁸<http://docs.vagrantup.com/v2/provisioning/ansible.html>

```

1  ---
2  - hosts: all
3  tasks:
4  - name: Ensure NTP (for time synchronization) is installed.
5    yum: name=ntp state=installed
6  - name: Ensure NTP is running.
7    service: name=ntpd state=started enabled=yes

```

I'll get into what this playbook is doing in a minute. For now, let's run the playbook on our VM. Make sure you're in the same directory as the `Vagrantfile` and new `playbook.yml` file, and enter `vagrant provision`. You should see status messages for each of the 'tasks' you defined, and then a recap showing what Ansible did on your VM—something like the following:

```

PLAY RECAP ****
default : ok=3    changed=1    unreachable=0    failed=0

```

Ansible just took the simple playbook you defined, parsed the YAML syntax, and ran a bunch of commands via SSH to configure the server as you specified. Let's go through the playbook, step by step:

```

1  ---

```

This first line is a marker showing that the rest of the document will be formatted in YAML (read a [getting started guide for YAML⁴⁹](#)).

```

2  - hosts: all

```

This line tells Ansible to which hosts this playbook applies. `all` works here, since Vagrant is invisibly using its own Ansible inventory file (instead of the one we created earlier in `/etc/ansible/hosts`), which just defines the Vagrant VM.

```

3  tasks:

```

All the tasks after this line will be run on all hosts (or, in our case, our one VM).

```

4  - name: Ensure NTP daemon (for time synchronization) is installed.
5    yum: name=ntp state=installed

```

This command is the equivalent of running `yum install ntp`, but is much more intelligent; it will check if `ntp` is installed, and, if not, install it. This is the equivalent of the following shell script:

⁴⁹<http://www.yaml.org/start.html>

```

if ! rpm -qa | grep -qw ntp; then
    yum install ntp
fi

```

However, the above script is still not quite as robust as Ansible's `yum` command. What if `ntpdate` is installed, but not `ntp`? This script would require extra tweaking and complexity to match the simple Ansible `yum` command, especially after we explore the `yum` module more intimately (or the `apt` module, when using Ubuntu and Debian-flavored Linux).

```

6   - name: Ensure NTP is running.
7     service: name=ntpd state=started enabled=yes

```

This final task both checks and ensures that the `ntpd` service is started and running, and sets it to start at system boot. A shell script with the same effect would be:

```

# Start ntpd if it's not already running.
if ps aux | grep -v grep | grep "[n]tpd" > /dev/null
then
    echo "ntpd is running." > /dev/null
else
    /sbin/service ntpd restart > /dev/null
    echo "Started ntpd."
fi
# Make sure ntpd is enabled on system startup.
chkconfig ntpd on

```

You can see how things start getting complex in the land of shell scripts! And this shell script is still not as robust as what you get with Ansible. To maintain idempotency and handle error conditions, you'll have to do a lot more extra work with basic shell scripts than you do with Ansible.

We could be even more terse (and really demonstrate Ansible's powerful simplicity) and not use Ansible's `name` module to give human-readable names to each command, resulting in the following playbook:

```

1 ---
2 - hosts: all
3   tasks:
4     - yum: name=ntp state=installed
5     - service: name=ntpd state=started enabled=yes

```



Just as with code and configuration files, documentation in Ansible (e.g. using the `name` function and/or adding comments to the YAML for complicated tasks) is not absolutely necessary. However, I'm a firm believer in thorough (but concise) documentation, so I almost always document what my tasks will do by providing a `name` for each one. This also helps when you're running the playbooks, so you can see what's going on in a human-readable format.

Summary

Your workstation is on the path to becoming an “infrastructure-in-a-box,” and you can now ensure your infrastructure is as well-tested as the code that runs on top of it. With one small example, you’ve got a glimpse at the simple-yet-powerful Ansible playbook. We’ll dive deeper into Ansible playbooks later, and we’ll also explore Vagrant a little more as we go.

```
/ I have not failed, I've just found      \
| 10,000 ways that won't work. (Thomas |
\ Edison)                                /
```

```
\  ^__^
 \  (oo)\_____
  (__)\       )\/\
    ||----w |
    ||     ||
```

Chapter 3 - Ad-Hoc Commands

In the previous chapter, we ended our exploration of local infrastructure testing with Vagrant by creating a very simple Ansible playbook. Earlier still, we used a simple `ansible` ad-hoc command to run a one-off command on a remote server.

We'll dive deeper into playbooks in coming chapters; for now, we'll explore how Ansible helps you quickly perform common tasks on, and gather data from, one or many servers with ad-hoc commands.

Conducting an orchestra

The number of servers managed by an individual administrator has risen dramatically in the past decade, especially as virtualization and growing cloud application usage has become standard fare. As a result, admins have had to find new ways of managing servers in a streamlined fashion.

On any given day, a systems administrator has many tasks:

- Apply patches and updates via `yum`, `apt`, and other package managers.
- Check resource usage (disk space, memory, CPU, swap space, network).
- Check log files.
- Manage system users and groups.
- Manage DNS settings, hosts files, etc.
- Copy files to and from servers.
- Deploy applications or run application maintenance.
- Reboot servers.
- Manage cron jobs.

Nearly all of these tasks can be (and usually are) at least partially automated—but some often need a human touch, especially when it comes to diagnosing issues in real time. And in today's complex multi-server environments, logging into servers individually is not a workable solution.

Ansible allows admins to run ad-hoc commands on one or hundreds of machines at the same time, using the `ansible` command. In Chapter 1, we ran a couple of commands (`ping` and `free -m`) on a server that we added to our Ansible inventory file. This chapter will explore ad-hoc commands and multi-server environments in much greater detail. Even if you decide to ignore the rest of Ansible's powerful features, you will be able to manage your servers much more efficiently after reading this chapter.



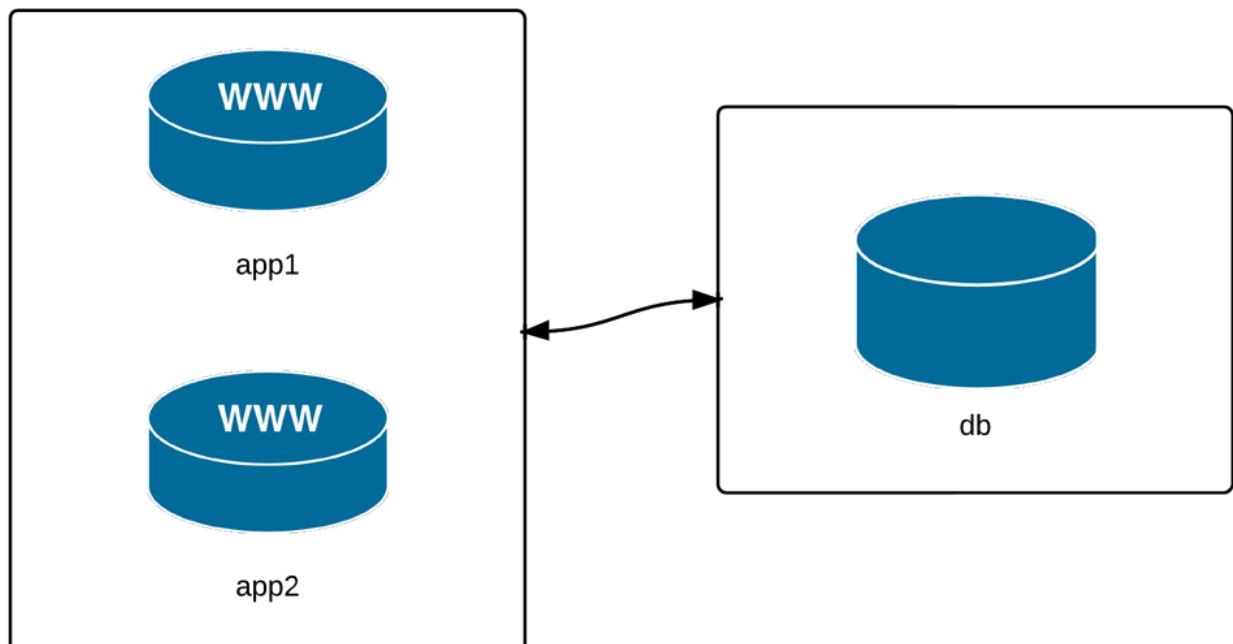
Some of the examples in this chapter will display how you can configure certain aspects of a server with ad-hoc commands. It is usually more appropriate to contain all configuration within playbooks and templates, so it's easier to provision your servers (running the playbook the first time) and then ensure their configuration is idempotent (you can run the playbooks over and over again, and your servers will be in the correct state).

The examples in this chapter are for illustration purposes only, and all might not be applicable to your environment. But even if you *only* used Ansible for server management and running individual tasks against groups of servers, and didn't use Ansible's playbook functionality at all, you'd still have a great orchestration and deployment tool in Ansible!

Build infrastructure with Vagrant for testing

For the rest of this chapter, since we want to do a bunch of experimentation without damaging any production servers, we're going to use Vagrant's powerful multi-machine capabilities to configure a few servers which we'll manage with Ansible.

Earlier, we used Vagrant to boot up one virtual machine running CentOS 7. In that example, we used all of Vagrant's default configuration defined in the Vagrantfile. In this example, we'll use Vagrant's powerful multi-machine management features.



Three servers: two application, one database.

We're going to manage three VMs: two app servers and a database server. Many simple web applications and websites have a similar architecture, and even though this may not reflect the vast realm of infrastructure combinations that exist, it will be enough to highlight Ansible's server management abilities.

To begin, create a new folder somewhere on your local drive (I like using `~/VMs/[dir]`), and create a new blank file named `Vagrantfile` (this is how we describe our virtual machines to Vagrant). Open the file in your favorite editor, and add the following, then save the file:

```

1 # -*- mode: ruby -*-
2 # vi: set ft=ruby :
3
4 VAGRANTFILE_API_VERSION = "2"
5
6 Vagrant.configure(VAGRANTFILE_API_VERSION) do |config|
7   config.ssh.insert_key = false
8   config.vm.provider :virtualbox do |vb|
9     vb.customize ["modifyvm", :id, "--memory", "256"]
10  end
11
12  # Application server 1.
13  config.vm.define "app1" do |app|
14    app.vm.hostname = "orc-app1.dev"
15    app.vm.box = "geerlingguy/centos7"
16    app.vm.network :private_network, ip: "192.168.60.4"
17  end
18
19  # Application server 2.
20  config.vm.define "app2" do |app|
21    app.vm.hostname = "orc-app2.dev"
22    app.vm.box = "geerlingguy/centos7"
23    app.vm.network :private_network, ip: "192.168.60.5"
24  end
25
26  # Database server.
27  config.vm.define "db" do |db|
28    db.vm.hostname = "orc-db.dev"
29    db.vm.box = "geerlingguy/centos7"
30    db.vm.network :private_network, ip: "192.168.60.6"
31  end
32 end

```

This `Vagrantfile` defines the three servers we want to manage, and gives each one a unique hostname,

machine name (for VirtualBox), and IP address. For simplicity's sake, all three servers will be running CentOS 7.

Open up a terminal window and change directory to the same folder where the Vagrantfile you just created exists. Enter `vagrant up` to let Vagrant begin building the three VMs. If you already downloaded the box while building the example from Chapter 2, this process shouldn't take too long—maybe 5-10 minutes.

While that's going on, we'll work on telling Ansible about the servers, so we can start managing them right away.

Inventory file for multiple servers

There are many ways you can tell Ansible about the servers you manage, but the most standard, and simplest, is to add them to your system's main Ansible inventory file, which is located at `/etc/ansible/hosts`. If you didn't create the file in the previous chapter, go ahead and create the file now; make sure your user account has read permissions for the file.

Add the following to the file:

```
1 # Lines beginning with a # are comments, and are only included for
2 # illustration. These comments are overkill for most inventory files.
3
4 # Application servers
5 [app]
6 192.168.60.4
7 192.168.60.5
8
9 # Database server
10 [db]
11 192.168.60.6
12
13 # Group 'multi' with all servers
14 [multi:children]
15 app
16 db
17
18 # Variables that will be applied to all servers
19 [multi:vars]
20 ansible_ssh_user=vagrant
21 ansible_ssh_private_key_file=~/vagrant.d/insecure_private_key
```

Let's step through this example, group by group:

1. The first block puts both of our application servers into an ‘app’ group.
2. The second block puts the database server into a ‘db’ group.
3. The third block tells ansible to define a new group ‘multi’, with child groups, and we add in both the ‘app’ and ‘db’ groups.
4. The fourth block adds variables to the multi group that will be applied to *all* servers within multi and all its children.



We'll dive deeper into variables, group definitions, group hierarchy, and other Inventory file topics later. For now, we just want Ansible to know about our servers, so we can start managing them quickly.

Save the updated inventory file, and then check to see if Vagrant has finished building the three VMs. Once Vagrant has finished, we can start managing the servers with Ansible.

Your first ad-hoc commands

One of the first things you need to do is to check in on your servers. Let's make sure they're configured correctly, have the right time and date (we don't want any time synchronization-related errors in our application!), and have enough free resources to run an application.



Many of the things we're manually checking here should also be monitored by an automated system on production servers; the best way to prevent disaster is to know when it could be coming, and to fix the problem *before* it happens. You should use tools like Munin, Nagios, Cacti, Hyperic, etc. to ensure you have a good idea of your servers' past and present resource usage! If you're running a website or web application available over the Internet, you should probably also use an external monitoring solution like Pingdom or Server Check.in.

Discover Ansible's parallel nature

First, I want to make sure Vagrant configured the VMs with the right hostnames. Use ansible with the -a argument ‘hostname’ to run hostname against all the servers:

```
$ ansible multi -a "hostname"
```

Ansible will run this command against all three of the servers, and return the results (if Ansible can't reach one a server, it will show an error for that server, but continue running the command on the others).



If Ansible reports No hosts matched or returns some other inventory-related error, try setting the `ANSIBLE_HOSTS` environment variable explicitly: `export ANSIBLE_HOSTS=/etc/ansible/hosts`. Generally Ansible will read the file in `/etc/ansible/hosts` automatically, but depending on how you installed Ansible, you may need to explicitly set `ANSIBLE_HOSTS` for the `ansible` command to work correctly.

You may have noticed that the command was not run on each server in the order you'd expect. Go ahead and run the command a few more times, and see the order:

```
# First run results:          # Second run results:  
192.168.60.5 | success | rc=0 >> 192.168.60.6 | success | rc=0 >>  
orc-app2.dev                  orc-db.dev  
  
192.168.60.6 | success | rc=0 >> 192.168.60.5 | success | rc=0 >>  
orc-db.dev  
  
192.168.60.4 | success | rc=0 >> 192.168.60.4 | success | rc=0 >>  
orc-app1.dev                  orc-app1.dev
```

By default, Ansible will run your commands in parallel, using multiple process forks, so the command will complete more quickly. If you're managing a few servers, this may not be much quicker than running the command serially, on one server after the other, but even managing 5-10 servers, you'll notice a dramatic speedup if you use Ansible's parallelism (which is enabled by default).

Run the same command again, but this time, add the argument `-f 1` to tell Ansible to use only one fork (basically, to perform the command on each server in sequence):

```
$ ansible multi -a "hostname" -f 1  
192.168.60.4 | success | rc=0 >>  
orc-app1.dev  
  
192.168.60.5 | success | rc=0 >>  
orc-app2.dev  
  
192.168.60.6 | success | rc=0 >>  
orc-db.dev
```

Run the same command over and over again, and it will always return results in the same order. It's fairly rare that you will ever need to do this, but it's much more frequent that you'll want to *increase* the value (like `-f 10`, or `-f 25...` depending on how much your system and network connection can handle) to speed up the process of running commands on tens or hundreds of servers.



Most people place the target of the action (`multi`) before the command/action itself (“on X servers, run Y command”), but if your brain works in the reverse order (“run Y command on X servers”), you could put the target *after* the other arguments (`ansible -a "hostname" multi`)—the commands are equivalent.

Learning about your environment

Now that we trust Vagrant’s ability to set hostnames correctly, let’s make sure everything else is in order.

First, let’s make sure the servers have disk space available for our application:

```
$ ansible multi -a "df -h"
192.168.60.6 | success | rc=0 >>
Filesystem           Size  Used Avail Use% Mounted on
/dev/mapper/centos-root  19G 1014M   18G  6% /
devtmpfs              111M    0  111M  0% /dev
tmpfs                 120M    0  120M  0% /dev/shm
tmpfs                 120M  4.3M  115M  4% /run
tmpfs                 120M    0  120M  0% /sys/fs/cgroup
/dev/sda1              497M 124M  374M 25% /boot
none                  233G 217G   17G 94% /vagrant

192.168.60.5 | success | rc=0 >>
Filesystem           Size  Used Avail Use% Mounted on
/dev/mapper/centos-root  19G 1014M   18G  6% /
devtmpfs              111M    0  111M  0% /dev
tmpfs                 120M    0  120M  0% /dev/shm
tmpfs                 120M  4.3M  115M  4% /run
tmpfs                 120M    0  120M  0% /sys/fs/cgroup
/dev/sda1              497M 124M  374M 25% /boot
none                  233G 217G   17G 94% /vagrant

192.168.60.4 | success | rc=0 >>
Filesystem           Size  Used Avail Use% Mounted on
/dev/mapper/centos-root  19G 1014M   18G  6% /
devtmpfs              111M    0  111M  0% /dev
tmpfs                 120M    0  120M  0% /dev/shm
tmpfs                 120M  4.3M  115M  4% /run
tmpfs                 120M    0  120M  0% /sys/fs/cgroup
/dev/sda1              497M 124M  374M 25% /boot
none                  233G 217G   17G 94% /vagrant
```

It looks like we have plenty of room for now; our application is pretty lightweight.

Second, let's also make sure there is enough memory on our servers:

```
$ ansible multi -a "free -m"
192.168.60.4 | success | rc=0 >>
      total        used        free      shared      buffers      cached
Mem:       238         187         50          4          1          69
-/+ buffers/cache:     116         121
Swap:      1055          0        1055

192.168.60.6 | success | rc=0 >>
      total        used        free      shared      buffers      cached
Mem:       238         190         47          4          1          72
-/+ buffers/cache:     116         121
Swap:      1055          0        1055

192.168.60.5 | success | rc=0 >>
      total        used        free      shared      buffers      cached
Mem:       238         186         52          4          1          67
-/+ buffers/cache:     116         121
Swap:      1055          0        1055
```

Memory is pretty tight, but since we're running three VMs on our localhost, we need to be a little conservative.

Third, let's make sure the date and time on each server is in sync:

```
$ ansible multi -a "date"
192.168.60.5 | success | rc=0 >>
Sat Feb  1 20:23:08 UTC 2021

192.168.60.4 | success | rc=0 >>
Sat Feb  1 20:23:08 UTC 2021

192.168.60.6 | success | rc=0 >>
Sat Feb  1 20:23:08 UTC 2021
```

Most applications are written with slight tolerances for per-server time jitter, but it's always a good idea to make sure the times on the different servers are as close as possible, and the simplest way to do that is to use the Network Time Protocol, which is easy enough to configure. We'll do that next, using Ansible's modules to make the process painless.



To get an exhaustive list of all the environment details ('facts', in Ansible's lingo) for a particular server (or for a group of servers), use the command `ansible [host-or-group] -m setup`. This will provide a list of every minute bit of detail about the server (including file systems, memory, OS, network interfaces... you name it, it's in the list).

Make changes using Ansible modules

We want to install the NTP daemon on the server to keep the time in sync. Instead of running the command `yum install -y ntp` on each of the servers, we'll use Ansible's `yum` module to do the same (just like we did in the playbook example earlier, but this time using an ad-hoc command).

```
$ ansible multi -s -m yum -a "name=ntp state=installed"
```

You should see three simple 'success' messages, reporting no change, since NTP was already installed on the three machines; this confirms everything is in working order.



The `-s` option (alias for `--sudo`) tells Ansible to run the command with sudo. This will work fine with our Vagrant VMs, but if you're running commands against a server where your user account requires a sudo password, you should also pass in `-k` (alias for `--ask-sudo-pass`), so you can enter your sudo password when Ansible needs it.

Now we'll make sure the NTP daemon is started and set to run on boot. We could use two separate commands, `service ntpd start` and `chkconfig ntpd on`, but we'll use Ansible's `service` module instead.

```
$ ansible multi -s -m service -a "name=ntp state=started enabled=yes"
```

All three servers should show a success message like:

```
"changed": true,
"enabled": true,
"name": "ntp",
"state": "started"
```

If you run the exact same command again, everything will be the same, but Ansible will report that nothing has changed, so the "changed" value becomes `false`.

When you use Ansible's modules instead of plain shell commands, you can use the powers of abstraction and idempotency offered by Ansible. Even if you're running shell commands, you could wrap them in Ansible's `shell` or `command` modules (like `ansible -m shell -a "date" multi`), but for these kind of commands, there's usually no need to use an Ansible module when running them ad-hoc.

The last thing we should do is check to make sure our servers are synced closely to the official time on the NTP server:

```
$ ansible multi -s -a "service ntpd stop"
$ ansible multi -s -a "ntpdate -q 0.rhel.pool.ntp.org"
$ ansible multi -s -a "service ntpd start"
```

For the `ntpdate` command to work, the `ntpd` service has to be stopped, so we stop the service, run the command to check our jitter, then start the service again.

In my test, I was within three one-hundredths of a second on all three servers—close enough for my purposes.

Configure groups of servers, or individual servers

Now that we've been able to get all our servers to a solid baseline (e.g. all of them at least have the correct time), we need to set up the application servers, then the database server.

Since we set up two separate groups in our inventory file, `app` and `db`, we can target commands to just the servers in those groups.

Configure the Application servers

Our hypothetical web application uses Django, so we need to make sure Django and its dependencies are installed. Django is not in the official CentOS yum repository, but we can install it using Python's `easy_install` (which, conveniently, has an Ansible module).

```
$ ansible app -s -m yum -a "name=MySQL-python state=present"
$ ansible app -s -m yum -a "name=python-setuptools state=present"
$ ansible app -s -m easy_install -a "name=django"
```

You could also install django using `pip`, which can be installed via `easy_install` (since Ansible's `easy_install` module doesn't allow you to uninstall packages like `pip` does), but for simplicity's sake, we've installed it with `easy_install`.

Check to make sure Django is installed and working correctly.

```
$ ansible app -a "python -c 'import django; print django.get_version()'"
192.168.60.4 | success | rc=0 >>
1.8

192.168.60.5 | success | rc=0 >>
1.8
```

Things look like they're working correctly on our app servers. We can now move on to our database server.



Almost all of the configuration we've done in this chapter would be much better off in an Ansible playbook (which will be explored in greater depth throughout the rest of this book). This chapter demonstrates how easy it is to manage multiple servers—for whatever purpose—using Ansible. Even if you set up and configure servers by hand using shell commands, using Ansible will save you a ton of time and help you do everything in the most secure and efficient manner possible.

Configure the Database servers

We configured the application servers using the `app` group defined in Ansible's main inventory, and we can configure the database server (currently the only server in the `db` group) using the similarly-defined `db` group.

Let's install MariaDB, start it, and configure the server's firewall to allow access on MariaDB's default port, 3306.

```
$ ansible db -s -m yum -a "name=mariadb-server state=present"
$ ansible db -s -m service -a "name=mariadb state=started enabled=yes"
$ ansible db -s -a "iptables -F"
$ ansible db -s -a "iptables -A INPUT -s 192.168.60.0/24 -p tcp \
-m tcp --dport 3306 -j ACCEPT"
```

If you try connecting to the database from the app servers (or your host machine) at this point, you won't be able to connect, since MariaDB still needs to be set up. Typically, you'd do this by logging into the server and running `mysql_secure_installation`. Luckily, though, Ansible can control a MariaDB server with its assorted `mysql_*` modules. For now, we need to allow MySQL access for one user from our app servers. The MySQL modules require the `MySQL-python` module to be present on the managed server.



Why MariaDB and not MySQL? RHEL 7 and CentOS 7 have MariaDB as the default supported MySQL-compatible database server. Some of the tooling around MariaDB still uses the old 'MySQL*' naming syntax, but if you're used to MySQL, things work similarly with MariaDB.

```
$ ansible db -s -m yum -a "name=MySQL-python state=present"  
$ ansible db -s -m mysql_user -a "name=django host=% password=12345 \  
priv=*.*:ALL state=present"
```

At this point, you should be able to create or deploy a Django application on the app servers, then point it at the database server with the username django and password 12345.



The MySQL configuration used here is for example/development purposes only! There are a few other things you should do to secure a production MySQL server, including removing the test database, adding a password for the root user account, restricting the IP addresses allowed to access port 3306 more closely, and some other minor cleanups. Some of these things will be covered later in this book, but, as always, you are responsible for securing your servers—make sure you’re doing it correctly!

Make changes to just one server

Congratulations! You now have a small web application environment running Django and MySQL. It’s not much, and there’s not even a load balancer in front of the app servers to spread out the requests; but we’ve configured everything pretty quickly, and without ever having to log into a server. What’s even more impressive is that you could run any of the ansible commands again (besides a couple of the simple shell commands), and they wouldn’t change anything—they would return “changed”: `false`, giving you peace of mind that the original configuration is intact.

Now that your local infrastructure has been running a while, you notice (hypothetically, of course) that the logs indicate one of the two app servers’ time has gotten way out of sync with the others, likely because the NTP daemon has crashed or somehow been stopped. Quickly, you enter the following command to check the status of `ntpd`:

```
$ ansible app -s -a "service ntpd status"
```

Then, you restart the service on the affected app server:

```
$ ansible app -s -a "service ntpd restart" --limit "192.168.60.4"
```

In this command, we used the `--limit` argument to limit the command to a specific host in the specified group. `--limit` will match either an exact string or a regular expression (prefixed with `~`). The above command could be stated more simply if you want to apply the command to only the `.4` server (assuming you know there are no other servers with the an IP address ending in `.4`), the following would work exactly the same:

```
# Limit hosts with a simple pattern (asterisk is a wildcard).
$ ansible app -s -a "service ntpd restart" --limit "*\.4"

# Limit hosts with a regular expression (prefix with a tilde).
$ ansible app -s -a "service ntpd restart" --limit ~".*\.\.4"
```

In these examples, we've been using IP addresses instead of hostnames, but in many real-world scenarios, you'll probably be using hostnames like nyc-dev-1.example.com; being able to match on regular expressions is often helpful.



Try to reserve the `--limit` option for running commands on single servers. If you often find yourself running commands on the same set of servers using `--limit`, consider instead adding them to a group in your inventory file. That way you can enter `ansible [my-new-group-name] [command]`, and save yourself a few keystrokes.

Manage users and groups

One of the most common uses for Ansible's ad-hoc commands in my day-to-day usage is user and group management. I don't know how many times I've had to re-read the man pages or do a Google search just to remember which arguments I need to create a user with or without a home folder, add the user to certain groups, etc.

Ansible's `user` and `group` modules make things pretty simple and standard across any Linux flavor.

First, add an `admin` group on the app servers for the server administrators:

```
$ ansible app -s -m group -a "name=admin state=present"
```

The `group` module is pretty simple; you can remove a group by setting `state=absent`, set a group id with `gid=[gid]`, and indicate that the group is a system group with `system=yes`.

Now add the user `johndoe` to the app servers with the group I just created and give him a home folder in `/home/johndoe` (the default location for most Linux distributions). Simple:

```
$ ansible app -s -m user -a "name=johndoe group=admin createhome=yes"
```

If you want to automatically create an SSH key for the new user (if one doesn't already exist), you can run the same command with the additional parameter `generate_ssh_key=yes`. You can also set the UID of the user by passing in `uid=[uid]`, set the user's shell with `shell=[shell]`, and the password with `password=[encrypted-password]`.

What if you want to delete the account?

```
$ ansible app -s -m user -a "name=johndoe state=absent remove=yes"
```

You can do just about anything you could do with `useradd`, `userdel`, and `usermod` using Ansible's `user` module, except you can do it more easily. The [official documentation of the User module](#)⁵⁰ explains all the possibilities in great detail.

Manage files and directories

Another common use for ad-hoc commands is remote file management. Ansible makes it easy to copy files from your host to remote servers, create directories, manage file and directory permissions and ownership, and delete files or directories.

Get information about a file

If you need to check a file's permissions, MD5, or owner, use Ansible's `stat` module:

```
$ ansible multi -m stat -a "path=/etc/environment"
```

This gives the same information you'd get when running the `stat` command, but passes back information in JSON, which can be parsed a little more easily (or, later, used in playbooks to conditionally do or not do certain tasks).

Copy a file to the servers

You probably use `scp` and/or `rsync` to copy files and directories to remote servers, and while Ansible has recently gained an `rsync` module, most file copy operations can be completed with Ansible's `copy` module:

```
$ ansible multi -m copy -a "src=/etc/hosts dest=/tmp/hosts"
```

The `src` can be a file or a directory. If you include a trailing slash, only the contents of the directory will be copied into the `dest`. If you omit the trailing slash, the contents *and* the directory itself will be copied into the `dest`.

The `copy` module is perfect for single-file copies, and works very well with small directories. When you want to copy hundreds of files, especially in very deeply-nested directory structures, you should consider either copying then expanding an archive of the files with Ansible's `unarchive` module, or using Ansible's `synchronize` module.

⁵⁰http://docs.ansible.com/user_module.html

Retrieve a file from the servers

The `fetch` module works almost exactly the same as the `copy` module, except in reverse. The major difference is that files will be copied down to the local dest in a directory structure that matches the host from which you copied them. For example, use the following command to grab the hosts file from the servers:

```
$ ansible multi -s -m fetch -a "src=/etc/hosts dest=/tmp"
```

Fetch will, by default, put the `/etc/hosts` file from each server into a folder in the destination with the name of the host (in our case, the three IP addresses), then in the location defined by `src`. So, the db server's hosts file will end up in `/tmp/192.168.60.6/etc/hosts`.

You can add the parameter `flat=yes`, and set the `dest` to `dest=/tmp/` (add a trailing slash), to make Ansible fetch the files directly into the `/tmp` directory. However, filenames must be unique for this to work, so it's not as useful when copying down files from multiple hosts. Only use `flat=yes` if you're copying files from a single host.

Create directories and files

You can use the `file` module to create files and directories (like `touch`), manage permissions and ownership on files and directories, modify SELinux properties, and create symlinks.

Here's how to create a directory:

```
$ ansible multi -m file -a "dest=/tmp/test mode=644 state=directory"
```

Here's how to create a symlink (set `state=link`):

```
$ ansible multi -m file -a "src=/src/symlink dest=/dest/symlink \
owner=root group=root state=link"
```

Delete directories and files

You can set the `state` to `absent` to delete a file or directory.

```
$ ansible multi -m file -a "dest=/tmp/test state=absent"
```

There are many simple ways to manage files remotely using Ansible. We've briefly covered the `copy` and `file` modules here, but be sure to read the documentation for the other file-management modules like `lineinfile`, `ini_file`, and `unarchive`. This book will cover these additional modules in depth in later chapters (when dealing with playbooks).

Run operations in the background

Some operations take quite a while (minutes or even hours). For example, when you run `yum update` or `apt-get update && apt-get dist-upgrade`, it could be a few minutes before all the packages on your servers are updated.

In these situations, you can tell Ansible to run the commands asynchronously, and poll the servers to see when the commands finish. When you're only managing one server, this is not really helpful, but if you have many servers, Ansible starts the command **very** quickly on all your servers (especially if you set a higher `--forks` value), then polls the servers for status until they're all up to date.

To run a command in the background, you set the following options:

- `-B <seconds>`: the maximum amount of time (in seconds) to let the job run.
- `-P <seconds>`: the amount of time (in seconds) to wait between polling the servers for an updated job status.

Update servers asynchronously, monitoring progress

Let's run `yum -y update` on all our servers to get them up to date. If we leave out `-P`, Ansible defaults to polling every 10 seconds:

```
$ ansible multi -s -B 3600 -a "yum -y update"
background launch...
```

```
192.168.60.6 | success >> {
    "ansible_job_id": "763350539037",
    "results_file": "/root/.ansible_async/763350539037",
    "started": 1
}

... [other hosts] ...
```

Wait a little while (or a *long* while, depending on how old the system image is we used to build our example VMs!), and eventually, you should see something like:

```
<job 763350539037> finished on 192.168.60.6 => {
    "ansible_job_id": "763350539037",
    "changed": true,
    "cmd": [
        "yum",
        "-y",
        "update"
    ],
    "delta": "0:13:13.973892",
    "end": "2021-02-09 04:47:58.259723",
    "finished": 1,
    ...
    ... [more info and stdout from job] ...
}
```

While a background task is running, you can also check on the status elsewhere using Ansible's `async_status` module, as long as you have the `ansible_job_id` value to pass in as `jid`:

```
$ ansible multi -m async_status -a "jid=763350539037"
```

Fire-and-forget tasks

You may also need to run occasional long-running maintenance scripts, or other tasks that take many minutes or hours to complete, and you'd rather not babysit the task. In these cases, you can set the `-B` value as high as you want (be generous, so your task will complete before Ansible kills it!), and set `-P` to '0', so Ansible fires off the command then forgets about it:

```
$ ansible multi -B 3600 -P 0 -a "/path/to/fire-and-forget-script.sh"
background launch...
```

```
192.168.60.5 | success >> {
    "ansible_job_id": "204960925196",
    "results_file": "/root/.ansible_async/204960925196",
    "started": 1
}
...
... [other hosts] ...
$
```

You won't be able to track progress using the `jid` anymore, but it's helpful for 'fire-and-forget' tasks.



For tasks you don't track remotely, it's usually a good idea to log the progress of the task *somewhere* and also send some sort of alert on failure—especially, for example, when running backgrounded tasks that perform backup operations, or when running business-critical database maintenance tasks.

You can also run tasks in Ansible playbooks in the background, asynchronously, by defining an `async` and `poll` parameter on the play. We'll discuss playbook task backgrounding more in later chapters.

Check log files

Sometimes, when debugging application errors, or diagnosing outages or other problems, you need to check server log files. Any common log file operation (like using `tail`, `cat`, `grep`, etc.) works through the `ansible` command, with a few caveats:

1. Operations that continuously monitor a file, like `tail -f`, won't work via Ansible, because Ansible only displays output after the operation is complete, and you won't be able to send the Control-C command to stop following the file. Someday, the `async` module might have this feature, but for now, it's not possible.
2. It's not a good idea to run a command that returns a huge amount of data via `stdout` via Ansible. If you're going to `cat` a file larger than a few KB, you should probably log into the server(s) individually.
3. If you redirect and filter output from a command run via Ansible, you need to use the `shell` module instead of Ansible's default `command` module (add `-m shell` to your commands).

As a simple example, let's view the last few lines of the messages log file on each of our servers:

```
$ ansible multi -s -a "tail /var/log/messages"
```

As stated in the caveats, if you want to filter the messages log with something like `grep`, you can't use Ansible's default `command` module, but instead, `shell`:

```
$ ansible multi -s -m shell -a "tail /var/log/messages | \
grep ansible-command | wc -l"

192.168.60.5 | success | rc=0 >>
12

192.168.60.4 | success | rc=0 >>
12

192.168.60.6 | success | rc=0 >>
14
```

This command shows how many ansible commands have been run on each server (the numbers you get may be different).

Manage cron jobs

Periodic tasks run via cron are managed by a system's crontab. Normally, to change cron job settings on a server, you would log into the server, use `crontab -e` under the account where the cron jobs reside, and type in an entry with the interval and job.

Ansible makes managing cron jobs easy with its `cron` module. If you want to run a shell script on all the servers every day at 4 a.m., add the cron job with:

```
$ ansible multi -s -m cron -a "name='daily-cron-all-servers' \
hour=4 job='/path/to/daily-script.sh'"
```

Ansible will assume * for all values you don't specify (valid values are `day`, `hour`, `minute`, `month`, and `weekday`). You could also specify special time values like `reboot`, `yearly`, or `monthly` using `special_time=[value]`. You can also set the user the job will run under via `user=[user]`, and create a backup of the current crontab by passing `backup=yes`.

What if we want to remove the cron job? Simple enough, use the same `cron` command, and pass the name of the cron job you want to delete, and `state=absent`:

```
$ ansible multi -s -m cron -a "name='daily-cron-all-servers' state=absent"
```

You can also use Ansible to manage custom crontab files; use the same syntax as you used earlier, but specify the location to the cron file with: `cron_file=cron_file_name` (where `cron_file_name` is a cron file located in `/etc/cron.d`).



Ansible denotes Ansible-managed crontab entries by adding a comment on the line above the entry like `#Ansible: daily-cron-all-servers`. It's best to leave things be in the crontab itself, and always manage entries via ad-hoc commands or playbooks using Ansible's `cron` module.

Deploy a version-controlled application

For simple application deployments, where you may need to update a git checkout, or copy a new bit of code to a group of servers, then run a command to finish the deployment, Ansible's ad-hoc mode can help. For more complicated deployments, use Ansible playbooks and rolling update features (which will be discussed in later chapters) to ensure successful deployments with zero downtime.

In the example below, I'll assume we're running a simple application on one or two servers, in the directory `/opt/myapp`. This directory is a git repository cloned from a central server or a service like GitHub, and application deployments and updates are done by updating the clone, then running a shell script at `/opt/myapp/scripts/update.sh`.

First, update the git checkout to the application's new version branch, 1.2.4, on all the app servers:

```
$ ansible app -s -m git -a "repo=git://example.com/path/to/repo.git \
dest=/opt/myapp update=yes version=1.2.4"
```

Ansible's git module lets you specify a branch, tag, or even a specific commit with the `version` parameter (in this case, we chose to checkout tag 1.2.4, but if you run the command again with a branch name, like `prod`, Ansible will happily do that instead). To force Ansible to update the checked-out copy, we passed in `update=yes`. The `repo` and `dest` options should be self-explanatory.

Then, run the application's `update.sh` shell script:

```
$ ansible app -s -a "/opt/myapp/update.sh"
```

Ad-hoc commands are fine for the simple deployments (like our example above), but you should use Ansible's more powerful and flexible application deployment features described later in this book if you have complex application or infrastructure needs. See especially the 'Rolling Updates' section later in this book.

Ansible's SSH connection history

One of Ansible's greatest features is its ability to function without running any extra applications or daemons on the servers it manages. Instead of using a proprietary protocol to communicate with

the servers, Ansible uses the standard and secure SSH connection that is commonly used for basic administration on almost every Linux server running today.

Since a stable, fast, and secure SSH connection is the heart of Ansible's communication abilities, Ansible's implementation of SSH has continually improved throughout the past few years—and is still improving today.

One thing that is universal to all of Ansible's SSH connection methods is that Ansible uses the connection to transfer one or a few files defining a play or command to the remote server, then runs the play/command, then deletes the transferred file(s), and reports back the results. This sequence of events may change and become more simple/direct with later versions of Ansible (see the notes on Ansible 1.5 below), but a fast, stable, and secure SSH connection is of paramount importance to Ansible.

Paramiko

In the beginning, Ansible used paramiko—an open source SSH2 implementation for Python—exclusively. However, as a single library for a single language (Python), development of paramiko doesn't keep pace with development of OpenSSH (the standard implementation of SSH used almost everywhere), and its performance and security is slightly worse than OpenSSH—at least to this writer's eyes.

Ansible continues to support the use of paramiko, and even chooses it as the default for systems (like RHEL 5/6) which don't support ControlPersist—an option present only in OpenSSH 5.6 or newer. (ControlPersist allows SSH connections to persist so frequent commands run over SSH don't have to go through the initial handshake over and over again until the ControlPersist timeout set in the server's SSH config is reached.)

OpenSSH (default)

Beginning in Ansible 1.3, Ansible defaulted to using native OpenSSH connections to connect to servers supporting ControlPersist. Ansible had this ability since version 0.5, but didn't default to it until 1.3.

Most local SSH configuration parameters (like hosts, key files, etc.) are respected, but if you need to connect via a port other than port 22 (the default SSH port), you need to specify the port in an inventory file (`ansible_ssh_port` option) or when running `ansible` commands.

OpenSSH is faster, and a little more reliable, than paramiko, but there are ways to make Ansible faster still.

Accelerated Mode

While not too helpful for ad-hoc commands, Ansible's Accelerated mode achieves greater performance for playbooks. Instead of connecting repeatedly via SSH, Ansible connects via SSH initially,

then uses the AES key used in the initial connection to communicate further commands and transfers via a separate port (5099 by default, but this is configurable).

The only extra package required to use accelerated mode is `python-keyczar`, and almost everything in normal OpenSSH/Paramiko mode works in Accelerated mode, with two exceptions when using `sudo`:

- Your sudoers file needs to have `requiretty` disabled (comment out the line with it, or set it per user by changing the line to `Defaults:username !requiretty`).
- You must disable sudo passwords by setting `NOPASSWD` in the sudoers file.

Accelerated mode can offer 2-4 times faster performance (especially for things like file transfers) compared to OpenSSH, and you can enable it for a playbook by adding the option `accelerate: true` to your playbook, like so:

```
---
- hosts: all
  accelerate: true
  ...
```

It goes without saying, if you use accelerated mode, you need to have the port through which it communicates open in your firewall (port 5099 by default, or whatever port you set with the `accelerate_port` option after `accelerate`).

Accelerate mode is a spiritual descendant of the now-deprecated ‘Fireball’ mode, which used a similar method for accelerating Ansible communications, but required ZeroMQ to be installed on the controlled server (which is at odds with Ansible’s simple no-dependency, no-daemon philosophy), and didn’t work with sudo commands at all.

Faster OpenSSH in Ansible 1.5+

Ansible 1.5 and later contains a very nice improvement to Ansible’s default OpenSSH implementation.

Instead of copying files, running them on the remote server, then removing them, the new method of OpenSSH transfer will send and execute commands for most Ansible modules directly over the SSH connection.

This method of connection is only available in Ansible 1.5+, and it can be enabled by adding `pipelining=True` under the `[ssh_connection]` section of the Ansible configuration file (`ansible.cfg`, which will be covered in more detail later).



The `pipelining=True` configuration option won’t help much unless you have removed or commented the `Defaults requiretty` option in `/etc/sudoers`. This is commented out in the default configuration for most OSes, but you might want to double-check this setting to make sure you’re getting the fastest connection possible!



If you're running a recent version of Mac OS X, Ubuntu, Windows with Cygwin, or most other OS for the host from which you run `ansible` and `ansible-playbook`, you should be running OpenSSH version 5.6 or later, which works perfectly with the `ControlPersist` setting used with all of Ansible's SSH connections settings.

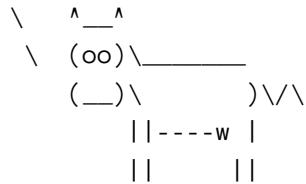
If the host on which Ansible runs has RHEL or CentOS, however, you might need to update your version of OpenSSH so it supports the faster/persistent connection method. Any OpenSSH version 5.6 or greater should work. To install a later version, either compile from source, or use a different repository (like [CentALT⁵¹](#) and `yum update openssh`.

Summary

In this chapter, you learned how to build a multi-server infrastructure for testing on your local workstation using Vagrant, and you configured, monitored, and managed the infrastructure without ever logging in to an individual server. You also learned how Ansible connects to remote servers, and how to use the `ansible` command to perform tasks on many servers quickly in parallel, or one by one.

By now, you should be getting familiar with the basics of Ansible, and you should be able to start managing your own infrastructure more efficiently.

```
/ It's easier to seek forgiveness than \
\ ask for permission. (Proverb)      /
```



⁵¹<http://mirror.neu.edu.cn/CentALT/readme.txt>

Chapter 4 - Ansible Playbooks

Power plays

Like many other configuration management solutions, Ansible uses a metaphor to describe its configuration files. They are called ‘playbooks’, and they list a set of tasks (‘plays’ in Ansible parlance) that will be run against a particular server or set of servers. In American football, a team follows a set of pre-written playbooks as the basis for a bunch of plays they execute to try to win a game. In Ansible, you write playbooks (a list of instructions describing the steps to bring your server to a certain configuration state) that are then *played* on your servers.

Playbooks are written in [YAML⁵²](#), a simple human-readable syntax popular for defining configuration. Playbooks may be included within other playbooks, and certain metadata and options cause different plays or playbooks to be run in different scenarios on different servers.

Ad-hoc commands alone make Ansible a powerful tool; playbooks turn Ansible into a top-notch server provisioning and configuration management tool.

What attracts most DevOps personnel to Ansible is the fact that it is easy to convert shell scripts (or one-off shell commands) directly into Ansible plays. Consider the following script, which installs Apache on a RHEL/CentOS server:

Shell Script

```
1 # Install Apache.
2 yum install --quiet -y httpd httpd-devel
3 # Copy configuration files.
4 cp /path/to/config/httpd.conf /etc/httpd/conf/httpd.conf
5 cp /path/to/config/httpd-vhosts.conf /etc/httpd/conf/httpd-vhosts.conf
6 # Start Apache and configure it to run at boot.
7 service httpd start
8 chkconfig httpd on
```

To run the shell script (in this case, a file named `shell-script.sh` with the contents as above), you would call it directly from the command line:

⁵²<http://docs.ansible.com/YAMLSyntax.html>

```
# (From the same directory in which the shell script resides).
$ ./shell-script.sh
```

Ansible Playbook

```
1  ---
2  - hosts: all
3    tasks:
4      - name: Install Apache.
5        command: yum install --quiet -y httpd httpd-devel
6      - name: Copy configuration files.
7        command: >
8          cp /path/to/config/httpd.conf /etc/httpd/conf/httpd.conf
9      - command: >
10        cp /path/to/config/httpd-vhosts.conf /etc/httpd/conf/httpd-vhosts.conf
11      - name: Start Apache and configure it to run at boot.
12        command: service httpd start
13      - command: chkconfig httpd on
```

To run the Ansible Playbook (in this case, a file named `playbook.yml` with the contents as above), you would call it using the `ansible-playbook` command:

```
# (From the same directory in which the playbook resides).
$ ansible-playbook playbook.yml
```

Ansible is powerful in that you quickly transition to using playbooks if you know how to write standard shell commands—the same commands you’ve been using for years—and then as you get time, rebuild your configuration to take advantage of Ansible’s helpful features.

In the above playbook, we use Ansible’s `command` module to run standard shell commands. We’re also giving each play a ‘name’, so when we run the playbook, the play has human-readable output on the screen or in the logs. The `command` module has some other tricks up its sleeve (which we’ll see later), but for now, be assured shell scripts are translated directly into Ansible playbooks without much hassle.



The greater-than sign (>) immediately following the command: module directive tells YAML “automatically quote the next set of indented lines as one long string, with each line separated by a space”. It helps improve task readability in some cases. There are different ways of describing configuration using valid YAML syntax, and these methods are discussed in-depth in the [YAML Conventions and Best Practices](#) section in Appendix B.

This book uses three different task-formatting techniques: For tasks which require one or two simple parameters, Ansible’s shorthand syntax (e.g. yum: name=apache2 state=installed) is used. For most uses of command or shell, where longer commands are entered, the > technique mentioned above is used. For tasks which require many parameters, YAML object notation is used—placing each key and variable on its own line. This assists with readability and allows for version control systems to easily distinguish changes line-by-line.

The above playbook will perform *exactly* like the shell script, but you can improve things greatly by using some of Ansible’s built-in modules to handle the heavy lifting:

Revised Ansible Playbook - Now with idempotence!

```
1  ---
2  - hosts: all
3    sudo: yes
4    tasks:
5      - name: Install Apache.
6        yum: name={{ item }} state=present
7        with_items:
8          - httpd
9          - httpd-devel
10     - name: Copy configuration files.
11       copy:
12         src: "{{ item.src }}"
13         dest: "{{ item.dest }}"
14         owner: root
15         group: root
16         mode: 0644
17       with_items:
18         - {
19           src: "/path/to/config/httpd.conf",
20           dest: "/etc/httpd/conf/httpd.conf"
21         }
22         - {
23           src: "/path/to/config/httpd-vhosts.conf",
24           dest: "/etc/httpd/conf/httpd-vhosts.conf"
```

```

25      }
26      - name: Make sure Apache is started and configure it to run at boot.
27          service: name=httpd state=started enabled=yes

```

Now we're getting somewhere. Let me walk you through this simple playbook:

1. The first line, ----, is how we mark this document as using YAML syntax (like using <html> at the top of an HTML document, or <?php at the top of a block of PHP code).
2. The second line, - hosts: all defines the first (and in this case, only) **play**, and tells Ansible to run the play on all hosts that it knows about.
3. The third line, sudo: yes tells Ansible to run all the commands through sudo, so the commands will be run as the root user.
4. The fourth line, tasks:, tells Ansible that what follows is a list of tasks to run as part of this playbook.
5. The first task begins with name: Install Apache.. name is not a module that does something to your server; rather, it's a way of giving a human-readable description to the play that follows. Seeing "Install Apache" is more relevant than seeing "yum name=httpd state=installed"... but if you drop the name line completely, that won't cause any problem.
 - We use the yum module to install Apache. Instead of the command `yum -y install httpd httpd-devel`, we can describe to Ansible exactly what we want. Ansible will take the items array we pass in `({{ variable }})` references a variable in Ansible's playbooks). We tell yum to make sure the packages we define are installed with state=present, but we could also use state=latest to ensure the latest version is installed, or state=absent to make sure the package is **not** installed.
 - Ansible allows simple lists to be passed into tasks using `with_items:` Define a list of items below, and each line will be passed into the play, one by one. In this case, each of the items will be substituted for the `{{ item }}` variable.
6. The second task again starts with a human-readable name (which could be left out if you'd like).
 - We use the copy module to copy files from a source (on our local workstation) to a destination (the server being managed). We could also pass in more variables, like file metadata including ownership and permissions (owner, group, and mode).
 - In this case, we are using an array with multiple elements for variable substitution; you use the syntax `{var1: value, var2: value}` to define each element (it can have as many variables as you want within, or even nested levels of variables!). When you reference the variables in the play, you use a dot to access the variable within the item, so `{{ item.var1 }}` would access the first variable. In our example, `item.src` accesses the `src` in each item.
7. The third task also uses a name to describe it in a human-readable format.
 - We use the service module to describe the desired state of a particular service, in this case httpd, Apache's http daemon. We want it to be running, so we set state=started, and we want it to run at system startup, so we say enabled=yes (the equivalent of running `chkconfig httpd on`).

The great thing about the way we've reformatted this list of commands is that Ansible keeps track of the state of everything on all our servers. If you run the playbook the first time, it will provision the server by ensuring Apache is installed and running, and your custom configuration is in place.

Even better, the **second** time you run it (if the server is in the correct state), it won't actually do anything besides tell you nothing has changed. So, with this one short playbook, you're able to provision and ensure the proper configuration for an Apache web server. Additionally, running the playbook with the `--check` option (see the next section below) verifies the configuration matches what's defined in the playbook, without actually running the tasks on the server.

If you ever want to update your configuration, or install another httpd package, either update the file locally or add the package to the `with_items` list and run the playbook again. Whether you have one or a thousand servers, all of their configurations will be updated to match your playbook—and Ansible will tell you if anything ever changes (you're not making ad-hoc changes on individual production servers, **are you?**).

Running Playbooks with `ansible-playbook`

If we run the playbooks in the examples above (which are set to run on `all` hosts), then the playbook would be run against every host defined in your Ansible inventory file (see Chapter 1's [basic inventory file example](#)).

Limiting playbooks to particular hosts and groups

You can limit a playbook to specific groups or individual hosts by changing the `hosts:` definition. The value can be set to `all` hosts, a group of hosts defined in your inventory, multiple groups of hosts (e.g. `webservers, dbservers`), individual hosts (e.g. `at1.example.com`), or a mixture of hosts. You can even do wildcard matches, like `*.example.com`, to match all subdomains of a top-level domain.

You can also limit the hosts on which the playbook is run via the `ansible-playbook` command:

```
$ ansible-playbook playbook.yml --limit webservers
```

In this case (assuming your inventory file contains a `webservers` group), even if the playbook is set to `hosts: all`, or includes hosts in addition to what's defined in the `webservers` group, it will only be run on the hosts defined in `webservers`.

You could also limit the playbook to one particular host:

```
$ ansible-playbook playbook.yml --limit xyz.example.com
```

If you want to see a list of hosts that would be affected by your playbook before you actually run it, use `--list-hosts`:

```
$ ansible-playbook playbook.yml --list-hosts
```

Running this should give output like:

```
playbook: playbook.yml

play #1 (all): host count=4
  127.0.0.1
  192.168.24.2
  foo.example.com
  bar.example.com
```

(Where count is the count of servers defined in your inventory, and following is a list of all the hosts defined in your inventory).

Setting user and sudo options with ansible-playbook

If no user is defined alongside the hosts in a playbook, Ansible assumes you'll connect as the user defined in your inventory file for a particular host, and then will fall back to your local user account name. You can explicitly define a remote user to use for remote plays using the --remote-user (-u) option:

```
$ ansible-playbook playbook.yml --remote-user=johndoe
```

In some situations, you will need to pass along your sudo password to the remote server to perform commands via sudo. In these situations, you'll need use the --ask-sudo-pass (-K) option. You can also explicitly force all tasks in a playbook to use sudo with --sudo. Finally, you can define the sudo user for tasks run via sudo (the default is root) with the --sudo-user (-U) option.

For example, the following command will run our example playbook with sudo, performing the tasks as the sudo user janedoe, and Ansible will prompt you for the sudo password:

```
$ ansible-playbook playbook.yml --sudo --sudo-user=janedoe --ask-sudo-pass
```

If you're not using key-based authentication to connect to your servers (read my warning about the security implications of doing so in Chapter 1), you can use --ask-pass.

Other options for ansible-playbook

The `ansible-playbook` command also allows for some other common options:

- `--inventory=PATH (-i PATH)`: Define a custom inventory file (default is the default Ansible inventory file, usually located at `/etc/ansible/hosts`).
- `--verbose (-v)`: Verbose mode (show all output, including output from successful options). You can pass in `-vvvv` to give every minute detail.
- `--extra-vars=VARS (-e VARS)`: Define variables to be used in the playbook, in "key=value, key=value" format.
- `--forks=NUM (-f NUM)`: Number for forks (integer). Set this to a number higher than 5 to increase the number of servers on which Ansible will run tasks concurrently.
- `--connection=TYPE (-c TYPE)`: The type of connection which will be used (this defaults to `ssh`; you might sometimes want to use `local` to run a playbook on your local machine, or on a remote server via cron).
- `--check`: Run the playbook in Check Mode ('Dry Run'); all tasks defined in the playbook will be checked against all hosts, but none will actually be run.

There are some other options and configuration variables that are important to get the most out of `ansible-playbook`, but this should be enough to get you started running the playbooks in this chapter on your own servers or virtual machines.



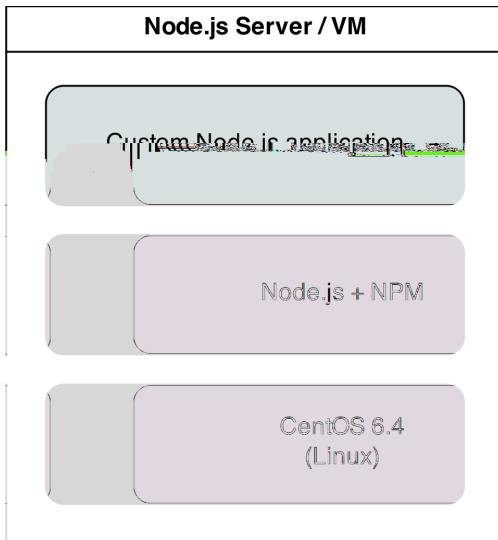
The rest of this chapter uses more realistic Ansible playbooks. All the examples in this chapter are in the [Ansible for DevOps GitHub repository](#)⁵³, and you can clone that repository to your computer (or browse the code online) to follow along more easily.

Real-world playbook: CentOS Node.js app server

The first example, while being helpful for someone who might want to post a simple static web page to a clunky old Apache server, is not a good representation of a real-world scenario. I'm going to run through some more complex playbooks that do many different things, most of which are actually being used to manage production infrastructure today.

The first playbook will configure a CentOS server with Node.js, and install and start a simple Node.js application. The server will have a very simple architecture:

⁵³<https://github.com/geerlingguy/ansible-for-devops>



Node.js app on CentOS.

To start things off, we need to create a YAML file (`playbook.yml` in this example) to contain our playbook. Let's keep things simple:

```
1  ---
2  - hosts: all
3
4  tasks:
```

First, define a set of hosts (`all`) on which this playbook will be run (see the section above about limiting the playbook to particular groups and hosts), then tell ansible that what follows will be a list of tasks to run on the hosts.

Add extra repositories

Adding extra package repositories (yum or apt) is one thing many admins will do before any other work on a server to ensure that certain packages are available, or are at a later version than the ones in the base installation.

In the shell script below, we want to add both the EPEL and Remi repositories, so we can get some packages like Node.js or later versions of other necessary software (these examples presume you're running RHEL/CentOS 6.x):

```
1 # Import EPEL GPG Key - see: https://fedoraproject.org/keys
2 wget https://fedoraproject.org/static/0608B895.txt \
3     -O /etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-6
4 rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-6
5
6 # Import Remi GPG key - see: http://rpms.famillecollet.com/RPM-GPG-KEY-remi
7 wget http://rpms.famillecollet.com/RPM-GPG-KEY-remi \
8     -O /etc/pki/rpm-gpg/RPM-GPG-KEY-remi
9 rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY-remi
10
11 # Install EPEL and Remi repos.
12 rpm -Uvh --quiet \
13     http://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm
14 rpm -Uvh --quiet \
15     http://rpms.famillecollet.com/enterprise/remi-release-6.rpm
16
17 # Install Node.js (npm plus all its dependencies).
18 yum --enablerepo=epel install node
```

This shell script uses the rpm command to import the EPEL and Remi repository GPG keys, then adds the repositories, and finally installs Node.js. It works okay for a simple deployment (or by hand), but it's silly to run all these commands (some of which could take time or stop your script entirely if your connection is flaky or bad) if the result has already been achieved (namely, two repositories and their GPG keys have been added).



If you wanted to skip a couple steps, you could skip adding the GPG keys, and just run your commands with `--nogpgcheck` (or, in Ansible, set the `disable_gpg_check` parameter of the `yum` module to `yes`), but it's a good idea to leave this enabled. GPG stands for **GNUPrivacy Guard**, and it's a way that developers and package distributors can sign their packages (so you know it's from the original author, and hasn't been modified or corrupted). Unless you **really** know what you're doing, don't disable security settings like GPG key checks.

Ansible makes things a little more robust. Even though the following is slightly more verbose, it performs the same actions in a more structured way, which is simpler to understand, and works with variables other nifty Ansible features we'll discuss later:

```

5  - name: Import EPEL and Remi GPG keys.
6    rpm_key: "key={{ item }} state=present"
7    with_items:
8      - "https://fedoraproject.org/static/0608B895.txt"
9      - "http://rpms.famillecollet.com/RPM-GPG-KEY-remi"
10
11 - name: Install EPEL and Remi repos.
12   command: "rpm -Uvh --force {{ item.href }} creates={{ itemcreates }}"
13   with_items:
14     -
15       href: "http://download.fedoraproject.org/pub/epel/6/i386/epel-release-6-8.no\
16 arch.rpm",
17       creates: "/etc/yum.repos.d/epel.repo"
18     }
19     -
20       href: "http://rpms.famillecollet.com/enterprise/remi-release-6.rpm",
21       creates: "/etc/yum.repos.d/remi.repo"
22     }
23
24 - name: Disable firewall (since this is a dev environment).
25   service: name=iptables state=stopped enabled=no
26
27 - name: Install Node.js and npm.
28   yum: name=npn state=present enablerepo=epel
29
30 - name: Install Forever (to run our Node.js app).
31   npm: name=forever global=yes state=latest

```

Let's walk through this playbook step-by-step:

1. `rpm_key` is a very simple Ansible module that takes and imports an RPM key from a URL or file, or the key id of a key that is already present, and ensures the key is either present or absent (the `state` parameter). We want to import two keys—one for EPEL from the Fedora project, and one for the Remi Repository.
2. Since Ansible doesn't have a built-in `rpm` module, we use the `rpm` command, but we use Ansible's `command` module, which allows us to do two things:
 1. Use the `creates` parameter to tell Ansible when to *not* run the command (in this case, we tell Ansible what file is present after the `rpm` command successfully completes).
 2. Use a multidimensional array of items (`with_items`) to define URLs and the resulting files checked with `creates`.
3. `yum` installs Node.js (along with all the required packages for `npm`, Node's package manager) if it's not present, and allows the EPEL repo to be searched via the `enablerepo` parameter (you could also explicitly *disable* a repository using `disablerepo`).

4. Since NPM is now installed, we use Ansible's `npm` module to install a Node.js utility, `forever` to launch our app and keep it running. Setting `global` to `yes` tells NPM to install the `forever` node module in `/usr/lib/node_modules/` so it will be available to all users and Node.js apps on the system.

We're beginning to have a nice little Node.js app server set up. Let's set up a little Node.js app that responds to HTTP requests on port 80.

Deploy a Node.js app

The next step is to install a simple Node.js app on our server. First, we'll create a really simple Node.js app by creating a new folder, `app`, in the same folder as your `playbook.yml`. Create a new file, `app.js`, in this folder, with the following contents:

```
1 // Load the express module.
2 var express = require('express'),
3 app = express.createServer();
4
5 // Respond to requests for / with 'Hello World'.
6 app.get('/', function(req, res){
7     res.send('Hello World!');
8 });
9
10 // Listen on port 80 (like a true web server).
11 app.listen(80);
12 console.log('Express server started successfully.');
```

Don't worry about the syntax or the fact that this is Node.js. We just need a quick example to deploy. This example could've been written in Python, Perl, Java, PHP, or another language, but since Node is a very simple language (JavaScript) that runs in a very simple and lightweight environment, it's a nice (and easy) language to use when testing things or prodding your server.

Since this little app is dependent on Express (a simple http framework for Node), we also need to tell NPM about this dependency via a `package.json` file in the same folder as `app.js`:

```

1  {
2    "name": "exemplenodeapp",
3    "description": "Example Express Node.js app.",
4    "author": "Jeff Geerling <geerlingguy@mac.com>",
5    "dependencies": {
6      "express": "3.x.x"
7    },
8    "engine": "node >= 0.10.6"
9  }

```

Now, add the following to your playbook, to copy the entire app to the server, and then have NPM download the required dependencies (in this case, express):

```

32  - name: Ensure Node.js app folder exists.
33    file: "path={{ node_apps_location }} state=directory"
34
35  - name: Copy example Node.js app to server.
36    copy: "src=app dest={{ node_apps_location }}"
37
38  - name: Install app dependencies defined in package.json.
39    npm: path={{ node_apps_location }}/app

```

First, we ensure the directory where our app will be installed exists, using the `file` module. The `{{ node_apps_location }}` variable used in each command can be defined under a `vars` section at the top of our playbook, in your inventory, or on the command line when calling `ansible-playbook`.

Second, we copy the entire app folder up to the server, using Ansible's `copy` command, which intelligently distinguishes between a single file or a directory of files, and recurses through the directory, similar to recursive `scp` or `rsync`.



Ansible's `copy` module works very well for single or small groups of files, and recurses through directories automatically. If you are copying hundreds of files, or deeply-nested directory structures, `copy` will get bogged down. In these situations, consider using the `synchronize` module if you need to copy a full directory, or `unarchive` if you want to copy up an archive and have it expanded in place on the server.

Third, we use `npm` again, this time, with no extra arguments besides the path to the app. This tells NPM to parse the `package.json` file and ensure all the dependencies are present.

We're *almost* finished! The last step is to start the app.

Launch a Node.js app

We'll now use `forever` (which we installed earlier) to start the app.

```

40 - name: Check list of running Node.js apps.
41   command: forever list
42   register: forever_list
43   changed_when: false
44
45 - name: Start example Node.js app.
46   command: "forever start {{ node_apps_location }}/app/app.js"
47   when: "forever_list.stdout.find('{{ node_apps_location }}/app/app.js') == -1"

```

In the first play, we’re doing two new things:

1. `register` creates a new variable, `forever_list`, to be used in the next play to determine when to run the play. `register` stashes the output (stdout, stderr) of the defined command in the variable name passed to it.
2. `changed_when` tells Ansible explicitly when this play results in a change to the server. In this case, we know the `forever list` command will never change the server, so we just say `false`—the server will never be changed when the command is run.

The second play actually starts the app, using Forever. We could also start the app by calling `node {{ node_apps_location }}/app/app.js`, but we would not be able to control the process easily, and we would also need to use `nohup` and `&` to avoid Ansible hanging on this play.

Forever tracks the Node apps it manages, and we use Forever’s `list` option to print a list of running apps. The first time we run this playbook, the list will obviously be empty—but on future runs, if the app is running, we don’t want to start another instance of it. To avoid that situation, we tell Ansible when we want to start the app with `when`. Specifically, we tell Ansible to start the app only when the app’s path in *not* in the `forever list` output.

Node.js app server summary

At this point, you have a complete playbook that will install a simple Node.js app which responds to HTTP requests on port 80 with “Hello World!”.

To run the playbook on a server (in our case, we could just set up a new VirtualBox VM for testing, either via Vagrant or manually), use the following command (pass in the `node_apps_location` variable via the command):

```
$ ansible-playbook playbook.yml \
--extra-vars="node_apps_location=/usr/local/opt/node"
```

Once the playbook has finished configuring the server and deploying your app, visit `http://hostname/` in a browser (or use `curl` or `wget` to request the site), and you should see the following:



Node.js Application home page.

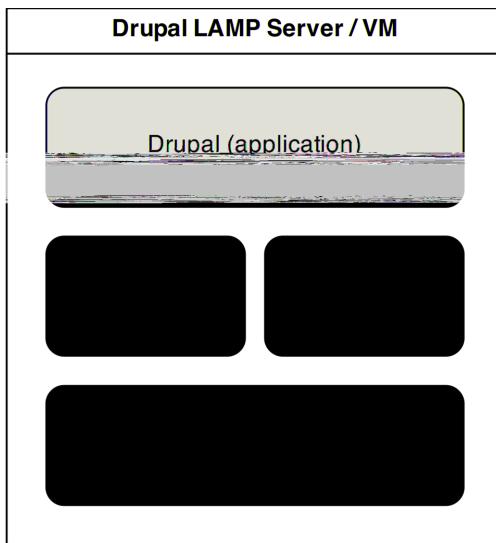
Simple, but very powerful. We've configured an entire Node.js application server In fewer than fifty lines of YAML!



The entire example Node.js app server playbook is in this book's code repository at <https://github.com/geerlingguy/ansible-for-devops⁵⁴>, in the nodejs directory.

Real-world playbook: Ubuntu LAMP server with Drupal

At this point, you should be getting comfortable with Ansible playbooks and the YAML syntax used to define them. Up to this point, most examples have assumed you're working with a CentOS, RHEL, or Fedora server. Ansible plays nicely with other flavors of Linux and BSD-like systems as well. In the following example, we're going to set up a traditional LAMP (Linux, Apache, MySQL, and PHP) server using Ubuntu 12.04 to run a Drupal website.



Drupal LAMP server.

Include a variables file, and discover pre_tasks and handlers

For this playbook, we're going to start organizing our playbook a little more efficiently. Instead of defining any requiring variables be passed in via the command line, let's begin the playbook by telling Ansible our variables are stored in a separate `vars.yml` file:

⁵⁴<https://github.com/geerlingguy/ansible-for-devops>

```

1 - hosts: all
2
3 vars_files:
4   - vars.yml

```

Using one or more included variable files cleans up your main playbook file, and lets you organize all your configurable variables in one place. At the moment, we don't have any variables to add; we'll define the contents of `vars.yml` later. For now, create the empty file, and continue on to the next section of the playbook, `pre_tasks`:

```

5 pre_tasks:
6   - name: Update apt cache if needed.
7     apt: update_cache=yes cache_valid_time=3600

```

Ansible lets you run tasks before or after the main set of tasks using `pre_tasks` and `post_tasks`. In this case, we need to ensure that our apt cache is updated before we run the rest of the playbook, so we have the latest package versions on our server. We use Ansible's `apt` module and tell it to update the cache if it's been more than 3600 seconds (1 hour) since the last update.

With that out of the way, we'll add another new section to our playbook, `handlers`:

```

8 handlers:
9   - name: restart apache
10    service: name=apache2 state=restarted

```

`handlers` are special kinds of tasks you run at the end of a group of tasks by adding the `notify` option to any of the tasks in that group. The handler will only be called if one of the tasks notifying the handler makes a change to the server (and doesn't fail), and it will only be notified at the `end of` the group of tasks.

To call this handler, add the option `notify: restart apache` after defining the rest of a play. We've defined this handler so we can restart the `apache2` service after a configuration change, which will be explained below.



Just like variables, handlers and tasks may be placed in separate files and included in your playbook to keep things tidy (we'll discuss this in chapter 6). For simplicity's sake, though, the examples in this chapter are shown as in a single playbook file. We'll discuss different playbook organization methods later.



By default, Ansible will stop all playbook execution when a task fails, and won't even notify any handlers that may need to be triggered. In some cases, this leads to unintended side effects. If you want to make sure handlers always run after a task uses `notify` to call the handler, even in case of playbook failure, add `--force-handlers` to your `ansible-playbook` command.

Basic LAMP server setup

The first step towards building an application server that depends on the LAMP stack is to build the actual LAMP part of it. This is the simplest process, but still requires a little extra work for our particular server. We want to install Apache, MySQL and PHP, but we'll also need a couple other dependencies, and we want a particular version of PHP (5.5), which is only available in an extra apt repository.

```
11  tasks:
12  - name: Get software for apt repository management.
13    apt: name={{ item }} state=installed
14    with_items:
15      - python-apt
16      - python-pycurl
17
18  - name: Add ondrej repository for later versions of PHP.
19    apt_repository: repo='ppa:ondrej/php5' update_cache=yes
20
21  - name: "Install Apache, MySQL, PHP, and other dependencies."
22    apt: name={{ item }} state=installed
23    with_items:
24      - git
25      - curl
26      - sendmail
27      - apache2
28      - php5
29      - php5-common
30      - php5-mysql
31      - php5-cli
32      - php5-curl
33      - php5-gd
34      - php5-dev
35      - php5-mcrypt
36      - php-apc
37      - php-pear
38      - python-mysqldb
39      - mysql-server
40
41  - name: Disable the firewall (since this is for local dev only).
42    service: name=ufw state=stopped
43
44  - name: "Start Apache, MySQL, and PHP."
45    service: "name={{ item }} state=started enabled=yes"
```

```
46      with_items
47          - apache2
48          + mysql - _
```

In this playbook, I've decided to add a simple prefix to each named play, so I can more easily follow the playbook's progress when it's running. I've begun with the common LAMP setup:

1. Install a couple helper libraries which allow Python to manage apt more precisely (`python-apt` and `python-pycurl` are required for the `apt_repository` module to do its work).
2. Since the default apt repositories for Ubuntu 12.04 don't include PHP 5.4.x (or any later versions), install ondrej's `PHP5-oldstable` repository, containing PHP 5.4.25 (at the time of this writing) and other associated PHP packages.
3. Install all the required packages for our LAMP server (including all the `php5` extensions we need to run Drupal).
- 4.

```

63   - name: Symlink Drupal virtualhost to sites-enabled.
64     file:
65       src: "/etc/apache2/sites-available/{{ domain }}.dev.conf"
66       dest: "/etc/apache2/sites-enabled/{{ domain }}.dev.conf"
67       state: link
68     notify: restart apache
69
70   - name: Remove default virtualhost file.
71     file:
72       path: "/etc/apache2/sites-enabled/000-default"
73       state: absent
74     notify: restart apache

```

The first command enables all the required Apache modules by symlinking them from /etc/apache2/mods-available to /etc/apache2/mods-enabled.

The second command copies a Jinja2 template we define inside the templates folder to Apache's sites-available folder, with the correct owner and permissions. Additionally, we notify the restart apache handler, because copying in a new VirtualHost means Apache needs to be restarted to pick up the change.

Let's look at our Jinja2 template (denoted by the extra .j2 on the end of the filename), drupal.dev.conf.j2:

```

1 <VirtualHost *:80>
2   ServerAdmin webmaster@localhost
3   ServerName {{ domain }}.dev
4   ServerAlias www.{{ domain }}.dev
5   DocumentRoot {{ drupal_core_path }}
6   <Directory "{{ drupal_core_path }}">
7     Options FollowSymLinks Indexes
8     AllowOverride All
9   </Directory>
10  </VirtualHost>

```

This is a fairly standard Apache VirtualHost definition, but we have a few Jinja2 template variables mixed in. The syntax for printing a variable in a Jinja2 template is the same syntax we use in our Ansible playbooks—two brackets around the variable's name (like so: {{ variable }}).

There are three variables we will need (drupal_core_version, drupal_core_path, and domain), so add them to the empty vars.yml file we created earlier:

```

1  ---
2  # The core version you want to use (e.g. 6.x, 7.x, 8.0.x).
3  drupal_core_version: "8.0.x"
4
5  # The path where Drupal will be downloaded and installed.
6  drupal_core_path: "/var/www/drupal-{{ drupal_core_version }}-dev"
7
8  # The resulting domain will be [domain].dev (with .dev appended).
9  domain: "drupaltest"

```

Now, when Ansible reaches the play that copies this template into place, the Jinja2 template will have the variable names replaced with the values 8.0.x and drupaltest (or whatever values you'd like!).

The last two tasks (lines 12-19) enable the VirtualHost we just added, and remove the default VirtualHost definition, which we no longer need.

At this point, you could start the server, but Apache will likely throw an error since the VirtualHost you've defined doesn't yet exist (there's no directory at {{ drupal_core_path }} yet!). This is why using `notify` is important—instead of adding a play after these three steps to restart Apache (which will fail the first time you run the playbook), `notify` will wait until after we've finished all the other steps in our main group of tasks (giving us time to finish setting up the server), *then* restart Apache.

Configure PHP with `lineinfile`

We briefly mentioned `lineinfile` earlier in the book, when discussing file management and ad-hoc task execution. Modifying PHP's configuration is a perfect way to demonstrate `lineinfile`'s simplicity and usefulness:

```

74      - name: Enable upload progress via APC.
75        lineinfile:
76          dest: "/etc/php5/apache2/conf.d/20-apcu.ini"
77          regexp: "^apc.rfc1867"
78          line: "apc.rfc1867 = 1"
79          state: present
80        notify: restart apache

```

Ansible's `lineinfile` module does a simple task: ensures that a particular line of text exists (or doesn't exist) in a file.

In this example, we need to enable APC's `rfc1867` option so Drupal can use APC's file upload progress tracking (there are better ways of doing this, but for our simple server, this will suffice).

First, we tell `lineinfile` the location of the file, in the `dest` parameter. Then, we give a regular expression (Python-style) to define what the line looks like (in this case, the line starts with the

exact phrase “apc.rfc1867”—we had to escape the period since it is a special character in regular expressions). Next, we tell `lineinfile` exactly how the resulting line should look. Finally, we explicitly state that we want this line to be present (with the `state` parameter).

Ansible will take the regular expression, and see if there’s a matching line. If there is, Ansible will make sure the line matches the `line` parameter. If not, Ansible will add the line as defined in the `line` parameter. Ansible will only report a change if it had to add or change the line to match `line`.

Configure MySQL

The next step is to remove MySQL’s default test database, and create a database (named for the domain we specified earlier) for our Drupal installation to use.

```
80      - name: Remove the MySQL test database.  
81          mysql_db: db=test state=absent  
82  
83      - name: Create a database for Drupal.  
84          mysql_db: "db={{ domain }}" state=present"
```

MySQL installs a database named `test` by default, and it is recommended that you remove the database as part of MySQL’s included `mysql_secure_installation` tool. The first step in configuring MySQL is removing this database. Next, we create a database named `{{ domain }}`—the database is named the same as the domain we’re using for the Drupal site.



Ansible works with many databases out of the box (MongoDB, MySQL, PostgreSQL, Redis and Riak as of this writing). In MySQL’s case, Ansible uses the `MySQLdb` Python package (`python-mysqldb`) to manage a connection to the database server, and assumes the default root account credentials ('root' as the username with no password). Obviously, leaving this default would be a bad idea! On a production server, one of the first steps should be to change the root account password, limit the root account to localhost, and delete any nonessential database users.

If you use different credentials, you can add a `.my.cnf` file to your remote user’s home directory containing the database credentials to allow Ansible to connect to the MySQL database without leaving passwords in your Ansible playbooks or variable files. Otherwise, you can prompt the user running the Ansible playbook for a MySQL username and password. This option, using prompts, will be discussed later in the book.

Install Composer and Drush

Drupal has a command-line companion in the form of Drush. Drush is developed independently of Drupal, and provides a full suite of CLI commands to manage Drupal. Drush, like most modern

PHP tools, integrates with external dependencies defined in a `composer.json` file which describes the dependencies to Composer.

We could just download Drupal and perform some setup in the browser by hand at this point, but the goal of this playbook is to have a fully-automated and idempotent Drupal installation. So, we need to install Composer, then Drush:

```
85  - name: Install Composer into the current directory.  
86    shell: >  
87      curl -sS https://getcomposer.org/installer | php  
88      creates=/usr/local/bin/composer  
89  
90  - name: Move Composer into globally-accessible location.  
91    shell: >  
92      mv composer.phar /usr/local/bin/composer  
93      creates=/usr/local/bin/composer
```

The first command runs Composer's php-based installer, which generates a 'composer.phar' PHP application archive. This archive is then copied (using the `mv` shell command) to the location `/usr/local/bin/composer` so we can use the simple `composer` command to install all of Drush's dependencies. Both commands are set to run only if the `/usr/local/bin/composer` file doesn't already exist (using the `creates` parameter).



Why use `shell` instead of `command`? Ansible's `command` module is the preferred option for running commands on a host (when an Ansible module won't suffice), and it works in most scenarios. However, `command` doesn't run the command via the remote shell `/bin/sh`, so options like `<`, `>`, `|`, and `&`, and local environment variables like `$HOME` won't work. `shell` allows you to pipe command output to other commands, access the local environment, etc.

There are two other modules which assist in executing shell commands remotely: `script` executes shell scripts (though it's almost always a better idea to convert shell scripts into idempotent Ansible playbooks!), and `raw` executes raw commands via SSH (it should only be used in circumstances where you can't use one of the other options).

It's best to use an Ansible module for every task. If you have to resort to a regular command-line command, try the `command` module first. If you require the options mentioned above, use `shell`. Use of `script` or `raw` should be exceedingly rare, and won't be covered in this book.

Now, we'll install Drush using the latest version from GitHub:

```
94      - name: Check out drush master branch.  
95          git:  
96              repo: https://github.com/drush-ops/drush.git  
97              dest: /opt/drush  
98  
99      - name: Install Drush dependencies with Composer.  
100         shell: >  
101             /usr/local/bin/composer install  
102             chdir=/opt/drush  
103             creates=/opt/drush/vendor/autoload.php  
104  
105     - name: Create drush bin symlink.  
106         file:  
107             src: /opt/drush/drush  
108             dest: /usr/local/bin/drush  
109             state: link
```

Earlier in the book, we cloned a git repository using an ad-hoc command. In this case, we're defining a play that uses the `git` module to clone Drush from its repository URL on GitHub. Since we want the master branch, pass in the `repo` (repository URL) and `dest` (destination path) parameters.

After drush is downloaded to `/opt/drush`, we use Composer to install all the required dependencies. In this case, we want Ansible to run `composer install` in the directory `/opt/drush` (this is so Composer finds drush's `composer.json` file automatically), so we pass along the parameter `chdir=/opt/drush`. Once Composer is finished, the file `/opt/drush/vendor/autoload.php` will be created, so we use the `creates` parameter to tell Ansible to skip this step if the file already exists (for idempotency).

Finally, we create a symlink from `/usr/local/bin/drush` to the executable at `/opt/drush/drush`, so we can call the `drush` command anywhere on the system.

Install Drupal with Git and Drush

We'll use `git` again to clone Drupal to the apache document root we defined earlier in our virtual host configuration, then we'll run Drupal's installation via drush, and fix a couple other file permissions issues so Drupal loads correctly within our VM.

```

108  - name: Check out Drupal Core to the Apache docroot.
109    git:
110      repo: http://git.drupal.org/project/drupal.git
111      version: "{{ drupal_core_version }}"
112      dest: "{{ drupal_core_path }}"
113
114  - name: Install Drupal.
115    command: >
116      drush si -y --site-name="{{ drupal_site_name }}" --account-name=admin
117      --account-pass=admin --db-url=mysql://root@localhost/{{ domain }}
118      chdir={{ drupal_core_path }}
119      creates={{ drupal_core_path }}/sites/default/settings.php
120    notify: restart apache
121
122  # SEE: https://drupal.org/node/2121849#comment-8413637
123  - name: Set permissions properly on settings.php.
124    file:
125      path: "{{ drupal_core_path }}/sites/default/settings.php"
126      mode: 0744
127
128  - name: Set permissions on files directory.
129    file:
130      path: "{{ drupal_core_path }}/sites/default/files"
131      mode: 0777
132      state: directory
133      recurse: yes

```

First, we cloned Drupal's git repository, using the `version` defined in our `vars.yml` file as `drupal_core_version`. The `git` module's `version` parameter defines the branch (`master`, `8.0.x`, etc.), tag (`1.0.1`, `7.24`, etc.), or individual commit hash (`50a1877`, etc.) to clone.

Next, we used Drush's `si` command (short for `site-install`) to run Drupal's installation (which configures the database, runs some maintenance, and sets some default configuration settings for the site). We passed in a few variables, like the `drupal_core_version` and `domain`; we also added a `drupal_site_name`, so add that variable to your `vars.yml` file:

```

10  # Your Drupal site name.
11  drupal_site_name: "D8 Test"

```

Also, Drupal's installation process results in the creation of a 'settings.php' file, so we use the location of that file with the `creates` parameter to let Ansible know if the site's already installed (so we don't accidentally try installing it again!). Once the site is installed, we also restart Apache for good measure (using `notify` again, like we did when updating Apache's configuration).

The final two tasks set permissions on Drupal's settings.php and files folder to 744 and 777, respectively.

Drupal LAMP server summary

At this point, if you access the server at `http://drupaltest.dev/` (assuming you've pointed drupal-test.dev to your server or VM's IP address), you'll see Drupal's default home page, and you could login with 'admin'/'admin'. (Obviously, you'd set a secure password on a production server!).

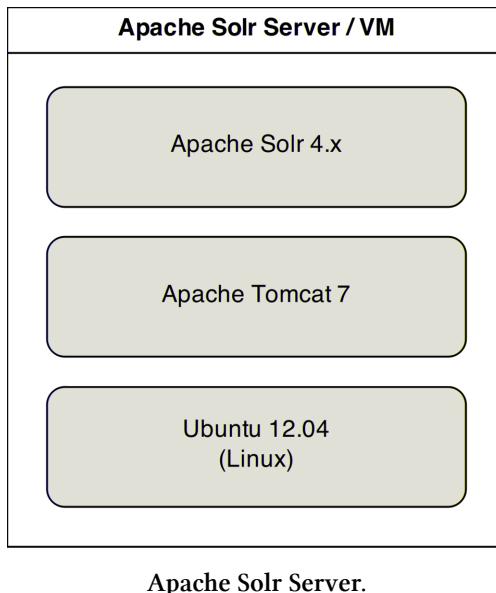
A similar server configuration, running Apache, MySQL, and PHP, can be used to run many popular web frameworks and CMSes besides Drupal, including Symfony, Wordpress, Joomla, Laravel, etc.



The entire example Drupal LAMP server playbook is in this book's code repository at [https://github.com/geerlingguy/ansible-for-devops⁵⁵](https://github.com/geerlingguy/ansible-for-devops), in the `drupal` directory.

Real-world playbook: Ubuntu Apache Tomcat server with Solr

Apache Solr is a fast and scalable search server optimized for full-text search, word highlighting, faceted search, fast indexing, and more. It's a very popular search server, and it's pretty easy to install and configure using Ansible. In the following example, we're going to set up Apache Solr using Ubuntu 12.04 and Apache Tomcat.



⁵⁵<https://github.com/geerlingguy/ansible-for-devops>

Include a variables file, and discover pre_tasks and handlers

Just like the previous LAMP server example, we'll begin this playbook by telling Ansible our variables will be in a separate `vars.yml` file:

```
1 - hosts: all
2
3   vars_files:
4     - vars.yml
```

Let's quickly create the `vars.yml` file, while we're thinking about it. Create the file in the same folder as your Solr playbook, and add the following contents:

```
1 download_dir: /tmp
2 solr_dir: /opt/solr
```

These two variables define two paths we'll use while downloading and installing Apache Solr.

Back in our playbook, after the `vars_files`, we also need to make sure the apt cache is up to date, using `pre_tasks` like the previous example:

```
5   pre_tasks:
6     - name: Update apt cache if needed.
7       apt: update_cache=yes cache_valid_time=3600
```

Like the Drupal playbook, we again use `handlers` to define certain tasks that are notified by tasks in the `tasks` section. This time, we just need a handler to restart `tomcat7`, the Java servlet container that powers Apache Solr:

```
8   handlers:
9     - name: restart tomcat
10      service: name=tomcat7 state=restarted
```

We can call this handler with the option `notify: restart tomcat` in any play in our playbook.

Install Apache Tomcat 7

It's easy enough to install Tomcat 7 on an Ubuntu Precise server; there are packages in the default apt repositories, so we just need to make sure they're installed, and that the `tomcat7` service is enabled and started:

```

11   tasks:
12     - name: Install Tomcat 7.
13       apt: "name={{ item }} state=installed"
14       with_items:
15         - tomcat7
16         - tomcat7-admin
17
18     - name: Ensure Tomcat 7 is started and enabled on boot.
19       service: name=tomcat7 state=started enabled=yes

```

That was easy enough! We used the `apt` module to install two packages, `tomcat7` and `tomcat7-admin` (so we can log into Tomcat's administrative backend), then started `tomcat7` and set it to start when the system boots.

Install Apache Solr

Ubuntu 12.04 includes a package for Apache Solr, but it installs a very old version, so we'll install the latest version of Solr from source. The first step is downloading the source:

```

20   - name: Download Solr.
21     get_url:
22       url: http://apache.osuosl.org/lucene/solr/4.9.1/solr-4.9.1.tgz
23       dest: "{{ download_dir }}/solr-4.9.1.tgz"
24       sha256sum: 4a546369a31d34b15bc4b99188984716bf4c0c158c0e337f3c1f98088aec70ee

```

We're installing Apache Solr 4.9.1, a recent stable version. When downloading files from remote servers, the `get_url` module provides more flexibility and convenience than raw `wget` or `curl` commands.

You have to pass `get_url` a `url` (the source of the file to be downloaded), and a `dest` (the location where the file will be downloaded). If you pass a directory to the `dest` parameter, Ansible will place the file inside, but will always re-download the file on subsequent runs of the playbook (and overwrite the existing download if it has changed). To avoid this extra overhead, we give the full path to the downloaded file.

We also use `sha256sum`, an optional parameter, for peace of mind; if you are downloading a file or archive that's critical to the functionality and security of your application, it's a good idea to check the file to make sure it is exactly what you're expecting. `sha256sum` compares a hash of the data in the downloaded file to a 256-bit hash that you specify (use `shasum -a 256 /path/to/file` to get the `sha256sum` of a file). If the checksum doesn't match the supplied hash, Ansible will fail and discard the freshly-downloaded (and invalid) file.

```

25 - name: Expand Solr.
26   command: >
27     tar -C /tmp -xvzf {{ download_dir }}/solr-4.9.1.tgz
28     creates={{ download_dir }}/solr-4.9.1/dist/solr-4.9.1.war
29
30 - name: Copy Solr into place.
31   command: >
32     cp -r {{ download_dir }}/solr-4.9.1 {{ solr_dir }}
33     creates={{ solr_dir }}/dist/solr-4.9.1.war

```

We need to expand the Apache Solr archive, then copy it into place. For both of these steps, use the built-in tar and cp utilities (with the appropriate options) to do the work. Setting creates tells Ansible to skip these steps in subsequent runs, since the Solr war file will already be in place.

```

34 # Use shell so commands are passed in correctly.
35 - name: Copy Solr components into place.
36   shell: >
37     cp -r {{ item.src }} {{ item.dest }}
38     creates={{ itemcreates }}
39   with_items:
40     # Solr example configuration and war file.
41     - {
42       src: "{{ solr_dir }}/example/webapps/solr.war",
43       dest: "{{ solr_dir }}/solr.war",
44       creates: "{{ solr_dir }}/solr.war"
45     }
46     - {
47       src: "{{ solr_dir }}/example/solr/*",
48       dest: "{{ solr_dir }}/",
49       creates: "{{ solr_dir }}/solr.xml"
50     }
51     # Solr log4j logging configuration.
52     - {
53       src: "{{ solr_dir }}/example/lib/ext/*",
54       dest: "/var/lib/tomcat7/shared/",
55       creates: "/var/lib/tomcat7/shared/log4j-1.2.16.jar"
56     }
57     - {
58       src: "{{ solr_dir }}/example/resources/log4j.properties",
59       dest: "/var/lib/tomcat7/shared/classes",
60       creates: "/var/lib/tomcat7/shared/classes/log4j.properties"
61     }
62   notify: restart tomcat

```

The next task copies into place certain directories and files required to run Apache Solr.

Nothing too special here, but this example illustrates the use of comments within `with_items` lists to help clarify the items in the list. We could've added each command as its own task, but doing it this way reduces the total number of Ansible tasks and allows us to move the `with_items` list to an external variable if desired.

```
63 - name: Ensure solr example directory is absent.
64   file:
65     path: "{{ solr_dir }}/example"
66     state: absent
67
68 - name: Set up solr data directory.
69   file:
70     path: "{{ solr_dir }}/data"
71     state: directory
72     owner: tomcat7
73     group: tomcat7
```

The latest version of Apache Solr searches through all the directories inside `{{ solr_dir }}` recursively, loading any potential search configuration it finds. Since we copied over one of the examples to use as the server's default search core, Solr would see it as a duplicate of one of the examples and crash. So, we use the `file` module with a `path` to the example directory to make sure the directory is gone (`state=absent`).

After removing the example directory (and in future runs, ensuring it's still gone), we set up the data directory where Solr will store index data, ensuring it exists as a directory and is owned by the `tomcat7` user and group.

```
73 - name: Configure solrconfig.xml for new data directory.
74   lineinfile:
75     dest: "{{ solr_dir }}/collection1/conf/solrconfig.xml"
76     regexp: "^.+<dataDir .+$"
77     line: "<dataDir>$solr.data.dir:{{ solr_dir }}/data</dataDir>"
78     state: present
```

As we found [earlier](#), `lineinfile` is a helpful module for ensuring consistent configuration file settings with idempotence. In this case, we need to make sure the `<dataDir>` line in our default search core's configuration file is set to a specific value.

```

79 - name: Set permissions for solr home.
80   file:
81     path: "{{ solr_dir }}"
82     recurse: yes
83     owner: tomcat7
84     group: tomcat7

```

To set ownership options on the entire contents of the {{ solr_dir }} correctly, we use the `file` module with the `reurse` parameter set to yes. This is equivalent to the shell command `chown -R tomcat7:tomcat7 {{ solr_dir }}`.

```

84 - name: Add Catalina configuration for solr.
85   template:
86     src: templates/solr.xml.j2
87     dest: /etc/tomcat7/Catalina/localhost/solr.xml
88     owner: root
89     group: tomcat7
90     mode: 0644
91     notify: restart tomcat

```

The final task copies a template file (`solr.xml.j2`) to the remote host, substituting variables via Jinja2 syntax, and sets the file's ownership and permissions as needed for Tomcat.

Before the task runs, the local template file will need to be created. Create a 'templates' folder in the same directory as your Apache Solr playbook, and create a new file named `solr.xml.j2` inside, with the following contents:

```

1 <?xml version="1.0" encoding="utf-8"?>
2 <Context docBase="{{ solr_dir }}/solr.war" debug="0" crossContext="true">
3   <Environment name="solr/home" type="java.lang.String" \
4     value="{{ solr_dir }}" override="true"/>
5 </Context>

```

Run the playbook with `$ ansible-playbook [playbook-name.yml]`, and after a few minutes (depending on your server's Internet connection speed), you should be able to access the Solr admin interface at `http://example.com:8080/solr` (where 'example.com' is your server's hostname or IP address).

Apache Solr server summary

The configuration we used when deploying Apache Solr allows for a multicore setup, so you could add more 'search cores' via the admin interface (as long as the directories and core schema

configuration is in place in the filesystem), and have multiple indexes for multiple websites and applications.

A playbook similar to the one above is used as part of the infrastructure for [Hosted Apache Solr⁵⁶](#), a service I run which hosts Apache Solr search cores for Drupal websites.



The entire example Apache Solr server playbook is in this book's code repository at <https://github.com/geerlingguy/ansible-for-devops⁵⁷>, in the `solr` directory.

Summary

At this point, you should be getting comfortable with Ansible's *modus operandi*. Playbooks are the heart of Ansible's configuration management and provisioning functionality, and the same modules and similar syntax can be used with ad-hoc commands for deployments and general server management.

Now that you're familiar with playbooks, we'll explore more advanced concepts in building playbooks, like organization of tasks, conditionals, variables, and more. Later, we'll explore the use of playbooks with roles to make them infinitely more flexible and to save time setting up and configuring your infrastructure.

```
/ If everything is under control, you are \
\ going too slow. (Mario Andretti)      /
```

```
-----
```

```
\  ^__^
 \  (oo)\_____
   (__)\       )\/\
     ||----w |
     ||     ||
```

⁵⁶<http://hostedapachesolr.com/>

⁵⁷<https://github.com/geerlingguy/ansible-for-devops>

Chapter 5 - Ansible Playbooks - Beyond the Basics

The playbooks and simple playbook organization we used in the previous chapter cover many common use cases. When discussing the breadth of system administration needs, there are thousands more features of Ansible you need to know.

We'll cover how to run plays with more granularity, how to organize your tasks and playbooks for simplicity and usability, and other advanced playbook topics that will help you manage your infrastructure with even more confidence.

Handlers

In chapter 4, the Ubuntu LAMP server example used a simple handler to restart Apache, and certain tasks that affected Apache's configuration notified the handler with the option `notify: restart apache`:

```
handlers:  
  - name: restart apache  
    service: name=apache2 state=restarted  
  
tasks:  
  - name: Enable Apache rewrite module.  
    apache2_module: name=rewrite state=present  
    notify: restart apache
```

In some circumstances you may want to notify multiple handlers, or even have handlers notify additional handlers. Both are easy to do with Ansible. To notify multiple handlers from one task, use a list for the `notify` option:

```
- name: Rebuild application configuration.  
  command: /opt/app/rebuild.sh  
  notify:  
    - restart apache  
    - restart memcached
```

To have one handler notify another, add a `notify` option onto the handler—handlers are basically glorified tasks that can be called by the `notify` option, but since they act as tasks themselves, they can chain themselves to other handlers:

```
handlers:
  - name: restart apache
    service: name=apache2 state=restarted
    notify: restart memcached

  - name: restart memcached
    service: name=memcached state=restarted
```

There are a few other considerations when dealing with handlers:

- Handlers will only be run if a task notifies the handler; if a task that would've notified the handlers is skipped due to a `when` condition or something of the like, the handler will not be run.
- Handlers will run once, and only once, at the end of a play. If you absolutely need to override this behavior and run handlers in the middle of a playbook, you can use the `meta` module to do so (e.g. `- meta: flush_handlers`).
- If the play fails on a particular host (or all hosts) before handlers are notified, the handlers will never be run. If it's desirable to always run handlers, even after the playbook has failed, you can use the `meta` module as described above as a separate task in the playbook, or you use the command line flag `--force-handlers` when running your playbook. Handlers won't run on any hosts that became unreachable during the playbook's run.

Environment variables

Ansible allows you to work with environment variables in a variety of ways. First of all, if you need to set some environment variables for your remote user account, you can do that by adding lines to the remote user's `.bash_profile`, like so:

```
- name: Add an environment variable to the remote user's shell.
  lineinfile: dest=~/.bash_profile regexp='^ENV_VAR=' line="ENV_VAR=value"
```

All subsequent tasks will then have access to this environment variable (remember, of course, only the `shell` module will understand shell commands that use environment variables!). To use an environment variable in further tasks, it's recommended you use a task's `register` option to store the environment variable in a variable Ansible can use later, for example:

```

1 - name: Add an environment variable to the remote user's shell.
2   lineinfile: dest=~/bash_profile regexp='^ENV_VAR=' line=ENV_VAR=value
3
4 - name: Get the value of the environment variable we just added.
5   shell: 'source ~/bash_profile && echo $ENV_VAR'
6   register: foo
7
8 - name: Print the value of the environment variable.
9   debug: msg="The variable is {{ foo.stdout }}"

```

We use `source ~/bash_profile` in line 4 because Ansible needs to make sure it's using the latest environment configuration for the remote user. In some situations, the tasks all run over a persistent or quasi-cached SSH session, over which `$ENV_VAR` wouldn't yet be defined.

(This is also the first time the `debug` module has made an appearance. It will be explored more in-depth along with other debugging techniques later.).



Why `~/bash_profile`? There are many different places you can store environment variables, including `.bashrc`, `.profile`, and `.bash_profile` in a user's home folder. In our case, since we want the environment variable to be available to Ansible, which runs a pseudo-TTY shell session, in which case `.bash_profile` is used to configure the environment. You can read more about shell session configuration and these dotfiles here: [Configuring your login sessions with dotfiles⁵⁸](#).

Linux will also read global environment variables added to `/etc/environment`, so you can add your variable there:

```

- name: Add a global environment variable.
  lineinfile: dest=/etc/environment regexp='^ENV_VAR=' line=ENV_VAR=value
  sudo: yes

```

In any case, it's pretty simple to manage environment variables on the server with `lineinfile`. If your application requires many environment variables (as is the case in many Java applications), you might consider using `copy` or `template` with a local file instead of using `lineinfile` with a large list of items.

Per-play environment variables

You can also set the environment for just one play, using the `environment` option for that play. As an example, let's say you need to set an http proxy for a certain file download. This can be done with:

⁵⁸<http://mywiki.wooledge.org/DotFiles>

```
- name: Download a file, using example-proxy as a proxy.
  get_url: url=http://www.example.com/file.tar.gz dest=~/Downloads/
  environment:
    http_proxy: http://example-proxy:80/
```

That could be rather cumbersome, though, especially if you have many tasks that require a proxy or some other environment variable. In this case, you can pass an environment in via a variable in your playbook's `vars` section (or via an included variables file), like so:

```
vars:
  var_proxy:
    http_proxy: http://example-proxy:80/
    https_proxy: https://example-proxy:443/
    [etc...]

tasks:
- name: Download a file, using example-proxy as a proxy.
  get_url: url=http://www.example.com/file.tar.gz dest=~/Downloads/
  environment: var_proxy
```

If a proxy needs to be set system-wide (as is the case behind many corporate firewalls), I like to do so using the global `/etc/environment` file:

```
1 # In the 'vars' section of the playbook (set to 'absent' to disable proxy):
2 proxy_state: present
3
4 # In the 'tasks' section of the playbook:
5 - name: Configure the proxy.
6   lineinfile:
7     dest: /etc/environment
8     regexp: "{{ item.regexp }}"
9     line: "{{ item.line }}"
10    state: "{{ proxy_state }}"
11  with_items:
12    - { regexp: "http_proxy=", line: "http_proxy=http://example-proxy:80/" }
13    - { regexp: "https_proxy=", line: "https_proxy=https://example-proxy:443/" }
14    - { regexp: "ftp_proxy=", line: "ftp_proxy=http://example-proxy:80/" }
```

Doing it this way allows me to configure whether the proxy is enabled per-server (using the `proxy_state` variable), and with one play, set the http, https, and ftp proxies. You can use a similar kind of play for any other types of environment variables you need to set system-wide.



You can test remote environment variables using the `ansible` command: `ansible test -m shell -a 'echo $TEST'`. When doing so, be careful with your use of quotes and escaping—you might end up using double quotes where you meant to use single quotes, or vice-versa, and end up printing a local environment variable instead of one from the remote server!

Variables

Variables in Ansible work just like variables in most other systems. Variables always begin with a letter ([A-Za-z]), and can include any number of underscores (_) or numbers ([0-9]).

Valid variable names include `foo`, `foo_bar`, `foo_bar_5`, and `fooBar`, though the standard is to use all lowercase letters, and typically avoid numbers in variable names (no camelCase or UpperCamelCase).

Invalid variable names include `_foo`, `foo-bar`, `5_foo_bar`, `foo.bar` and `foo bar`.

In an inventory file, a variable's value is assigned using an equals sign, like so:

```
foo=bar
```

In a playbook or variables include file, a variable's value is assigned using a colon, like so:

```
foo: bar
```

Playbook Variables

There are many different ways you can define variables to use in tasks.

Variables can be passed in via the command line, when calling `ansible-playbook`, with the `--extra-vars` option:

```
ansible-playbook example.yml --extra-vars "foo=bar"
```

You can also pass in extra variables using quoted JSON, YAML, or even by passing a JSON or YAML file directly, like `--extra-vars "@even_more_vars.json"` or `--extra-vars "@even_more_vars.yml"`, but at this point, you might be better off using one of the other methods below.

Variables may be included inline with the rest of a playbook, in a `vars` section:

```

1  ---
2  - hosts: example
3  vars:
4    foo: bar
5  tasks:
6    # Prints "Variable 'foo' is set to bar".
7    - debug: msg="Variable 'foo' is set to {{ foo }}"

```

Variables may also be included in a separate file, using the `vars_files` section:

```

1  ---
2  # Main playbook file.
3  - hosts: example
4  vars_files:
5    - vars.yml
6  tasks:
7    - debug: msg="Variable 'foo' is set to {{ foo }}"

```



```

1  ---
2  # Variables file 'vars.yml' in the same folder as the playbook.
3  foo: bar

```

Notice how the variables are all at the root level of the YAML file. They don't need to be under any kind of `vars` heading when they are included as a standalone file.

Variable files can also be imported conditionally. Say, for instance, you have one set of variables for your CentOS servers (where the Apache service is named `httpd`), and another for your Debian servers (where the Apache service is named `apache2`). In this case, you could use a conditional `vars_files` include:

```

1  ---
2  - hosts: example
3  vars_files:
4    - [ "apache_{{ ansible_os_family }}.yml", "apache_default.yml" ]
5  tasks:
6    - service: name={{ apache }} state=running

```

Then, add two files in the same folder as your example playbook, `apache_CentOS.yml`, and `apache_default.yml`. Define the variable `apache: httpd` in the CentOS file, and `apache: apache2` in the default file.

As long as your remote server has `facter` or `ohai` installed, Ansible will be able to read the OS of the server, translate that to a variable (`ansible_os_family`), and include the `vars` file with the resulting name. If `ansible` can't find a file with that name, it will use the second option (`apache_default.yml`). So, on a Debian or Ubuntu server, Ansible would correctly use `apache2` as the service name, even though there is no `apache_Debian.yml` or `apache_Ubuntu.yml` file available.

Inventory variables

Variables may also be added via Ansible inventory files, either inline with a host definition, or after a group:

```
1 # Host-specific variables (defined inline).
2 [washington]
3 app1.example.com proxy_state=present
4 app2.example.com proxy_state=absent
5
6 # Variables defined for the entire group.
7 [washington:vars]
8 cdn_host=washington.static.example.com
9 api_version=3.0.1
```

If you need to define more than a few variables, especially variables that apply to more than one or two hosts, inventory files can be cumbersome. In fact, Ansible's documentation recommends **not** storing variables within the inventory. Instead, you can use `group_vars` and `host_vars` YAML variable files within a specific path, and Ansible will assign them to individual hosts and groups defined in your inventory.

For example, to apply a set of variables to the host `app1.example.com`, create a blank file named `app1.example.com` at the location `/etc/ansible/host_vars/app1.example.com`, and add variables as you would in an included `vars_files` YAML file:

```
---
foo: bar
baz: qux
```

To apply a set of variables to the entire `washington` group, create a similar file in the location `/etc/ansible/group_vars/washington` (substitute `washington` for whatever group name's variables you're defining).

You can also put these files (named the same way) in `host_vars` or `group_vars` directories in your playbook's directory. Ansible will use the variables defined in the inventory `/etc/ansible/[host|group]_vars` directory first (if the appropriate files exist), then it will use variables defined in the playbook directories.

Another alternative to using `host_vars` and `group_vars` is to use conditional variable file imports, as was mentioned above.

Registered Variables

There are many times that you will want to run a command, then use its return code, stderr, or stdout to determine whether to run a later task. For these situations, Ansible allows you to use register to store the output of a particular command in a variable at runtime.

In the previous chapter, we used register to get the output of the forever list command, then used the output to determine whether we needed to start our Node.js app:

```
39 - name: "Node: Check list of Node.js apps running."
40   command: forever list
41   register: forever_list
42   changed_when: false
43
44 - name: "Node: Start example Node.js app."
45   command: forever start {{ node_apps_location }}/app/app.js
46   when: "forever_list.stdout.find('{{ node_apps_location }}/app/app.js') == -1"
```

In that example, we used a string function built into Python (`find`) to search for the path to our app, and if it was not present, the Node.js app was started.

We will explore the use of register further later in this chapter.

Accessing Variables

Simple variables (gathered by Ansible, defined in inventory files, or defined in playbook or variable files) can be used as part of a task using syntax like `{{ variable }}`. For example:

```
- command: /opt/my-app/rebuild {{ my_environment }}
```

When the command is run, Ansible will substitute the contents of `my_environment` for `{{ my_environment }}`. So the resulting command would be something like `/opt/my-app/rebuild dev`.

Many variables you will use are structured as arrays (or ‘lists’), and accessing the array `foo` would not give you enough information to be useful (except when passing in the array in a context where Ansible will use the entire array, like when using `with_items`).

If you define a list variable like so:

```
foo_list:
  - one
  - two
  - three
```

You could access the first item in that array with either of the following syntax:

```
foo[0]
foo|first
```

Note that the first line uses standard Python array access syntax ('retrieve the first (0-indexed) element of the array'), whereas the second line uses a convenient *filter* provided by Jinja2. Either way is equally valid and useful, and it's really up to you whether you like the first or second technique.

For larger and more structured arrays (for example, when retrieving the IP address of the server using the facts Ansible gathers from your server), you can access any part of the array by drilling through the array keys, either using bracket ([]) or dot (.) syntax. For example, if you would like to retrieve the information about the eth0 network interface, you could first take a look at the entire array using debug in your playbook:

```
# In your playbook.

tasks:
  - debug: var=ansible_eth0
```

```
TASK: [debug var=ansible_eth0] ****
ok: [webserver] => {
    "ansible_eth0": {
        "active": true,
        "device": "eth0",
        "ipv4": {
            "address": "10.0.2.15",
            "netmask": "255.255.255.0",
            "network": "10.0.2.0"
        },
        "ipv6": [
            {
                "address": "fe80::a00:27ff:feb1:589a",
                "prefix": "64",
                "scope": "link"
            }
        ],
    }
```

```
    "macaddress": "08:00:27:b1:58:9a",
    "module": "e1000",
    "mtu": 1500,
    "promisc": false,
    "type": "ether"
}
}
```

Now that you know the overall structure of the variable, you can use either of the following techniques to retrieve only the IPv4 address of the server:

```
{{ ansible_eth0.ipv4.address }}  
{{ ansible_eth0['ipv4']['address'] }}
```

Host and Group variables

Ansible conveniently lets you define or override variables on a per-host or per-group basis. As we learned earlier, your inventory file can define groups and hosts like so:

```
1 [group]
2 host1
3 host2
```

The simplest way to define variables on a per-host or per-group basis is to do so directly within the inventory file:

```
1 [group]
2 host1 admin_user=jane
3 host2 admin_user=jack
4 host3
5
6 [group:vars]
7 admin_user=john
```

In this case, Ansible will use the group default variable ‘john’ for {{ admin_user }}, but for host1 and host2, the admin users defined alongside the hostname will be used.

This is convenient and works well when you need to define a variable or two per-host or per-group, but once you start getting into more involved playbooks, you might need to add a few (3+) host-specific variables. In these situations, you can define the variables in a different place to make maintenance and readability much easier.

group_vars and host_vars

Ansible will search within the same directory as your inventory file (or inside /etc/ansible if you're using the default inventory file at /etc/ansible/hosts) for two specific directories: group_vars and host_vars.

You can place YAML files inside these directories named after the group name or hostname defined in your inventory file. Continuing our example above, let's move the specific variables into place:

```
1 ---  
2 # File: /etc/ansible/group_vars/group  
3 admin_user: john
```

```
1 ---  
2 # File: /etc/ansible/host_vars/host1  
3 admin_user: jane
```

Even if you're using the default inventory file (or an inventory file outside of your playbook's root directory), Ansible will also use host and group variables files located within your playbook's own group_vars and host_vars directories. This is convenient when you want to package together your entire playbook and infrastructure configuration (including all host/group-specific configuration) into a source-control repository.

You can also define a group_vars/all file that would apply to *all* groups, as well as a host_vars/all file that would apply to *all* hosts. Usually, though, it's a better idea to define sane defaults in your playbooks and roles (which will be discussed later).

Magic variables with host and group variables and information

If you ever need to retrieve a specific host's variables from another host, Ansible provides a magic hostvars variable containing all the defined host variables (from inventory files and any discovered YAML files inside host_vars directories).

```
# From any host, returns "jane".  
{{ hostvars['host1']['admin_user'] }}
```

There are a variety of other variables Ansible provides that you may need to use from time to time:

- groups: A list of all group names in the inventory.
- group_names: A list of all the groups of which the *current* host is a part.
- inventory_hostname: The hostname of the current host, according to the *inventory*(this can differ from ansible_hostname, which is the hostname reported by the system).

- `inventory_hostname_short`: The first part of `inventory_hostname`, up to the first period.
- `play_hosts`: All hosts on which the current play will be run.

Please see [Magic Variables, and How To Access Information About Other Hosts⁵⁹](#) in Ansible's official documentation for the latest information and further usage examples.

Facts (Variables derived from system information)

By default, whenever you run an Ansible playbook, Ansible first gathers information (“facts”) about each host in the play. You may have noticed this whenever we ran playbooks in earlier chapters:

```
$ ansible-playbook playbook.yml

PLAY [group] ****
GATHERING FACTS ****
ok: [host1]
ok: [host2]
ok: [host3]
```

Facts can be extremely helpful when you're running playbooks; you can use gathered information like host IP addresses, CPU type, disk space, operating system information, and network interface information to change when certain tasks are run, or to change certain information used in configuration files.

To get a list of every gathered fact available, you can use the `ansible` command with the `setup` module:

```
$ ansible munin -m setup
munin.midwesternmac.com | success >> {
    "ansible_facts": {
        "ansible_all_ipv4_addresses": [
            "167.88.120.81"
        ],
        "ansible_all_ipv6_addresses": [
            "2604:180::a302:9076",
        ]
    }
}
```

If you don't need to use facts, and would like to save a few seconds per-host when running playbooks (this can be especially helpful when running an Ansible playbook against dozens or hundreds of servers), you can set `gather_facts: no` in your playbook:

⁵⁹http://docs.ansible.com/playbooks_variables.html#magic-variables-and-how-to-access-information-about-other-hosts

```
- hosts: db
  gather_facts: no
```

Many of my own playbooks and roles use facts like `ansible_os_family`, `ansible_hostname`, and `ansible_memtotal_mb` to register new variables or in tandem with `when`, to determine whether to run certain tasks.



If you have [Facter⁶⁰](#) or [Ohai⁶¹](#) installed on a remote host, Ansible will also include their gathered facts as well, prefixed by `facter_` and `ohai_`, respectively. If you're using Ansible in tandem with Puppet or Chef, and are already familiar with those system-information-gathering tools, you can conveniently use them within Ansible as well. If not, Ansible's Facts are usually sufficient for whatever you need to do, and can be made even more flexible through the use of Local Facts.



If you run a playbook against similar servers or virtual machines (e.g. all your servers are running the same OS, same hosting provider, etc.), facts are almost always consistent in their behavior. When running playbooks against a diverse set of hosts (for example, hosts with different OSes, virtualization stacks, or hosting providers), know that some facts may contain different information than you were expecting. For [Server Check.in⁶²](#), I have servers from no less than five different hosting providers, running on vastly different hardware, so I am sure to monitor the output of my `ansible-playbook` runs for abnormalities, especially when adding new servers to the mix.

Local Facts (Facts.d)

Another way of defining host-specific facts is to place `.fact` file in a special directory on remote hosts, `/etc/ansible/facts.d/`. These files can be either JSON or INI files, or you could use executables that return JSON. As an example, create the file `/etc/ansible/facts.d/settings.fact` on a remote host, with the following contents:

```
1 [users]
2 admin=jane, john
3 normal=jim
```

Next, use Ansible's `setup` module to display the new facts on the remote host:

⁶⁰<https://tickets.puppetlabs.com/browse/FACT>

⁶¹<http://docs.getchef.com/ohai.html>

⁶²<https://servercheck.in/>

```
$ ansible hostname -m setup -a "filter=ansible_local"
munin.midwesternmac.com | success >> {
    "ansible_facts": {
        "ansible_local": {
            "settings": {
                "users": {
                    "admin": "jane, john",
                    "normal": "jim"
                }
            }
        }
    },
    "changed": false
}
```

If you are using a playbook to provision a new server, and part of that playbook adds a local `.fact` file which generates local facts that are used later, you can explicitly tell Ansible to reload the local facts using a task like the following:

```
1 - name: Reload local facts.
2   setup: filter=ansible_local
```



While it may be tempting to use local facts rather than `host_vars` or other variable definition methods, remember that it's often better to build your playbooks in a way that doesn't rely (or care about) specific details of individual hosts. Sometimes it is necessary to use local facts (especially if you are using executables in `facts.d` to define the facts based on changing local environments), but it's almost always better to keep configuration in a central repository, and move away from host-specific facts.



Note that `setup` module options (like `filter`) won't work on remote Windows hosts, as of this writing.

Variable Precedence

It should be rare that you would need to dig into the details of which variable is used when you define the same variable in five different places, but since there are odd occasions where this is the case, Ansible's documentation provides the following ranking:

1. Variables from the command line (`-e` in the command line) always win.

2. Connection variables defined in inventory (`ansible_ssh_user`, etc.).
3. “Most everything else” (command line switches, variables defined in a play, included variables, role variables, etc.).
4. Other (non-connection) inventory variables.
5. Local facts and automatically discovered facts (via `gather_facts`).
6. Role default variables (inside a role’s `defaults/main.yml` file).

After lots of experience building playbooks, roles, and managing inventories, you’ll likely find the right mix of variable definition for your needs, but there are a few general things that will mitigate any pain in setting and overriding variables on a per-play, per-host, or per-run basis:

- Roles (to be discussed in the next chapter) should provide sane default values via the role’s ‘`defaults`’ variables. These variables will be the fallback in case the variable is not defined anywhere else in the chain.
- Playbooks should rarely define variables (e.g. via `set_fact`), but rather, variables should be defined either in included `vars_files` or, less often, via inventory.
- Only truly host- or group-specific variables should be defined in host or group inventories.
- Dynamic and static inventory sources should contain a minimum of variables, especially as these variables are often less visible to those maintaining a particular playbook.
- Command line variables (`-e`) should be avoided when possible. One of the main use cases is when doing local testing or running one-off playbooks where you aren’t worried about the maintainability or idempotence of the tasks you’re running.

See Ansible’s [Variable Precedence⁶³](#) documentation for more detail and examples.

If/then/when - Conditionals

Many tasks need only be run in certain circumstances. Some tasks use modules with built-in idempotence (as is the case when ensuring a yum or apt package is installed), and you usually don’t need to define further conditional behaviors for these tasks.

However, there are many tasks—especially those using Ansible’s `command` or `shell` modules—which require further input as to when they’re supposed to run, whether they’ve changed anything after they’ve been run, or when they’ve failed to run.

We’ll cover all the main conditionals behaviors you can apply to Ansible tasks, as well as how you can tell Ansible when a play has done something to a server or failed.

⁶³http://docs.ansible.com/playbooks_variables.html#variable-precedence-where-should-i-put-a-variable

Jinja2 Expressions, Python built-ins, and Logic

Before discussing all the different uses of conditionals in Ansible, it's worthwhile to cover a small part of Jinja2 (the syntax Ansible uses both for templates and for conditionals), and available Python functions (often referred to as 'built-ins'). Ansible uses expressions and built-ins with `when`, `changed_when`, and `failed_when` so you can describe these things to Ansible with as much precision as possible.

Jinja2 allows the definition of literals like strings ("string"), integers (42), floats (42.33), lists ([1, 2, 3]), tuples (like lists, but can't be modified) dictionaries ({key: value, key2: value2}), and booleans (true or false).

Jinja2 also allows basic math operations, like addition, subtraction, multiplication and division, and comparisons (== for equality, != for inequality, >= for greater than or equal to, etc.). Logical operators are and, or, and not, and you can group expressions by placing them within parenthesis.

If you're familiar with almost any programming language, you will probably pick up basic usage of Jinja2 expressions in Ansible very quickly.

For example:

```
# The following expressions evaluate to 'true':  
1 in [1, 2, 3]  
'see' in 'Can you see me?'  
foo != bar  
(1 < 2) and ('a' not in 'best')  
  
# The following expressions evaluate to 'false':  
4 in [1, 2, 3]  
foo == bar  
(foo != foo) or (a in [1, 2, 3])
```

Jinja2 also offers a helpful set of 'tests' you can use to test a given object. For example, if you define the variable `foo` for only a certain group of servers, but not others, you can use the expression `foo is defined` with a conditional to evaluate to 'true' if the variable is defined, or false if not.

There are many other checks you can perform as well, like `undefined` (the opposite of `defined`), `equalto` (works like ==), `even` (returns true if the variable is an even number), and `iterable` (if you can iterate over the object). We'll cover the full gamut later in the book, but for now, know that you can use Ansible conditionals with Jinja2 expressions to do some powerful things!

For the few cases where Jinja2 doesn't provide enough power and flexibility, you can invoke Python's built-in library functions (like `string.split`, `[number].is_signed()`) to manipulate variables and determine whether a given task should be run, resulted in a change, failed, etc.

As an example, I need to parse version strings from time to time, to find the major version of a particular project. Assuming the variable `software_version` is set to 4.6.1, I can get the major

version by splitting the string on the `.` character, then using the first element of the array. I can check if the major version is 4 using `when`, and choose to run (or not run) a certain task:

```
1 - name: Do something only for version 4 of the software.  
2   [task here]  
3   when: software_version.split('.')[0] == '4'
```

It's generally best to stick with simpler Jinja2 filters and variables, but it's nice to be able to use Python when you're doing more advanced variable manipulation.

register

In Ansible, any play can ‘register’ a variable, and once registered, that variable will be available to all subsequent tasks. Registered variables work just like normal variables or host facts.

Many times, you may need the output (stdout or stderr) of a shell command, and you can get that in a variable using the following syntax:

```
- shell: my_command_here  
register: my_command_result
```

Later, you can access stdout (as a string) with `my_command_result.stdout`, and stderr with `my_command_result.stderr`.

Registered facts are very helpful for many types of tasks, and can be used both with conditionals (defining when and how a play runs), and in any part of the play. As an example, if you have a command that outputs a version number string like “10.0.4”, and you register the output as `version`, you can use the string later when doing a code checkout by printing the variable `{{ version.stdout }}`.



If you want to see the different properties of a particular registered variable, you can run a playbook with `-v` to inspect play output. Usually, you'll get access to values like `changed` (whether the play resulted in a change), `delta` (the time it took to run the play), `stderr` and `stdout`, etc. Some Ansible modules (like `stat`) add much more data to the registered variable, so always inspect the output with `-v` if you need to see what's inside.

when

One of the most helpful extra keys you can add to a play is a `when` statement. Let's take a look at a simple use of `when`:

```
- yum: name=mysql-server state=present
  when: is_db_server
```

The above statement assumes you've defined the `is_db_server` variable as a boolean (`true` or `false`) earlier, and will run the play if the value is true, or skip the play when the value is false.

If you only define the `is_db_server` variable on database servers (meaning there are times when the variable may not be defined at all), you could run tasks conditionally like so:

```
- yum: name=mysql-server state=present
  when: (is_db_server is defined) and is_db_server
```

`when` is even more powerful if used in conjunction with variables registered by previous tasks. As an example, we want to check the status of a running application, and run a play only when that application reports it is 'ready' in its output:

```
- command: my-app --status
  register: myapp_result

- command: do-something-to-my-app
  when: "'ready' in myapp_result.stdout"
```

These examples are a little contrived, but they illustrate basic uses of `when` in your tasks. Here are some examples of uses of `when` in real-world playbooks:

```
# From our Node.js playbook - register a command's output, then see
# if the path to our app is in the output. Start the app if it's
# not present.
- command: forever list
  register: forever_list
- command: forever start /path/to/app/app.js
  when: "forever_list.stdout.find('/path/to/app/app.js') == -1"

# Run 'ping-hosts.sh' script if 'ping_hosts' variable is true.
- command: /usr/local/bin/ping-hosts.sh
  when: ping_hosts

# Run 'git-cleanup.sh' script if a branch we're interested in is
# missing from git's list of branches in our project.
- command: chdir=/path/to/project git branch
  register: git_branches
- command: /path/to/project/scripts/git-cleanup.sh
```

```

when: "(is_app_server == true) and ('interesting-branch' not in \
git_branches.stdout)"

# Downgrade PHP version if the current version contains '7.0'.
- shell: php --version
  register: php_version
- shell: yum -y downgrade php*
  when: "'7.0' in php_version.stdout"

# Copy a file to the remote server if the hosts file doesn't exist.
- stat: path=/etc/hosts
  register: hosts_file
- copy: src=path/to/local/file dest=/path/to/remote/file
  when: hosts_file.stat.exists == false

```

changed_when and failed_when

Just like `when`, you can use `changed_when` and `failed_when` to influence Ansible's reporting of when a certain task results in changes or failures.

It is difficult for Ansible to determine if a given command results in changes, so if you use the `command` or `shell` module without also using `changed_when`, Ansible will always report a change. Most Ansible modules report whether they resulted in changes correctly, but you can also override this behavior by invoking `changed_when` yourself.

When using PHP Composer as a command to install project dependencies, it's useful to know when Composer installed something, or when nothing changed. Here's an example:

```

1 - name: Install dependencies via Composer.
2   command: "/usr/local/bin/composer global require phpunit/phpunit --prefer-dist"
3   register: composer
4   changed_when: "'Nothing to install or update' not in composer.stdout"

```

You can see we used `register` to store the results of the command, then we checked whether a certain string was in the registered variable's `stdout`. Only when Composer doesn't do anything will it print "Nothing to install or update", so we use that string to tell Ansible if the task resulted in a change.

Many command-line utilities print results to `stderr` instead of `stdout`, so `failed_when` can be used to tell Ansible when a task has *actually* failed and is not just reporting its results in the wrong way. Here's an example where we need to parse the `stderr` of a Jenkins CLI command to see if Jenkins did, in fact, fail to perform the command we requested:

```

1 - name: Import a Jenkins job via CLI.
2   shell: >
3     java -jar /opt/jenkins-cli.jar -s http://localhost:8080/
4     create-job "My Job" < /usr/local/my-job.xml
5   register: import
6   failed_when: "import.stderr and 'already exists' not in import.stderr"

```

In this case, we only want Ansible to report a failure when the command returns an error, and that error doesn't contain 'already exists'. It's debatable whether the command should report a job already exists via stderr, or just print the result to stdout... but it's easy to account for whatever the command does with Ansible!

ignore_errors

Sometimes there are commands that should be run always, and they often report errors. Or there are scripts you might run that output errors left and right, and the errors don't actually indicate a problem, but they're just annoying (and they cause your playbooks to stop executing).

For these situations, you can add `ignore_errors` to the task, and Ansible will remain blissfully unaware of any problems running a particular task. Be careful using this, though; it's usually best if you can find a way to work with and around the errors generated by tasks so playbooks *do* fail if there are actual problems.

Delegation, Local Actions, and Pauses

Some tasks, like sending a notification, communicating with load balancers, or making changes to DNS, networking, or monitoring servers, require Ansible to run the task on the host machine (running the playbook) or another host besides the one(s) being managed by the playbook. Ansible allows any task to be delegated to a particular host using `delegate_to`:

```

1 - name: Add server to Munin monitoring configuration.
2   command: monitor-server webservers {{ inventory_hostname }}
3   delegate_to: "{{ monitoring_master }}"

```

Delegation is often used to manage a server's participation in a load balancer or replication pool; you might either run a particular command locally (as in the example below), or you could use one of Ansible's built-in load balancer modules and `delegate_to` a specific load balancer host directly:

```
1 - name: Remove server from load balancer.
2   command: remove-from-lb {{ inventory_hostname }}
3   delegate_to: 127.0.0.1
```

If you're delegating a task to localhost, Ansible has a convenient shorthand you can use, `local_action`, instead of adding the entire `delegate_to` line:

```
1 - name: Remove server from load balancer.
2   local_action: command remove-from-lb {{ inventory_hostname }}
```

Pausing playbook execution with `wait_for`

You might also use `local_action` in the middle of a playbook to wait for a freshly-booted server or application to start listening on a particular port:

```
1 - name: Wait for webserver to start.
2   local_action:
3     module: wait_for
4     host: "{{ inventory_hostname }}"
5     port: "{{ webserver_port }}"
6     delay: 10
7     timeout: 300
8     state: started
```

The above task waits until `webserver_port` is open on `inventory_hostname`, as checked from the host running the Ansible playbook, with a 5-minute timeout (and 10 seconds before the first check, and between checks).

`wait_for` can be used to pause your playbook execution to wait for many different things:

- Using `host` and `port`, wait a maximum of `timeout` seconds for the port to be available (or not).
- Using `path` (and `search_regex` if desired), wait a maximum of `timeout` seconds for the file to be present (or absent).
- Using `host` and `port` and `drained` for the `state` parameter, check if a given port has drained all its active connections.
- Using `delay`, you can simply pause playbook execution for a given amount of time (in seconds).

Running an entire playbook locally

When running playbooks on the server or workstation where the tasks need to be run (e.g. self-provisioning), or when a playbook should be otherwise run on the same host as the `ansible-playbook` command is run, you can use `--connection=local` to speed up playbook execution by avoiding the SSH connection overhead.

As a quick example, here's a short playbook that you can run with the command `ansible-playbook test.yml --connection=local`:

```
1  ---
2  - hosts: 127.0.0.1
3    gather_facts: no
4
5    tasks:
6      - name: Check the current system date.
7        command: date
8        register: date
9
10     - name: Print the current system date.
11       debug: var=date.stdout
```

This playbook will run on localhost and output the current date in a debug message. It should run **very fast** (it took about .2 seconds on my Mac!) since it's running entirely over a local connection.

Running a playbook with `--connection=local` is also useful when you're either running a playbook with `--check` mode to verify configuration (e.g. on a cron job that emails you when changes are reported), or when testing playbooks on testing infrastructure (e.g. via Travis, Jenkins, or some other CI tool).

Prompts

Under rare circumstances, you may require the user to enter the value of a variable that will be used in the playbook. If the playbook requires a user's personal login information, or if you prompt for a version or other values that may change depending on who is running the playbook, or where it's being run, and if there's no other way this information can be configured (e.g. using environment variables, inventory variables, etc.), use `vars_prompt`.

As a simple example, you can request a user to enter a username and password that could be used to login to a network share:

```
1  ---
2  - hosts: all
3
4  vars_prompt:
5    - name: share_user
6      prompt: "What is your network username?"
7
8    - name: share_pass
9      prompt: "What is your network password?"
10     private: yes
```

Before Ansible runs the play, Ansible prompts the user for a username and password, the latter's input being hidden on the command line for security purposes.

There are a few special options you can add to prompts:

- `private`: If set to yes, the user's input will be hidden on the command line.
- `default`: You can set a default value for the prompt, to save time for the end user.
- `encrypt` / `confirm` / `salt_size`: These values can be set for passwords so you can verify the entry (the user will have to enter the password twice if `confirm` is set to yes), and encrypt it using a salt (with the specified size and crypt scheme). See Ansible's [Prompts⁶⁴](#) documentation for detailed information on prompted variable encryption.

Prompts are a simple way to gather user-specific information, but in most cases, you should avoid them unless absolutely necessary. It's preferable to use role or playbook variables, inventory variables, or even local environment variables, to maintain complete automation of the playbook run.

Tags

Tags allow you to run (or exclude) subsets of a playbook's tasks.

You can tag roles, included files, individual tasks, and even entire plays. The syntax is simple, and below are examples of the different ways you can add tags:

⁶⁴http://docs.ansible.com/playbooks_prompts.html#prompts

```
1  ---
2  # You can apply tags to an entire play.
3  - hosts: webservers
4  tags: deploy
5
6  roles:
7      # Tags applied to a role will be applied to the tasks in the role.
8      - { role: tomcat, tags: ['tomcat', 'app'] }
9
10 tasks:
11     - name: Notify on completion.
12         local_action:
13             module: osx_say
14             msg: "{{inventory_hostname}} is finished!"
15             voice: Zarvox
16         tags:
17             - notifications
18             - say
19
20     - include: foo.yml
21     tags: foo
```

Assuming we save the above playbook as `tags.yml`, you could run the command below to only run the `tomcat` role and the `Notify on completion` task:

```
1 $ ansible-playbook tags.yml --tags "tomcat,say"
```

If you want to exclude anything tagged with `notifications`, you can use `--skip-tags`.

```
1 $ ansible-playbook tags.yml --skip-tags "notifications"
```

This is incredibly handy if you have a decent tagging structure; when you want to only run a particular portion of a playbook, or one play in a series (or, alternatively, if you want to exclude a play or included tasks), then it's easy to do using `--tags` or `--skip-tags`.

There is one caveat when adding one or multiple tags using the `tags` option in a playbook: you can use the shorthand `tags: tagname` when adding just one tag, but if adding more than one tag, you have to use YAML's list syntax, for example:

```
# Shorthand list syntax.  
tags: ['one', 'two', 'three']  
  
# Explicit list syntax.  
tags:  
- one  
- two  
- three  
  
# Non-working example.  
tags: one, two, three
```

In general, I tend to use tags for larger playbooks, especially with individual roles and plays, but unless I'm debugging a set of tasks, I generally avoid adding tags to individual tasks or includes (not adding tags everywhere reduces visual clutter). You will need to find a tagging style that suits your needs and lets you run (or *not* run) the specific parts of your playbooks you desire.

Summary

Playbooks are Ansible's primary means of automating infrastructure management. After reading this chapter, you should know how to use (and hopefully not abuse!) variables, inventories, handlers, conditionals, tags, and more.

The more you understand the fundamental components of a playbook, the more efficient you will be at building and expanding your infrastructure with Ansible.

/ Men have become the tools of their \
\ tools. (Henry David Thoreau) /

\ ^__^
 \ (oo)_____
 ()\)\/\
 ||----w |
 || ||

Chapter 6 - Playbook Organization - Roles and Includes

So far, we've used fairly straightforward examples in this book. Most examples are created for a particular server, and are in one long playbook.

Ansible is flexible when it comes to organizing tasks in more efficient ways so you can make playbooks more maintainable, reusable, and powerful. We'll look at two ways to split up tasks more efficiently using includes and roles, and we'll explore Ansible Galaxy, a repository of some community-maintained roles that help configure common packages and applications.

Includes

We've already seen one of the most basic ways of including other files in Chapter 4, when `vars_files` was used to place variables into a separate `vars.yml` file instead of inline with the playbook:

```
- hosts: all  
  
  vars_files:  
    - vars.yml
```

Tasks can easily be included in a similar way. In the `tasks:` section of your playbook, you can add `include` directives like so:

```
tasks:  
  - include: included-playbook.yml
```

Just like with variable include files, tasks are formatted in a flat list in the included file. As an example, the `included-playbook.yml` could look like this:

```
---
```

- name: Add profile info for user.
 - copy:
 - src: example_profile
 - dest: "/home/{{ username }}/.profile"
 - owner: "{{ username }}"
 - group: "{{ username }}"
 - mode: 0744
- name: Add private keys for user.
 - copy:
 - src: "{{ item.src }}"
 - dest: "/home/.ssh/{{ item.dest }}"
 - owner: "{{ username }}"
 - group: "{{ username }}"
 - mode: 0600
 - with_items: ssh_private_keys
- name: Restart example service.
 - service: name=example state=restarted

In this case, you'd probably want to name the file `user-config.yml`, since it's used to configure a user account and restart some service. Now, in this and any other playbook that provisions or configures a server, if you want to configure a particular user's account, add the following in your playbook's tasks section:

```
- include: example-app-config.yml
```

We used `{{ username }}` and `{{ ssh_private_keys }}` variables in this include file instead of hard-coded values so we could make this include file reusable. You could define the variables in your playbook's inline variables or an included variables file, but Ansible also lets you pass variables directly into includes using normal YAML syntax. For example:

```
- { include: user-config.yml, username: johndoe, ssh_private_keys: [] }
- { include: user-config.yml, username: janedoe, ssh_private_keys: [] }
```

To make the syntax more readable, you can use structured variables, like so:

```
- include: user-config.yml
  vars:
    username: johndoe
    ssh_private_keys:
      - { src: /path/to/johndoe/key1, dest: id_rsa }
      - { src: /path/to/johndoe/key2, dest: id_rsa_2 }
- include: user-config.yml
  vars:
    username: janedoe
    ssh_private_keys:
      - { src: /path/to/janedoe/key1, dest: id_rsa }
      - { src: /path/to/janedoe/key2, dest: id_rsa_2 }
```

Include files can even include other files, so you could have something like the following:

```
tasks:
  - include: user-config.yml
```

inside `user-config.yml`

```
- include: ssh-setup.yml
```

Handler includes

Handlers can be included just like tasks, within a playbook's `handlers` section. For example:

```
handlers:
  - include: included-handlers.yml
```

This can be helpful in limiting the noise in your main playbook, since handlers are usually used for things like restarting services or loading a configuration, and can distract from the playbook's primary purpose.

Playbook includes

Playbooks can even be included in other playbooks, using the same `include` syntax in the top level of your playbook. For example, if you have two playbooks—one to set up your webservers (`web.yml`), and one to set up your database servers (`db.yml`), you could use the following playbook to run both at the same time:

```
- hosts: all
  remote_user: root

  tasks:
  ...

- include: web.yml
- include: db.yml
```

This way, you can create playbooks to configure all the servers in your infrastructure, then create a master playbook that includes each of the individual playbooks. When you want to initialize your infrastructure, make changes across your entire fleet of servers, or check to make sure their configuration matches your playbook definitions, you can run one `ansible-playbook` command!

Complete includes example

What if I told you we could remake the 137-line Drupal LAMP server playbook from Chapter 4 in just 21 lines? With includes, it's easy; just break out each of the sets of tasks into their own include files, and you'll end up with a main playbook like this:

```
1  ---
2  - hosts: all
3
4  vars_files:
5    - vars.yml
6
7  pre_tasks:
8    - name: Update apt cache if needed.
9      apt: update_cache=yes cache_valid_time=3600
10
11 handlers:
12   - include: handlers/handlers.yml
13
14 tasks:
15   - include: tasks/common.yml
16   - include: tasks/apache.yml
17   - include: tasks/php.yml
18   - include: tasks/mysql.yml
19   - include: tasks/composer.yml
20   - include: tasks/drush.yml
21   - include: tasks/drupal.yml
```

All you need to do is create two new folders in the same folder where you saved the `Drupal playbook.yml` file, `handlers` and `tasks`, then create files inside for each section of the playbook.

For example, inside `handlers/handlers.yml`, you'd have:

```
1 ---  
2 - name: restart apache  
3   service: name=apache2 state=restarted
```

And inside `tasks/drush.yml`:

```
1 ---  
2 - name: Check out drush master branch.  
3   git:  
4     repo: https://github.com/drush-ops/drush.git  
5     dest: /opt/drush  
6  
7 - name: Install Drush dependencies with Composer."  
8   shell: >  
9     /usr/local/bin/composer install  
10    chdir=/opt/drush  
11    creates=/opt/drush/vendor/autoload.php  
12  
13 - name: Create drush bin symlink.  
14   file:  
15     src: /opt/drush/drush  
16     dest: /usr/local/bin/drush  
17     state: link
```

Separating all the tasks into separate includes files means you'll have more files to manage for your playbook, but it helps keep the main playbook more compact. It's easier to see all the installation and configuration steps the playbook contains, and it separates tasks into individual, maintainable groupings. Instead of having to browse one playbook with twenty-three separate tasks, you now maintain eight included files with two to five tasks, each.

It's much easier to maintain small groupings of related tasks than one long playbook. However, there's no reason to try to *start* writing a playbook with lots of individual includes. Most of the time, it's best to start with a monolithic playbook while you're working on the setup and configuration details, then move sets of tasks out to included files after you start seeing logical groupings.

You can also use tags (demonstrated in the previous chapter) to limit the playbook run to a certain include file. Using the above example, if you wanted to add a 'drush' tag to the included drush file (so you could run `ansible-playbook playbook.yml --tags=drush` and only run the drush tasks), you can change line 20 to the following:

```
20 - include: tasks/drush.yml tags=drush
```



You can find the entire example Drupal LAMP server playbook using include files in this book's code repository at [https://github.com/geerlingguy/ansible-for-devops⁶⁵](https://github.com/geerlingguy/ansible-for-devops), in the includes directory.



You can't use variables for task include file names (like you could with `include_vars` directives, e.g. `include_vars: "{{ ansible_os_family }}.yml"` as a task, or with `vars_files`). There's usually a better way than conditional task includes to accomplish conditional task inclusion using a different playbook structure, or roles, which we will discuss next.

Roles

Including playbooks inside other playbooks makes your playbook organization a little more sane, but once you start wrapping up your entire infrastructure's configuration in playbooks, you might end up with something resembling Russian nesting dolls.

Wouldn't it be nice if there were a way to take bits of related configuration, and package them together nicely? Additionally, what if we could take these packages (often configuring the same thing on many different servers) and make them flexible so that we can use the same package throughout our infrastructure, with slightly different settings on individual servers or groups of servers?

Ansible Roles can do all that and more!

Let's dive into what makes an Ansible role by taking one of the playbook examples from Chapter 4 and splitting it into a more flexible structure using roles.

Role scaffolding

Instead of requiring you to explicitly include certain files and playbooks in a role, Ansible automatically includes any `main.yml` files inside specific directories that make up the role.

There are only two directories required to make a working Ansible role:

```
role_name/
  meta/
  tasks/
```

If you create a directory structure like the one shown above, with a `main.yml` file in each directory, Ansible will run all the tasks defined in `tasks/main.yml` if you call the role from your playbook using the following syntax:

⁶⁵<https://github.com/geerlingguy/ansible-for-devops>

```
1  ---
2  - hosts: all
3  roles:
4    - role_name
```

Your roles can live in a couple different places: the default global Ansible role path (configurable in `/etc/ansible/ansible.cfg`), or a `roles` folder in the same directory as your main playbook file.



Another simple way to build the scaffolding for a role is to use the command: `ansible-galaxy init role_name`. Running this command creates an example role in the current working directory, which you can modify to suit your needs. Using the `init` command also ensures the role is structured correctly in case you want to someday contribute the role to Ansible Galaxy.

Building your first role

Let's clean up the Node.js server example from Chapter four, and break out one of the main parts of the configuration—installing Node.js and any required npm modules.

Create a `roles` folder in the same directory as the main `playbook.yml` file like we created in Chapter 4's first example. Inside the `roles` folder, create a new folder: `nodejs` (which will be our role's name). Create two folders inside the `nodejs` role directory: `meta` and `tasks`.

Inside the `meta` folder, add a simple `main.yml` file with the following contents:

```
1  ---
2  dependencies: []
```

The meta information for your role is defined in this file. In basic examples and simple roles, you just need to list any role dependencies (other roles that are required to be run before the current role can do its work). You can add more to this file to describe your role to Ansible and to Ansible Galaxy, but we'll dive deeper into meta information later. For now, save the file and head over to the `tasks` folder.

Create a `main.yml` file in this folder, and add the following contents (basically copying and pasting the configuration from the Chapter 4 example):

```

1  ---
2  - name: Install Node.js (npm plus all its dependencies).
3    yum: name=npn state=present enablerepo=epel
4
5  - name: Install forever module (to run our Node.js app).
6    npm: name=forever global=yes state=latest

```

The Node.js directory structure should now look like the following:

```

1 nodejs-app/
2   app/
3     app.js
4     package.json
5   playbook.yml
6   roles/
7     nodejs/
8       meta/
9         main.yml
10    tasks/
11      main.yml

```

You now have a complete Ansible role that you can use in your node.js server configuration playbook. Delete the Node.js app installation lines from `playbook.yml`, and reformat the playbook so the other tasks run first (in a `pre_tasks:` section instead of `tasks:`), then the role, then the rest of the tasks (in the main `tasks:` section). Something like:

```

pre_tasks:
  # EPEL/GPG setup, firewall configuration...

roles:
  - nodejs

tasks:
  # Node.js app deployment tasks...

```



You can view the full example of this playbook in the [ansible-for-devops code repository⁶⁶](https://github.com/geerlingguy/ansible-for-devops/blob/master/nodejs-role/).

Once you finish reformatting the main playbook, everything will run exactly the same during an `ansible-playbook` run, with the exception of the tasks inside the `nodejs` role being prefixed with `nodejs | [Task name here]`.

⁶⁶<https://github.com/geerlingguy/ansible-for-devops/blob/master/nodejs-role/>

This little bit of extra data shown during playbook runs is useful because it automatically prefixes tasks with the role that provides them, without you having to add in descriptions as part of the name values of the tasks.

Our role isn't all that helpful at this point, though, because it still does only one thing, and it's not really flexible enough to be used on other servers that might need different Node.js modules to be installed.

More flexibility with role vars and defaults

To make our role more flexible, we can make it use a list of npm modules instead of a hardcoded value, then allow playbooks using the role to provide their own module list variable to override our role's default list.

When running a role's tasks, Ansible picks up variables defined in a role's `vars/main.yml` file and `defaults/main.yml` (I'll get to the differences between the two later), but will allow your playbooks to override the defaults or other role-provided variables if you want.

Modify the `tasks/main.yml` file to use a list variable and iterate through the list to install as many packages as your playbook wants:

```
1  ---
2  - name: Install Node.js (npm plus all its dependencies).
3    yum: name=npn state=present enablerepo=epel
4
5  - name: Install npm modules required by our app.
6    npm: name={{ item }} global=yes state=latest
7    with_items: node_npm_modules
```

Let's provide a sane default for the new `node_npm_modules` variable in `defaults/main.yml`:

```
1  ---
2  node_npm_modules:
3    - forever
```

Now, if you run the playbook as-is, it will still do the exact same thing—install the `forever` module. But since the role is more flexible, we could create a new playbook like our first, but add a variable (either in a `vars` section or in an included file via `vars_files`) to override the default, like so:

```

1 node_npm_modules:
2   - forever
3   - async
4   - request

```

When you run the playbook with this custom variable (we didn't change **anything** with our `nodejs` role), all three of the above npm modules will be installed.

Hopefully you're beginning to see how this can be powerful!

Imagine if you had a playbook structure like:

```

1 ---
2 - hosts: appservers
3   roles:
4     - yum-repo-setup
5     - firewall
6     - nodejs
7     - app-deploy

```

Each one of the roles lives in its own isolated world, and can be shared with other servers and groups of servers in your infrastructure.

- A `yum-repo-setup` role could enable certain repositories and import their GPG keys.
- A `firewall` role could have per-server or per-inventory-group options for ports and services to allow or deny.
- An `app-deploy` role could deploy your app to a directory (configurable per-server) and set certain app options per-server or per-group.

These things are easy to manage when you have small bits of functionality separated into different roles. Instead of managing 100+ lines of playbook tasks, and manually prefixing every `name:` with something like “Common |” or “App Deploy |”, you now manage a few roles with 10-20 lines of YAML each.

On top of that, when you're building your main playbooks, they can be extremely simple (like the above example), enabling you to see **everything** being configured and deployed on a particular server without scrolling through dozens of included playbook files and hundreds of tasks.



Variable precedence: Note that Ansible handles variables placed in included files in `defaults` with less precedence than those placed in `vars`. If you have certain variables you need to allow hosts/playbooks to easily override, you should probably put them into `defaults`. If they are common variables that should almost always be the values defined in your role, put them into `vars`. For more on variable precedence, see the aptly-named “Variable Precedence” section in the previous chapter.

Other role parts: handlers, files, and templates

Handlers

In one of the prior examples, we introduced handlers—tasks that could be called via the `notify` option after any playbook task resulted in a change—and an example handler for restarting Apache was given:

```
1 handlers:
2   - name: restart apache
3     service: name=apache2 state=restarted
```

In Ansible roles, handlers are first-class citizens, alongside tasks, variables, and other configuration. You can store handlers directly inside a `main.yml` file inside a role's `handlers` directory. So if we had a role for Apache configuration, our `handlers/main.yml` file could look like this:

```
1 ---
2 - name: restart apache
3   command: service apache2 restart
```

You can call handlers defined in a role's `handlers` folder just like those included directly in your playbooks (e.g. `notify: restart apache`).

Files and Templates

For the following examples, let's assume our role is structured with files and templates inside `files` and `templates` directories, respectively:

```
1 roles/
2   example/
3     files/
4       example.conf
5     meta/
6       main.yml
7     templates/
8       example.xml.j2
9     tasks/
10    main.yml
```

when copying a file directly to the server, add the filename or the full path from within a role's `files` directory, like so:

```
- name: Copy configuration file to server directly.  
  copy: >  
    src=example.conf  
    dest=/etc/myapp/example.conf  
    mode=644
```

Similarly, when specifying a template, add the filename or the full path from within a role's `templates` directory, like so:

```
- name: Copy configuration file to server using a template.  
  template: >  
    src=example.xml.j2  
    dest=/etc/myapp/example.xml  
    mode=644
```

The `copy` module copies files from within the module's `files` folder, and the `template` module runs given template files through the Jinja2 templating engine, merging in any variables available during your playbook run before copying the file to the server.

Organizing more complex and cross-platform roles

For simple package installation and configuration roles, you can get by with placing all tasks, variables, and handlers directly in the respective `main.yml` file Ansible automatically loads. But you can also *include* other files from within a role's `main.yml` files if needed.

As a rule of thumb, I keep my playbook and role task files under 100 lines of YAML if at all possible. It's easier to keep the entire set of tasks in my head while making changes or fixing bugs. If I start nearing that limit, I usually split the tasks into logical groupings, and include files from the `main.yml` file.

Let's take a look at the way my `geerlingguy.apache` role is set up (it's [available on Ansible Galaxy](#)⁶⁷ and can be downloaded to your roles directory with the command `ansible-galaxy install geerlingguy.apache`; we'll discuss Ansible Galaxy itself later).

Initially, the role's main `tasks/main.yml` file looked something like the following (generally speaking):

⁶⁷<https://galaxy.ansible.com/list#/roles/428>

```
1 - name: Ensure Apache is installed (via apt).
2
3 - name: Configure Apache with lineinfile.
4
5 - name: Enable Apache modules.
```

Soon after creating the role, though, I wanted to make the role work with both Debian and RedHat hosts. I could've added two sets of tasks in the `main.yml` file, resulting in twice the number of tasks and a bunch of extra `when` statements:

```
1 - name: Ensure Apache is installed (via apt).
2   when: ansible_os_family == 'Debian'
3
4 - name: Ensure Apache is installed (via yum).
5   when: ansible_os_family == 'RedHat'
6
7 - name: Configure Apache with lineinfile (Debian).
8   when: ansible_os_family == 'Debian'
9
10 - name: Configure Apache with lineinfile (Redhat).
11   when: ansible_os_family == 'RedHat'
12
13 - name: Enable Apache modules (Debian).
14   when: ansible_os_family == 'Debian'
15
16 - name: Other OS-agnostic tasks...
```

If I had gone this route, and continued with the rest of the playbook tasks in one file, I would've quickly surpassed my informal 100-line limit. So I chose to use includes in my main tasks file:

```
1 - name: Include OS-specific variables.
2   include_vars: "{{ ansible_os_family }}.yml"
3
4 - include: setup-RedHat.yml
5   when: ansible_os_family == 'RedHat'
6
7 - include: setup-Debian.yml
8   when: ansible_os_family == 'Debian'
9
10 - name: Other OS-agnostic tasks...
```

Two important things to notice about this style of distribution-specific inclusion:

1. When including vars files (with `include_vars`), you can actually **use variables in the name of the file** This is handy in many situations, and here we're including a vars file in the format `distribution_name.yml`. For our purposes, since the role will be used on Debian and RedHat-based hosts, we can create `Debian.yml` and `RedHat.yml` files in our role's `defaults` and `vars` folders, and put distribution-specific variables there.
2. When including playbook files (with `include`), you can't use variables in the name of the file, but you can do the next best thing: include the files by name explicitly, and use a condition to tell Ansible whether to run the tasks inside (the `when` condition will be applied to every task inside the included playbook).

After setting things up this way, I put RedHat and CentOS-specific tasks (like `yum` tasks) into `tasks/setup-RedHat.yml`, and Debian and Ubuntu-specific tasks (like `apt` tasks) into `tasks/setup-Debian.yml`. There are other ways of making roles work cross-platform, but using distribution-specific variables files and included playbooks is one of the simplest.

Now this Apache role can be used across different distributions, and with clever usage of variables in tasks and in configuration templates, it can be used in a wide variety of infrastructure that needs Apache installed.

Ansible Galaxy

Ansible roles are powerful and flexible; they allow you to encapsulate sets of configuration and deployable units of playbooks, variables, templates, and other files, so you can easily reuse them across different servers.

It's annoying to have to start from scratch every time, though; wouldn't it be better if people could share roles for commonly-installed applications and services?

Enter [Ansible Galaxy](#)⁶⁸.

Ansible Galaxy, or just 'Galaxy', is a repository of community-contributed roles for common Ansible content. There are already hundreds of roles available which can configure and deploy common applications, and they're all available through the `ansible-galaxy` command, introduced in Ansible 1.4.2.

Galaxy offers the ability to add, download, and rate roles. With an account, you can contribute your own roles or rate others' roles (though you don't need an account to use roles).

Getting roles from Galaxy

One of the primary functions of the `ansible-galaxy` command is retrieving roles from Galaxy. Roles must be downloaded before they can be used in playbooks.

Remember the basic LAMP (Linux, Apache, MySQL and PHP) server we installed earlier in the book? Let's create it again, but this time, using a few roles from Galaxy:

⁶⁸<https://galaxy.ansible.com/>

```
$ ansible-galaxy install geerlingguy.apache geerlingguy.mysql geerlingguy.php
```



The latest version or a role will be downloaded if no version is specified. To specify a version, add the version after the role name, for example: `$ ansible-galaxy install geerlingguy.apache,1.0.0.`



Ansible Galaxy is still evolving rapidly, and has seen many improvements. There are a few areas where Galaxy could use some improvement (like browsing for roles by Operating System in the online interface, or automatically downloading roles that are included in playbooks), but most of these little bugs or rough spots will be fixed in time. Please check Ansible Galaxy's [About⁶⁹](#) page and stay tuned to Ansible's blog for the latest updates.

Using role requirements files to manage dependencies

If your infrastructure configuration requires five, ten, fifteen or more Ansible roles, installing them all via `ansible-galaxy install` commands can get exhausting. Additionally, if you host roles internally (e.g. via an internal Git or Mercurial repository), you can't install the roles through Ansible Galaxy. You can, however, pass the `ansible-galaxy` command a "requirements" file to automatically download all the included dependencies, whether they exist on Ansible Galaxy or in some other repository.

There are two syntaxes you can use:

1. Plain text files, which end in `.txt` and are similar to Python `pip` requirements files.
2. YAML files, which end in `.yml` and use a more structured and expressive syntax.

The first format works in very basic situations. Define each required role on a single line, with an optional version number after the role (the same basic syntax you would use with the `ansible-galaxy install` command), like this:

```
1  geerlingguy.apache,1.3.1
2  geerlingguy.mysql
3  geerlingguy.php,1.4.1
```

Specify one Ansible Galaxy role per line either by itself, or with a particular version number, and then run `ansible-galaxy install -r requirements.txt`. Ansible will download all the roles from Galaxy into your local roles path.

The second syntax is much more expressive, and allows you to install roles from other sources, like GitHub, an HTTP download, BitBucket, or your own repository. It also allows you to specify the path into which the roles should be downloaded. An example `requirements.yml` file looks like this:

⁶⁹<https://galaxy.ansible.com/intro>

```

1 # From Ansible Galaxy, like the earlier requirements.txt example.
2 - src: geerlingguy.firewall
3
4 # From GitHub, into a particular path, with a custom name and version.
5 - src: https://github.com/geerlingguy/ansible-role-passenger
6   path: /etc/ansible/roles/
7   name: passenger
8   version: 1.0.2
9
10 # From a web server, with a custom name.
11 - src: https://www.example.com/ansible/roles/my-role-name.tar.gz
12   name: my-role

```

Installing roles defined in this file is similar to the .txt example: `ansible-galaxy install -r requirements.yml`. For more documentation on Ansible requirements files, see the official documentation: [Advanced Control over Role Requirements Files⁷⁰](#).

A LAMP server in six lines of YAML

With the Apache, MySQL, and PHP roles installed, we can quickly create a LAMP server. This example assumes you already have a CentOS-based linux VM or server booted and can connect to it or run Ansible as a provisioner via Vagrant on it, and that you've run the `ansible-galaxy install` command above to download the required roles.

First, create an Ansible playbook named `lamp.yml` with the following contents:

```

1 ---
2 - hosts: all
3   roles:
4     - geerlingguy.mysql
5     - geerlingguy.apache
6     - geerlingguy.php

```

Now, run the playbook against a host:

```
$ ansible-playbook -i path/to/custom-inventory lamp.yml
```

After a few minutes, an entire LAMP server should be set up and running. If you add in a few variables, you can configure virtualhosts, PHP configuration options, MySQL server settings, etc.

⁷⁰<http://docs.ansible.com/galaxy.html#advanced-control-over-role-requirements-files>

We've effectively reduced about thirty lines of YAML (from previous examples dealing with LAMP or LAMP-like servers) down to three. Obviously, the roles have extra code in them, but the power here is in abstraction. Since most companies have many servers using similar software, but with slightly different configurations, having centralized, flexible roles saves a lot of repetition.

You could think of Galaxy roles as glorified packages; they not only install software, but they configure it *exactly* how you want it, every time, with minimal adjustment. Additionally, many of these roles work across different flavors of Linux and UNIX, so you have better configuration portability!

A Solr server in six lines of YAML

Let's grab a few more roles and build an Apache Solr search server, which requires Java and Apache Tomcat to be installed and configured.

```
$ ansible-galaxy install gearlingguy.java gearlingguy.tomcat6 gearlingguy.solr
```

Then create a playbook named `solr.yml` with the following contents:

```
1  ---
2  - hosts: all
3    roles:
4      - gearlingguy.java
5      - gearlingguy.tomcat6
6      - gearlingguy.solr
```

Now we have a fully-functional Solr server, and we could add some variables to configure it exactly how we want, by using a non-default port, or changing the memory allocation for Tomcat6.

I could've also left out the `java` and `tomcat6` roles, since they'll be automatically picked up during installation of the `gearlingguy.solr` role (they're listed in the `solr` role's dependencies).

A role's page on the Ansible Galaxy website highlights available variables for setting things like what version of Solr to install, where to install it, etc. For an example, view the [gearlingguy.solr Galaxy page⁷¹](#).

You can build a wide variety of servers with minimal effort with existing contributed roles on Galaxy. Instead of having to maintain lengthy playbooks and roles unique to each server, Galaxy lets you build a list of the required roles, and a few variables that set up the servers with the proper versions and paths. Configuration management with Ansible Galaxy becomes *true* configuration management—you get to spend more time managing your server's configuration, and less time on packaging and building individual services!

⁷¹<https://galaxy.ansible.com/list#/roles/445>

Helpful Galaxy commands

Some other helpful `ansible-galaxy` commands you might use from time to time:

- `ansible-galaxy list` displays a list of installed roles, with version numbers
- `ansible-galaxy remove [role]` removes an installed role
- `ansible-galaxy init` can be used to create a role template suitable for submission to Ansible Galaxy

You can configure the default path where Ansible roles will be downloaded by editing your `ansible.cfg` configuration file (normally located in `/etc/ansible/ansible.cfg`), and setting a `roles_path` in the `[defaults]` section.

Contributing to Ansible Galaxy

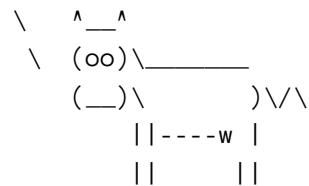
If you've been working on some useful Ansible roles, and you'd like to share them with others, all you need to do is make sure they follow Ansible Galaxy's basic template (especially within the `meta/main.yml` and `README.md` files). To get started, use `ansible-galaxy init` to generate a basic Galaxy template, and make your own role match the Galaxy template's structure.

Then push your role up to a new project on GitHub (I usually name my Galaxy roles like `ansible-role-[rolename]`, so I can easily see them when browsing my repos on GitHub), and add a new role while logged into `galaxy.ansible.com`.

Summary

Using includes and Ansible roles organizes Playbooks and makes them maintainable. This chapter introduced different ways of using `include`, the power and flexible structure of roles, and how you can utilize Ansible Galaxy, the community repository of configurable Ansible roles that do just about anything.

```
/ When the only tool you own is a hammer, \
| every problem begins to resemble a      |
\ nail. (Abraham Maslow)                  /
```



Chapter 7 - Inventories

Earlier in the book, a basic inventory file example was given (see Chapter 1's [basic inventory file example](#)). For the simplest of purposes, an inventory file at the default location (`/etc/ansible/hosts`) will suffice to describe to Ansible how to reach the servers you want to manage.

Later, a slightly more involved inventory file was introduced (see Chapter 3's [inventory file for multiple servers](#)), which allowed us to tell Ansible about multiple servers, and even group them into role-related groups, so we could run certain playbooks against certain groups.

Let's jump back to a basic inventory file example and build from there:

```
1 # Inventory file at /etc/ansible/hosts
2
3 # Groups are defined using square brackets (e.g. [groupname]). Each server
4 # in the group is defined on its own line.
5 [myapp]
6 www.myapp.com
```

If you want to run an ansible playbook on all the `myapp` servers in this inventory (so far, just one, `www.myapp.com`), you can set up the playbook like so:

```
---
- hosts: myapp

  tasks:
    [...]
```

If you want to run an ad-hoc command against all the `myapp` servers in the inventory, you can run a command like so:

```
# Use ansible to check memory usage on all the myapp servers.
$ ansible myapp -a "free -m"
```

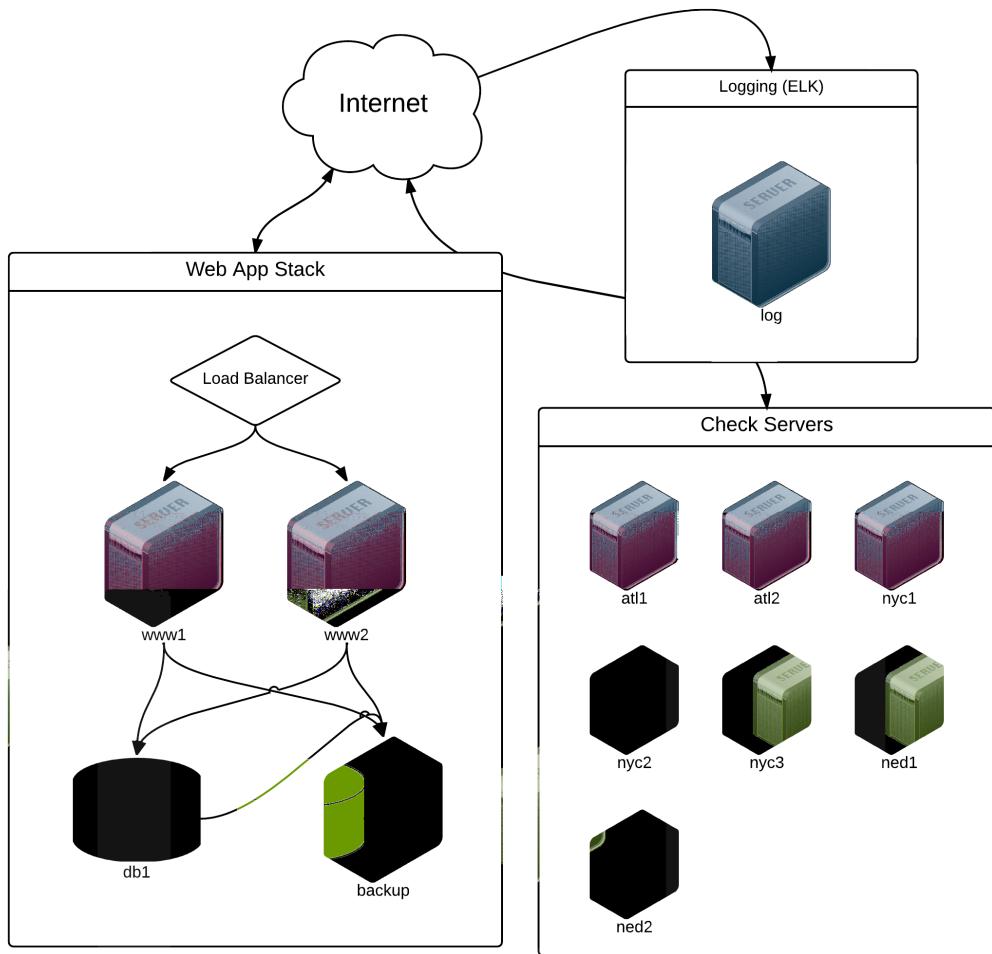
A real-world web application server inventory

The example above might be adequate for single-server services and tiny apps or websites, but most real-world applications require many more servers, and usually separate servers per application concern (database, caching, application, queuing, etc.). Let's take a look at a real-world inventory file for a small web application that monitors server uptime, [Server Check.in](#)⁷².

⁷²<https://servercheck.in/>

```
1 # Individual Server Check.in servers.
2 [servercheck-web]
3 www1.servercheck.in
4 www2.servercheck.in
5
6 [servercheck-web:vars]
7 ansible_ssh_user=servercheck_svc
8
9 [servercheck-db]
10 db1.servercheck.in
11
12 [servercheck-log]
13 log.servercheck.in
14
15 [servercheck-backup]
16 backup.servercheck.in
17
18 [servercheck-nodejs]
19 at11.servercheck.in
20 at12.servercheck.in
21 nyc1.servercheck.in
22 nyc2.servercheck.in
23 nyc3.servercheck.in
24 ned1.servercheck.in
25 ned2.servercheck.in
26
27 [servercheck-nodejs:vars]
28 ansible_ssh_user=servercheck_svc
29 foo=bar
30
31 # Server Check.in distribution-based groups.
32 [centos:children]
33 servercheck-web
34 servercheck-db
35 servercheck-nodejs
36 servercheck-backup
37
38 [ubuntu:children]
39 servercheck-log
```

This inventory may look a little overwhelming at first, but if you break it apart into simple groupings (web app servers, database servers, logging server, and node.js app servers), it describes a straightforward architecture.



Server Check.in Infrastructure.

Lines 1-29 describe a few groups of servers (some with only one server), so playbooks and `ansible` commands can refer to the group by name. Lines 6-7 and 27-29 set variables that will apply only to the servers in the group (e.g. variables below `[servercheck-nodejs:vars]` will only apply to the servers in the `servercheck-nodejs` group).

Lines 31-39 describe groups of groups (using `groupname:children` to describe ‘child’ groups) that allow for some helpful abstractions.

Describing infrastructure in such a way affords a lot of flexibility when using Ansible. Consider the task of patching a vulnerability on all your CentOS servers; instead of having to log into each of the servers, or even having to run an `ansible` command against all the groups, using the above structure allows you to easily run an `ansible` command or playbook against all `centos` servers.

As an example, when the [Shellshock](#)⁷³ vulnerability was disclosed in 2014, patched bash packages were released for all the major distributions within hours. To update all the Server Check.in servers,

⁷³[https://en.wikipedia.org/wiki/Shellshock_\(software_bug\)](https://en.wikipedia.org/wiki/Shellshock_(software_bug))

all that was needed was:

```
$ ansible centos -m yum -a "name=bash state=latest"
```

You could even go further and create a small playbook that would patch the vulnerability, then run tests to make sure the vulnerability was no longer present, as illustrated in [this playbook](#)⁷⁴. This would also allow you to run the playbook in check mode or run it through a continuous integration system to verify the fix works in a non-prod environment.

This infrastructure inventory is also nice in that you could create a top-level playbook that runs certain roles or tasks against all your infrastructure, others against all servers of a certain Linux flavor, and another against all servers in your entire infrastructure.

Consider, for example, this example master playbook to completely configure all the servers:

```
1  ---
2  # Set up basic, standardized components across all servers.
3  - hosts: all
4    sudo: true
5    roles:
6      - security
7      - logging
8      - firewall
9
10 # Configure web application servers.
11 - hosts: servercheck-web
12   roles:
13     - nginx
14     - php
15     - servercheck-web
16
17 # Configure database servers.
18 - hosts: servercheck-db
19   roles:
20     - pgsql
21     - db-tuning
22
23 # Configure logging server.
24 - hosts: servercheck-log
25   roles:
26     - java
27     - elasticsearch
```

⁷⁴https://raymii.org/s/articles/Patch_CVE-2014-6271_Shellshock_with_Ansible.html

```
28      - logstash
29      - kibana
30
31 # Configure backup server.
32 - hosts: servercheck-backup
33   roles:
34     - backup
35
36 # Configure Node.js application servers.
37 - hosts: servercheck-nodejs
38   roles:
39     - servercheck-node
```

There are a number of different ways you can structure your infrastructure-management playbooks and roles, and we'll explore some in later chapters, but for a simple infrastructure, something like this is adequate and maintainable.

Non-prod environments, separate inventory files

Using the above playbook and the globally-configured Ansible inventory file is great for your production infrastructure, but what happens when you want to configure a separate but similar infrastructure for, say a development or user certification environment?

In this case, it's easiest to use individual inventory files, rather than the central, locally-managed Ansible inventory file. For typical team-managed infrastructure, I would recommend including an inventory file for each environment in the same version-controlled repository as your Ansible playbooks, perhaps within an 'inventories' directory.

For example, I could take the entire contents of `/etc/ansible/hosts` above, and stash that inside an inventory file named `inventory-prod`, then duplicate it, changing server names where appropriate (e.g. the `[servercheck-web]` group would only have `www-dev1.servercheck.in` for the development environment), and naming the files for the environments:

```
servercheck/
  inventories/
    inventory-prod
    inventory-cert
    inventory-dev
  playbook.yml
```

Now, when running `playbook.yml` to configure the development infrastructure, I would pass in the path to the dev inventory (assuming my current working directory is `servercheck/`):

```
$ ansible-playbook playbook.yml -i inventory-dev
```

Using inventory variables (which will be explored further), and well-constructed roles and/or tasks that use the variables effectively, you could architect your entire infrastructure, with environment-specific configurations, by changing some things in your inventory files.

Inventory variables

Chapter 5 introduced basic methods of managing variables for individual hosts or groups of hosts through your inventory in the [inventory variables](#) section, but it's worth exploring the different ways of defining and overriding variables through inventory here.

For extremely simple use cases—usually when you need to define one or two connection-related variables (like `ansible_ssh_user` or `ansible_ssh_port`)—you can place variables directly inside an inventory file.

Assuming we have a standalone inventory file for a basic web application, here are some examples of variable definition inside the file:

```
1 [www]
2 # You can define host-specific variables inline with the host.
3 www1.example.com ansible_ssh_user=johndoe
4 www2.example.com
5
6 [db]
7 db1.example.com
8 db2.example.com
9
10 # You can add a '[group:vars]' heading to create variables that will apply
11 # to an entire inventory group.
12 [db:vars]
13 ansible_ssh_port=5222
14 database_performance_mode=true
```

It's usually better to avoid throwing too many variables inside static inventory files, because not only are these variables typically less visible, they are also mixed in with your architecture definition. Especially for host-specific vars (which appear on one long line per host), this is an unmaintainable, low-visibility approach to host and group-specific variables.

Fortunately, Ansible provides a more flexible way of declaring host and group variables.

host_vars

For [Hosted Apache Solr](#)⁷⁵, different servers in a `solr` group have different memory requirements. The simplest way to tell Ansible to override a default variable in our Ansible playbook (in this case, the `tomcat_xmx` variable) is to use a `host_vars` directory (which can be placed either in the same location as your inventory file, or in a playbook's root directory), and place a YAML file named after the host which needs the overridden variable.

As an illustration of the use of `host_vars`, we'll assume we have the following directory layout:

```
hostedapachesolr/
  host_vars/
    nyc1.hostedapachesolr.com
  inventory/
    hosts
    main.yml
```

The `inventory/hosts` file contains a simple definition of all the servers by group:

```
1 [solr]
2 nyc1.hostedapachesolr.com
3 nyc2.hostedapachesolr.com
4 jap1.hostedapachesolr.com
5 ...
6
7 [log]
8 log.hostedapachesolr.com
```

Ansible will search for a file at either `hostedapachesolr/host_vars/nyc1.hostedapachesolr.com` or `hostedapachesolr/inventory/host_vars/nyc1.hostedapachesolr.com`, and if there are any variables defined in the file (in YAML format), those variables will override all other playbook and role variables and gathered facts, *only for the single host*.

The `nyc1.hostedapachesolr.com` `host_vars` file looks like:

```
1 ---
2 tomcat_xmx: "1024m"
```

The default for `tomcat_xmx` may normally be `640m`, but when Ansible runs a playbook against `nyc1.hostedapachesolr.com`, the value of `tomcat_xmx` will be `1024m` instead.

Overriding host variables with `host_vars` is much more maintainable than doing so directly in static inventory files, and also provides greater visibility into what hosts are getting what overrides.

⁷⁵<https://hostedapachesolr.com/>

group_vars

Much like `host_vars`, Ansible will automatically load any files named after inventory groups in a `group_vars` directory placed inside the playbook or inventory file's location.

Using the same example as above, we'll override one particular variable for an entire group of servers. First, we add a `group_vars` directory with a file named after the group needing the overridden variable:

```
hostedapachesolr/
  group_vars/
    solr
  host_vars/
    nyc1.hostedapachesolr.com
  inventory/
    hosts
  main.yml
```

Then, inside `group_vars/solr`, use YAML to define a list of variables that will be applied to servers in the `solr` group:

```
1  ---
2  do_something_amazing=true
3  foo=bar
```

Typically, if your playbook is only being run on one group of hosts, it's easier to define the variables in the playbook via an included `vars` file. However, in many cases you will be running a playbook or applying a set of roles to multiple inventory groups. In these situations, you may need to use `group_vars` to override specific variables for one or more groups of servers.

Ephemeral infrastructure: Dynamic inventory

In many circumstances, static inventories are adequate for describing your infrastructure. When working on small applications, low-traffic web applications, and individual workstations, it's simple enough to manage an inventory file by hand.

However, in the age of cloud computing and highly scalable application architecture, it's often necessary to add dozens or hundreds of servers to an infrastructure in a short period of time—or to add and remove servers continuously, to scale as traffic grows and subsides. In this circumstance, it would be tedious (if not impossible) to manage a single inventory file by hand, especially if you're using auto-scaling infrastructure new instances are provisioned and need to be configured in minutes or seconds.

Even in the case of container-based infrastructure, new instances need to be configured correctly, with the proper port mappings, application settings, and filesystem configuration.

For these situations, Ansible allows you to define inventory *dynamically*. If you’re using one of the larger cloud-based hosting providers, chances are there is already a dynamic inventory script (which Ansible uses to build an inventory) for you to use. Ansible core already includes scripts for Amazon Web Services, Cobbler, DigitalOcean, Linode, OpenStack, and other large providers, and later we’ll explore creating our own dynamic inventory script (if you aren’t using one of the major hosting providers or cloud management platforms).

Dynamic inventory with DigitalOcean

Digital Ocean is one of the world’s top five hosting companies, and has grown rapidly since it’s founding in 2011. One of the reasons for the extremely rapid growth is the ease of provisioning new ‘droplets’ (cloud VPS servers), and the value provided; as of this writing, you could get a fairly speedy VPS with 512MB of RAM and a generous portion of fast SSD storage for \$5 USD per month.

Digital Ocean’s API and simple developer-friendly philosophy has made it easy for Ansible to interact with Digital Ocean droplets; you can create, manage, and delete droplets with Ansible, as well as use droplets with your playbooks using dynamic inventory.

DigitalOcean account prerequisites

Before you can follow the rest of the examples in this section, you will need:

1. A DigitalOcean account (sign up at www.digitalocean.com).
2. dopy, a Python wrapper for Digital Ocean API interaction (you can install it with pip: `sudo pip install dopy`).
3. Your DigitalOcean account API key and client ID (Ansible currently supports the v1 API, so you need to go to the ‘Apps & API’ page in your profile, then click the ‘API v1.0 Page’ link to get a key and client ID).
4. An SSH key pair, which will be used to connect to your DigitalOcean servers. Follow [this guide⁷⁶](#) to create a key pair and add the public key to your DigitalOcean account.

Once you have these four things set up and ready to go, you should be able to communicate with your DigitalOcean account through Ansible.

Connecting to your DigitalOcean account

There are a few different ways you can specify your DigitalOcean client ID and API key (including command line arguments `--client-id` and `--api-key`, as values inside a `digital_ocean.ini` file, or as environment variables). For our example, we’ll use environment variables (since these are easy to configure, and work both with Ansible’s `digital_ocean` module and the dynamic inventory script). Open up a terminal session, and enter the following commands:

⁷⁶<https://www.digitalocean.com/community/tutorials/how-to-use-ssh-keys-with-digitalocean-droplets>

```
$ export DO_CLIENT_ID=YOUR_CLIENT_ID_HERE  
$ export DO_API_KEY=YOUR_API_KEY_HERE
```

Before we can use a dynamic inventory script to discover our DigitalOcean droplets, let's use Ansible to quickly provision a new droplet.



Creating cloud instances ('Droplets', in DigitalOcean parlance) will incur minimal charges for the time you use them (currently less than \$0.01/hour for the size in this example). For the purposes of this tutorial (and in general, for any testing), make sure you shut down and destroy your instances when you're finished using them, or you will be charged through the next billing cycle! Even so, using low-priced instances (like a \$5/month DigitalOcean droplet with hourly billing) means that, even in the worst case, you won't have to pay much. If you create and destroy an instance in a few hours, you'll be charged a few pennies.

Creating a droplet with Ansible

Create a new playbook named `provision.yml`, with the following contents:

```
1  ---  
2  - hosts: localhost  
3    connection: local  
4    gather_facts: false  
5  
6    tasks:  
7      - name: Create new Droplet.  
8        digital_ocean:  
9          state: present  
10         command: droplet  
11         name: ansible-test  
12         private_networking: yes  
13         # 512mb  
14         size_id: 66  
15         # CentOS 7.0 x64  
16         image_id: 6713409  
17         # nyc2  
18         region_id: 4  
19         ssh_key_ids: 138954  
20         # Required for idempotence/only one droplet creation.  
21         unique_name: yes  
22         register: do
```

The `digital_ocean` module lets you create, manage, and delete droplets with ease. You can read the documentation for all the options, but the above is an overview of the main options. `name` sets the hostname for the droplet, `state` can also be set to `deleted` if you want the droplet to be destroyed, and other options tell DigitalOcean where to set up the droplet, and with what OS and configuration.



You can use DigitalOcean's API, along with your `client_id` and `api_key`, to get the IDs for `size_id` (the size of the Droplet), `image_id` (the system or distro image to use), `region_id` (the data center in which your droplet will be created), and `ssh_key_ids` (a comma separate list of SSH keys to be included in the root account's `authorized_keys` file).

As an example, to get all the available images, use `curl "https://api.digitalocean.com/images/?client_id=CLIENT_ID&api_key=API_KEY&filter=global" | python -m json.tool`, substituting your own `CLIENT_ID` and `API_KEY`, and you'll receive a JSON listing of all available values. Browse the [DigitalOcean API](#)⁷⁷ for information on how to query SSH key information, size information, etc.

We used `register` as part of the `digital_ocean` task so we could immediately start using and configuring the new host if needed. Running the above playbook returns the following output (using `debug: var=do` in an additional task to dump the contents of our registered variable, `do`):

```
$ ansible-playbook do_test.yml

PLAY [localhost] ****
TASK: [Create new Droplet.] ****
changed: [localhost]

TASK: [debug var=do] ****
ok: [localhost] => {
    "do": {
        "changed": true,
        "droplet": {
            "backups": [],
            "backups_active": false,
            "created_at": "2014-10-22T02:09:20Z",
            "event_id": 34915980,
            "id": 2940194,
            "image_id": 6918990,
            "ip_address": "162.243.20.29",
            "locked": false,
            "name": "ansible-test",
            "region": "nyc1"
        }
    }
}
```

⁷⁷<https://developers.digitalocean.com/>

```

        "private_ip_address": null,
        "region_id": 4,
        "size_id": 66,
        "snapshots": [],
        "status": "active"
    },
    "invocation": {
        "module_args": "",
        "module_name": "digital_ocean"
    }
}
}
}

PLAY RECAP ****
localhost : ok=2      changed=1      unreachable=0      failed=0

```

Since `do` contains the new droplet's IP address (alongside other relevant information), you can place your freshly-created droplet in an existing inventory group using Ansible's `add_host` module. Adding to the playbook we started above, you could set up your playbook to provision an instance and immediately configure it (after waiting for port 22 to become available) with something like:

```

24     - name: Add new host to our inventory.
25       add_host:
26         name: "{{ do.droplet.ip_address }}"
27         groups: do
28         when: do.droplet is defined
29
30 - hosts: do
31   remote_user: root
32   gather_facts: false
33
34 tasks:
35   - name: Wait for port 22 to become available.
36     local_action: "wait_for port=22 host={{ inventory_hostname }}"
37
38   - name: Install tcpdump.
39     yum: name=tcpdump state=installed

```

At this point, if you run the playbook (`$ ansible-playbook provision.yml`), it should create a new droplet (if it has not already been created), then add that droplet to the `do` inventory group, and finally, run a new play on all the `do` hosts (including the new droplet). Here are the results:

```
$ ansible-playbook provision.yml

PLAY [localhost] ****
TASK: [Create new Droplet.] ****
changed: [localhost]

TASK: [Add new host to our inventory.] ****
ok: [localhost]

PLAY [do] ****
TASK: [Install tcpdump.] ****
changed: [162.243.20.29]

PLAY RECAP ****
162.243.20.29 : ok=2    changed=1    unreachable=0    failed=0
localhost      : ok=2    changed=1    unreachable=0    failed=0
```

If you run the same playbook again, it should report no changes—the entire playbook is idempotent! You might be starting to see just how powerful it is to have a tool as flexible as Ansible at your disposal; not only can you configure servers, you can create them (singly, or dozens at a time), and configure them at once. And even if a ham-fisted sysadmin jumps in and deletes an entire server, you can run the playbook again, and rest assured your server will be recreated and reconfigured exactly as it was when it was first set up.



Note that you might need to disable strict host key checking to get provisioning and instant configuration to work correctly, otherwise you may run into an error stating that Ansible can't connect to the new droplet during the second play. To do this, add the line `host_key_checking=False` under the `[defaults]` section in your `ansible.cfg` file (located in `/etc/ansible` by default).

You should normally leave `host_key_checking` enabled, but when rapidly building and destroying VMs for testing purposes, it is simplest to disable it temporarily.

DigitalOcean dynamic inventory with `digital_ocean.py`

Once you have some DigitalOcean droplets, you need a way for Ansible to dynamically build an inventory of your servers so you can build playbooks and use the servers in logical groupings (or run playbooks and `ansible` commands directly on all droplets).

There are a few steps to getting DigitalOcean's official dynamic inventory script working:

1. Install `dopy` via pip (the DigitalOcean Python library): `$ pip install dopy.`
2. Download the [DigitalOcean dynamic inventory script⁷⁸](#) from Ansible on GitHub: `$ curl -O https://raw.githubusercontent.com/ansible/ansible/devel/plugins/inventory/digital_ocean.py.`
3. Make the inventory script executable: `$ chmod +x digital_ocean.py.`
4. Make sure you have the credentials configured in `digital_ocean.ini` (as explained earlier in this chapter). Alternatively, you can set `DO_CLIENT_ID` and `DO_API_KEY` in your environment, or pass the command line options `--client-id` and `--api-key`.
5. Make sure the script is working by running the script directly: `$./digital_ocean.py --pretty.` After a second or two, you should see all your droplets (likely just the one you created earlier) listed by IP address and dynamic group as JSON.
6. Ping all your DigitalOcean droplets: `$ ansible all -m ping -i digital_ocean.py -u root.`

Now that you have all your hosts being loaded through the dynamic inventory script, you can use `add_hosts` to build groups of the Droplets for use in your playbooks. Alternatively, if you want to fork the `digital_ocean.py` inventory script, you can modify it to suit your needs; exclude certain servers, build groups based on certain criteria, etc.



Ansible currently supports DigitalOcean's v1 API, which makes working with DigitalOcean slightly more difficult. The v2 API allows you to use region names (e.g. "nyc2") instead of numeric IDs, allows you to [add metadata to your droplets⁷⁹](#), and much more. Ansible should soon support the v2 API. If you're interested in the current status of this effort, or would like to help in migrating to the v2 API, visit [the v2 API support issue on GitHub⁸⁰](#).

Dynamic inventory with AWS

Many of this book's readers are familiar with Amazon Web Services (especially EC2, S3, ElastiCache, and Route53), and likely have managed or currently manage an infrastructure within Amazon's cloud. Ansible has very strong support for managing AWS-based infrastructure, and includes a [dynamic inventory script⁸¹](#) to help you run playbooks on your hosts in a variety of ways.

There are a few excellent guides to using Ansible with AWS, for example:

- [Ansible - Amazon Web Services Guide⁸²](#)
- [Ansible for AWS⁸³](#)

⁷⁸https://raw.githubusercontent.com/ansible/ansible/devel/plugins/inventory/digital_ocean.py

⁷⁹<https://www.digitalocean.com/community/tutorials/an-introduction-to-droplet-metadata>

⁸⁰<https://github.com/ansible/ansible-modules-core/issues/209>

⁸¹<https://raw.githubusercontent.com/ansible/ansible/devel/plugins/inventory/ec2.py>

⁸²http://docs.ansible.com/guide_aws.html

⁸³<https://leanpub.com/ansible-for-aws>

I won't be covering dynamic inventory in this chapter, but will mention that the `ec2.py` dynamic inventory script, along with Ansible's extensive support for AWS infrastructure through `ec2_*` modules, makes Ansible the best and most simple tool for managing a broad AWS infrastructure.

In the next chapter, one of the examples will include a guide for provisioning infrastructure on AWS, along with a quick overview of dynamic inventory on AWS.

Inventory on-the-fly: `add_host` and `group_by`

Sometimes, especially when provisioning new servers, you will need to modify the in-memory inventory during the course of a playbook run. Ansible offers the `add_host` and `group_by` modules to help you manage inventory for these scenarios.

In the DigitalOcean example above, `add_host` was used to add the new droplet to the `do` group:

```
[...]
- name: Add new host to our inventory.
  add_host:
    name: "{{ do.droplet.ip_address }}"
    groups: do
    when: do.droplet is defined

- hosts: do
  remote_user: root

  tasks:
[...]
```

You could add multiple groups with `add_host`, and you can also add other variables for the host inline with `add_host`. As an example, let's say you created a VM using an image that exposes SSH on port 2288 and requires an application-specific memory limit specific to this VM:

```
- name: Add new host to our inventory.
  add_host:
    name: "{{ do.droplet.ip_address }}"
    ansible_ssh_port: 2288
    myapp_memory_maximum: "1G"
    when: do.droplet is defined
```

The custom port will be used when Ansible connects to this host, and the `myapp_memory_maximum` will be passed into the playbooks just as any other inventory variable.

The `group_by` module is even simpler, and allows you to create dynamic groups during the course of a playbook run. Usage is extremely simple:

```
- hosts: all
  gather_facts: yes
  tasks:
    - name: Create an inventory group for each architecture.
      group_by: "key=architecture-{{ ansible_machine }}"
    - debug: var=groups
```

After running the above playbook, you'd see all your normal inventory groups, plus groups for architecture-x86_64, i386, etc. (depending on what kind of server architectures you use).

Multiple inventory sources - mixing static and dynamic inventories

If you need to combine static and dynamic inventory, or even if you wish to use multiple dynamic inventories (for example, if you are managing servers hosted by two different cloud providers), you can pass a directory to `ansible` or `ansible-playbook`, and Ansible will combine the output of all the inventories (both static and dynamic) inside the directory:

```
`ansible-playbook -i path/to/inventories main.yml`
```

One caveat: Ansible ignores `.ini` and backup files in the directory, but will attempt to parse every text file and execute every executable file in the directory—don't leave random files in mixed inventory folders!

Creating custom dynamic inventories

Most infrastructure can be managed with a custom inventory file or an off-the-shelf cloud inventory script, but there are many situations where more control is needed. Ansible will accept any kind of executable file as an inventory file, so you can build your own dynamic inventory however you like, as long as you can pass it to Ansible as JSON.

You could create an executable binary, a script, or anything else that can be run and will output JSON to `stdout`, and Ansible will call it with the argument `--list` when you run, as an example, `ansible all -i my-inventory-script -m ping`.

Let's start working our own custom dynamic inventory script by outlining the basic JSON format Ansible expects:

```

1  {
2      "group": {
3          "hosts": [
4              "192.168.28.71",
5              "192.168.28.72"
6          ],
7          "vars": {
8              "ansible_ssh_user": "johndoe",
9              "ansible_ssh_private_key_file": "~/.ssh/mykey",
10             "example_variable": "value"
11         }
12     },
13     "_meta": {
14         "hostvars": {
15             "192.168.28.71": {
16                 "host_specific_var": "bar"
17             },
18             "192.168.28.72": {
19                 "host_specific_var": "foo"
20             }
21         }
22     }
23 }

```

Ansible expects a dictionary of groups (each group having a list of hosts, and group variables in the group's vars dictionary), and a _meta dictionary that stores host variables for all hosts individually (inside a hostvars dictionary).



When you return a _meta dictionary in your inventory script, Ansible stores that data in its cache and doesn't call your inventory script N times for all the hosts in the inventory. You can leave out the _meta variables if you'd rather structure your inventory file to return host variables one host at a time (Ansible will call your script with the arguments --host [hostname] for each host), but it's often faster and easier to simply return all variables in the first call. In this book, all the examples will use the _meta dictionary.

The dynamic inventory script can do anything to get the data (call an external API, pull information from a database or file, etc.), and Ansible will use it as an inventory source as long as it returns a JSON structure like the one above when the script is called with the --list.

Building a Custom Dynamic Inventory in Python

To create a test dynamic inventory script for demonstration purposes, let's set up a quick set of two VMs using Vagrant. Create the following `Vagrantfile` in a new directory:

```
1 VAGRANTFILE_API_VERSION = "2"
2
3 Vagrant.configure(VAGRANTFILE_API_VERSION) do |config|
4   config.ssh.insert_key = false
5   config.vm.provider :virtualbox do |vb|
6     vb.customize ["modifyvm", :id, "--memory", "256"]
7   end
8
9   # Application server 1.
10  config.vm.define "inventory1" do |inventory|
11    inventory.vm.hostname = "inventory1.dev"
12    inventory.vm.box = "geerlingguy/ubuntu1404"
13    inventory.vm.network :private_network, ip: "192.168.28.71"
14  end
15
16  # Application server 2.
17  config.vm.define "inventory2" do |inventory|
18    inventory.vm.hostname = "inventory2.dev"
19    inventory.vm.box = "geerlingguy/ubuntu1404"
20    inventory.vm.network :private_network, ip: "192.168.28.72"
21  end
22 end
```

Run `vagrant up` to boot two VMs running Ubuntu 14.04, with the IP addresses 192.168.28.71, and 192.168.28.72. A simple inventory file could be used to control the VMs with Ansible:

```
1 [group]
2 192.168.28.71 host_specific_var=foo
3 192.168.28.72 host_specific_var=bar
4
5 [group:vars]
6 ansible_ssh_user=vagrant
7 ansible_ssh_private_key_file=~/vagrant.d/insecure_private_key
8 example_variable=value
```

However, let's assume the VMs were provisioned by another system, and you need to get the information through a dynamic inventory script. Here's a simple implementation of a dynamic inventory script in Python:

```
1 #!/usr/bin/env python
2
3 """
4 Example custom dynamic inventory script for Ansible, in Python.
5 """
6
7 import os
8 import sys
9 import argparse
10
11 try:
12     import json
13 except ImportError:
14     import simplejson as json
15
16 class ExampleInventory(object):
17
18     def __init__(self):
19         self.inventory = {}
20         self.read_cli_args()
21
22         # Called with `--list`.
23         if self.args.list:
24             self.inventory = self.example_inventory()
25         # Called with `--host [hostname]`.
26         elif self.args.host:
27             # Not implemented, since we return _meta info `--list`.
28             self.inventory = self.empty_inventory()
29         # If no groups or vars are present, return an empty inventory.
30         else:
31             self.inventory = self.empty_inventory()
32
33     print json.dumps(self.inventory);
34
35     # Example inventory for testing.
36     def example_inventory(self):
37         return {
38             'group': {
39                 'hosts': ['192.168.28.71', '192.168.28.72'],
40                 'vars': {
41                     'ansible_ssh_user': 'vagrant',
42                     'ansible_ssh_private_key_file':
```

```
43             '~/.vagrant.d/insecure_private_key',
44             'example_variable': 'value'
45         }
46     },
47     '_meta': {
48         'hostvars': {
49             '192.168.28.71': {
50                 'host_specific_var': 'foo'
51             },
52             '192.168.28.72': {
53                 'host_specific_var': 'bar'
54             }
55         }
56     }
57 }
58
59 # Empty inventory for testing.
60 def empty_inventory(self):
61     return {'_meta': {'hostvars': {}}}
62
63 # Read the command line args passed to the script.
64 def read_cli_args(self):
65     parser = argparse.ArgumentParser()
66     parser.add_argument('--list', action = 'store_true')
67     parser.add_argument('--host', action = 'store')
68     self.args = parser.parse_args()
69
70 # Get the inventory.
71 ExampleInventory()
```

Save the above as `inventory.py` in the same folder as the `Vagrantfile` you created earlier (and make sure you booted the two VMs with `vagrant up`), and make the file executable `chmod +x inventory.py`.

Run the inventory script manually to verify it returns the proper JSON response when run with `--list`:

```
$ ./inventory.py --list
{"group": {"hosts": ["192.168.28.71", "192.168.28.72"], "vars": {"ansible_ssh_user": "vagrant", "ansible_ssh_private_key_file": "~/.vagrant.d/insecure_private_key", "example_variable": "value"}}, "_meta": {"hostvars": {"192.168.28.72": {"host_specific_var": "bar"}, "192.168.28.71": {"host_specific_var": "foo"}}}}
```

Test Ansible's ability to use the inventory script to contact the two VMs:

```
$ ansible all -i inventory.py -m ping
192.168.28.71 | success >> {
    "changed": false,
    "ping": "pong"
}

192.168.28.72 | success >> {
    "changed": false,
    "ping": "pong"
}
```

Since Ansible can connect, verify the configured host variables (`foo` and `bar`) are set correctly on each of their respective hosts:

```
$ ansible all -i inventory.py -m debug -a "var=host_specific_var"
192.168.28.71 | success >> {
    "var": {
        "host_specific_var": "foo"
    }
}

192.168.28.72 | success >> {
    "var": {
        "host_specific_var": "bar"
    }
}
```

The only changes you'd need to make to the above `inventory.py` script for real-world usage is to change the `example_inventory()` method to something that incorporates the business logic you need for your own inventory—whether calling an external API with all the server data, or pulling in the information from a database or other data store.

Building a Custom Dynamic Inventory in PHP

You can build an inventory script in whatever language you'd like; the same Python script above can be ported to functional PHP as follows:

```
1 #!/usr/bin/php
2 <?php
3
4 /**
5 * @file
6 * Example custom dynamic inventory script for Ansible, in PHP.
7 */
8
9 /**
10 * Example inventory for testing.
11 *
12 * @return array
13 * An example inventory with two hosts.
14 */
15 function example_inventory() {
16     return [
17         'group' => [
18             'hosts' => ['192.168.28.71', '192.168.28.72'],
19             'vars' => [
20                 'ansible_ssh_user' => 'vagrant',
21                 'ansible_ssh_private_key_file' => '~/.vagrant.d/insecure_private_key',
22                 'example_variable' => 'value',
23             ],
24         ],
25         '_meta' => [
26             'hostvars' => [
27                 '192.168.28.71' => [
28                     'host_specific_var' => 'foo',
29                 ],
30                 '192.168.28.72' => [
31                     'host_specific_var' => 'bar',
32                 ],
33             ],
34         ],
35     ];
36 }
37
38 /**
39 * Empty inventory for testing.
40 *
41 * @return array
42 * An empty inventory.
```

```
43  /*
44  function empty_inventory() {
45      return ['_meta' => ['hostvars' => new stdClass()]];
46  }
47
48 /**
49 * Get inventory.
50 *
51 * @param array $argv
52 *   Array of command line arguments (as returned by $_SERVER['argv']).
53 *
54 * @return array
55 *   Inventory of groups or vars, depending on arguments.
56 */
57 $function get_inventory($argv = []) {
58     $inventory = new stdClass();
59
60     // Called with `--list`.
61     if (!empty($argv[1]) && $argv[1] == '--list') {
62         $inventory = example_inventory();
63     }
64     // Called with `--host [hostname]`.
65     elseif ((!empty($argv[1]) && $argv[1] == '--host') && !empty($argv[2])) {
66         // Not implemented, since we return _meta info `--list`.
67         $inventory = empty_inventory();
68     }
69     // If no groups or vars are present, return an empty inventory.
70     else {
71         $inventory = empty_inventory();
72     }
73
74
```



All the files mentioned in these dynamic inventory examples are available in the [Ansible for DevOps GitHub repository](#)⁸⁴, in the `dynamic-inventory` folder.

Managing a PaaS with a Custom Dynamic Inventory

[Hosted Apache Solr](#)⁸⁵'s infrastructure is built using a custom dynamic inventory to allow for centrally-controlled server provisioning and configuration. Here's how the server provisioning process works on Hosted Apache Solr:

1. A Drupal website holds a 'Server' content type that stores metadata about each server (e.g. chosen hostname, data center location, choice of OS image, and memory settings).
2. When a new server is added, a remote Jenkins job is triggered, which:
 1. Builds a new cloud server on DigitalOcean using an Ansible playbook.
 2. Runs a provisioning playbook on the server to initialize the configuration.
 3. Adds a new DNS entry for the server.
 4. Posts additional server metadata (like the IP address) back to the Drupal website via a private API.
3. When a server is updated, or there is new configuration to be deployed to the server(s), a different Jenkins job is triggered, which:
 1. Runs the same provisioning playbook on all the DigitalOcean servers. This playbook uses an inventory script which calls back to an inventory API endpoint that returns all the server information as JSON (the inventory script on the Jenkins server passes the JSON through to stdout).
 2. Reports back success or failure of the ansible playbook to the REST API.

The above process transformed the management of the entire Hosted Apache Solr platform. Instead of taking twenty to thirty minutes to build a new server (when using an Ansible playbook with a few manual steps), the process can be completed in just a few minutes, with no manual intervention.



The security of your server inventory and infrastructure management should be a top priority; Hosted Apache Solr uses HTTPS everywhere, and has a hardened private API for inventory access and server metadata. If you have any automated processes that run over a network, you should make doubly sure you audit these processes and all the involved systems thoroughly!

Summary

From the most basic infrastructure consisting of one server to a multi-tenant, dynamic infrastructure with thousands of servers, Ansible offers many options for describing your servers, and overriding playbook and role variables for specific hosts or groups. You should be able to describe all your servers, however they're managed and wherever they're hosted, with Ansible's flexible inventory system.

⁸⁴<https://github.com/geerlingguy/ansible-for-devops>

⁸⁵<https://hostedapachesolr.com/>

/ A pint of sweat saves a gallon of \
\ blood. (General Patton) /

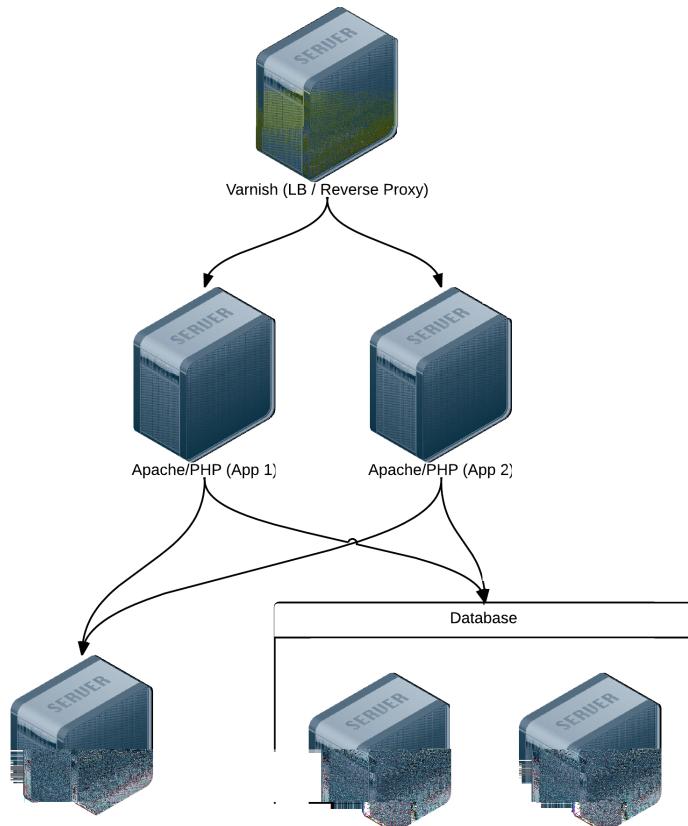
\ ^__^
\ (oo)_____
(__) \)\ /\
||----w |
|| ||

Chapter 8 - Ansible Cookbooks

Most of the book up to this point has demonstrated individual aspects of Ansible—inventory, playbooks, ad-hoc tasks, etc.—but this chapter will start to synthesize everything and show how Ansible is applied to real-world infrastructure management scenarios.

Highly-Available Infrastructure with Ansible

Real-world web applications require redundancy and horizontal scalability with multi-server infrastructure. In the following example, we'll use Ansible to configure a complex infrastructure (illustrated below) on servers provisioned either locally via Vagrant and VirtualBox, or on a set of automatically-provisioned instances running on either DigitalOcean or Amazon Web Services:



Highly-Available Infrastructure.

Varnish acts as a load balancer and reverse proxy, fronting web requests and routing them to the application servers. We could just as easily use something like **Nginx** or **HAProxy**, or even a proprietary cloud-based solution like an Amazon's **Elastic Load Balancer** or Linode's **NodeBalancer**, but for simplicity's sake, and for flexibility in deployment, we'll use Varnish.

Apache and **mod_php** run a PHP-based application that displays the entire stack's current status and outputs the current server's IP address for load balancing verification.

A **Memcached** server provides a caching layer that can be used to store and retrieve frequently-accessed objects in lieu of slower database storage.

Two **MySQL** servers, configured as a master and slave, offer redundant and performant database access; all data will be replicated from the master to the slave, and the slave can also be used as a secondary server for read-only queries to take some load off the master.

Directory Structure

In order to keep our configuration organized, we'll use the following structure for our playbooks and configuration:

```
lamp-infrastructure/
  inventories/
  playbooks/
    db/
    memcached/
    varnish/
    www/
  provisioners/
  configure.yml
  provision.yml
  requirements.txt
  Vagrantfile
```

Organizing things this way allows us to focus on each server configuration individually, then build playbooks for provisioning and configuring instances on different hosting providers later. This organization also keeps server playbooks completely independent, so we can modularize and reuse individual server configurations.

Individual Server Playbooks

Let's start building our individual server playbooks (in the `playbooks` directory). To make our playbooks more efficient, we'll use some contributed Ansible roles on Ansible Galaxy rather than install and configure everything step-by-step. We're going to target CentOS 6.x servers in these

playbooks, but only minimal changes would be required to use the playbooks with Ubuntu, Debian, or later versions of CentOS.

Varnish

Create a `main.yml` file within the `playbooks/varnish` directory, with the following contents:

```
1  ---
2  - hosts: lamp-varnish
3    sudo: yes
4
5  vars_files:
6    - vars.yml
7
8  roles:
9    - geerlingguy.firewall
10   - geerlingguy.repo-epel
11   - geerlingguy.varnish
12
13 tasks:
14   - name: Copy Varnish default.vcl.
15     template:
16       src: "templates/default.vcl.j2"
17       dest: "/etc/varnish/default.vcl"
18     notify: restart varnish
```

We're going to run this playbook on all hosts in the `lamp-varnish` inventory group (we'll create this later), and we'll run a few simple roles to configure the server:

- `geerlingguy.firewall` configures a simple iptables-based firewall using a couple variables defined in `vars.yml`.
- `geerlingguy.repo-epel` adds the EPEL repository (a prerequisite for varnish).
- `geerlingguy.varnish` installs and configures Varnish.

Finally, a task copies over a custom `default.vcl` that configures Varnish, telling it where to find our web servers and how to load balance requests between the servers.

Let's create the two files referenced in the above playbook. First, `vars.yml`, in the same directory as `main.yml`:

```

1  ---
2  firewall_allowed_tcp_ports:
3    - "22"
4    - "80"
5
6  varnish_use_default_vcl: false

```

The first variable tells the `geerlingguy.firewall` role to open TCP ports 22 and 80 for incoming traffic. The second variable tells the `geerlingguy.varnish` we will supply a custom `default.vcl` for Varnish configuration.

Create a `templates` directory inside the `playbooks/varnish` directory, and inside, create a `default.vcl.j2` file. This file will use Jinja2 syntax to build Varnish's custom `default.vcl` file:

```

1 vcl 4.0;
2
3 import directors;
4
5 {% for host in groups['lamp-www'] %}
6 backend www{{ loop.index }} {
7   .host = "{{ host }}";
8   .port = "80";
9 }
10 {% endfor %}
11
12 sub vcl_init {
13   new vdir = directors.random();
14   {% for host in groups['lamp-www'] %}
15     vdir.add_backend(www{{ loop.index }}, 1);
16   {% endfor %}
17 }
18
19 sub vcl_recv {
20   set req.backend_hint = vdir.backend();
21
22   # For testing ONLY; makes sure load balancing is working correctly.
23   return (pass);
24 }

```

We won't study Varnish's VCL syntax in depth but we'll run through `default.vcl` and highlight what is being configured:

1. (1-3) Indicate that we're using the 4.0 version of the VCL syntax and import the `directors` `varnish` module (which is used to configure load balancing).

2. (5-10) Define each web server as a new backend; give a host and a port through which varnish can contact each host.
3. (12-17) `vc1_init` is called when Varnish boots and initializes any required varnish modules. In this case, we're configuring a load balancer `vdir`, and adding each of the `www[*]` backends we defined earlier as backends to which the load balancer will distribute requests. We use a `random` director so we can easily demonstrate Varnish's ability to distribute requests to both app backends, but other load balancing strategies are also available.
4. (19-24) `vc1_recv` is called for each request, and routes the request through Varnish. In this case, we route the request to the `vdir` backend defined in `vc1_init`, and indicate that Varnish should **not** cache the result.

According to #4, we're actually *bypassing Varnish's caching layer*, which is not helpful in a typical production environment. If you only need a load balancer without any reverse proxy or caching capabilities, there are better options. However, we need to verify our infrastructure is working as it should. If we used Varnish's caching, Varnish would only ever hit one of our two web servers during normal testing.

In terms of our caching/load balancing layer, this should suffice. For a true production environment, you should remove the final `return (pass)` and customize `default.vcl` according to your application's needs.

Apache / PHP

Create a `main.yml` file within the `playbooks/www` directory, with the following contents:

```
1  ---
2  - hosts: lamp-www
3    sudo: yes
4
5  vars_files:
6    - vars.yml
7
8  roles:
9    - gearlingguy.firewall
10   - gearlingguy.repo-epel
11   - gearlingguy.apache
12   - gearlingguy.php
13   - gearlingguy.php-mysql
14   - gearlingguy.php-memcached
15
16 tasks:
17   - name: Remove the Apache test page.
18     file:
19       path: /var/www/html/index.html
```

```
20      state: absent
21  - name: Copy our fancy server-specific home page.
22    template:
23      src: templates/index.php.j2
24      dest: /var/www/html/index.php
```

As with Varnish's configuration, we'll configure a firewall and add the EPEL repository (required for PHP's memcached integration), and we'll also add the following roles:

- `geerlingguy.apache` installs and configures the latest available version of the Apache web server.
- `geerlingguy.php` installs and configures PHP to run through Apache.
- `geerlingguy.php-mysql` adds MySQL support to PHP.
- `geerlingguy.php-memcached` adds Memcached support to PHP.

Two final tasks remove the default `index.html` home page included with Apache, and replace it with our PHP app.

As in the Varnish example, create the two files referenced in the above playbook. First, `vars.yml`, alongside `main.yml`:

```
1 ---
2 firewall_allowed_tcp_ports:
3   - "22"
4   - "80"
```

Create a `templates` directory inside the `playbooks/www` directory, and inside, create an `index.php.j2` file. This file will use Jinja2 syntax to build a (relatively) simple PHP script to display the health and status of all the servers in our infrastructure:

```
1 <?php
2 /**
3  * @file
4  * Infrastructure test page.
5  *
6  * DO NOT use this in production. It is simply a PoC.
7  */
8
9 $mysql_servers = array(
10 {% for host in groups['lamp-db'] %}
11   '{{ host }}',
```

```
12  {% endfor %}  
13 );  
14 $mysql_results = array();  
15 foreach ($mysql_servers as $host) {  
16     if ($result = mysql_test_connection($host)) {  
17         $mysql_results[$host] = '<span style="color: green;">PASS</span>';  
18         $mysql_results[$host] .= ' (' . $result['status'] . ')';  
19     }  
20     else {  
21         $mysql_results[$host] = '<span style="color: red;">FAIL</span>';  
22     }  
23 }  
24  
25 // Connect to Memcached.  
26 $memcached_result = '<span style="color: red;">FAIL</span>';  
27 if (class_exists('Memcached')) {  
28     $memcached = new Memcached;  
29     $memcached->addServer('{{ groups['lamp-memcached'][0] }}', 11211);  
30  
31     // Test adding a value to memcached.  
32     if ($memcached->add('test', 'success', 1)) {  
33         $result = $memcached->get('test');  
34         if ($result == 'success') {  
35             $memcached_result = '<span style="color: green;">PASS</span>';  
36             $memcached->delete('test');  
37         }  
38     }  
39 }  
40  
41 /**  
42 * Connect to a MySQL server and test the connection.  
43 *  
44 * @param string $host  
45 *   IP Address or hostname of the server.  
46 *  
47 * @return array  
48 *   Array with keys 'success' (bool) and 'status' ('slave' or 'master').  
49 *   Empty if connection failure.  
50 */  
51 function mysql_test_connection($host) {  
52     $username = 'mycompany_user';  
53     $password = 'secret';
```

```
54 try {
55     $db = new PDO(
56         'mysql:host=' . $host . ';dbname=mycompany_database',
57         $username,
58         $password,
59         array(PDO::ATTR_ERRMODE => PDO::ERRMODE_EXCEPTION));
60
61     // Query to see if the server is configured as a master or slave.
62     $statement = $db->prepare("SELECT variable_value
63         FROM information_schema.global_variables
64         WHERE variable_name = 'LOG_BIN');");
65     $statement->execute();
66     $result = $statement->fetch();
67
68     return array(
69         'success' => TRUE,
70         'status' => ($result[0] == 'ON') ? 'master' : 'slave',
71     );
72 }
73 catch (PDOException $e) {
74     return array();
75 }
76 }
77 ?>
78 <!DOCTYPE html>
79 <html>
80 <head>
81     <title>Host {{ inventory_hostname }}</title>
82     <style>* { font-family: Helvetica, Arial, sans-serif }</style>
83 </head>
84 <body>
85     <h1>Host {{ inventory_hostname }}</h1>
86     <?php foreach ($mysql_results as $host => $result): ?>
87         <p>MySQL Connection (<?php print $host; ?>): <?php print $result; ?></p>
88     <?php endforeach; ?>
89     <p>Memcached Connection: <?php print $memcached_result; ?></p>
90 </body>
91 </html>
```



Don't try transcribing this example manually; you can get the code from this book's repository on GitHub. Visit the [ansible-for-devops⁸⁶](#) repository and download the source for `index.php.j2`⁸⁷

As this is the heart of the example application we're deploying to the infrastructure, it's necessarily a bit more complex than most examples in the book, but a quick run through follows:

- (9-23) Iterate through all the `lamp-db` MySQL hosts defined in the playbook inventory, and test the ability to connect to them, and whether they are configured as master or slave, using the `mysql_test_connection()` function defined later (40-73).
- (25-39) Check the first defined `lamp-memcached` Memcached host defined in the playbook inventory, confirming the ability to connect and create, retrieve, and delete a value from the cache.
- (41-76) Define the `mysql_test_connection()` function which tests the the ability to connect to a MySQL server and also returns its replication status.
- (78-91) Print the results of all the MySQL and Memcached tests, along with `{{ inventory_hostname }}` as the page title, so we can easily see which web server is serving the viewed page.

At this point, the heart of our infrastructure—the application that will test and display the status of all our servers—is ready to go.

Memcached

Compared to the earlier playbooks, the Memcached playbook is quite simple. Create `playbooks/memcached/main.yml` with the following contents:

```

1  ---
2  - hosts: lamp-memcached
3    sudo: yes
4
5    vars_files:
6      - vars.yml
7
8    roles:
9      - geerlingguy.firewall
10     - geerlingguy.memcached

```

As with the other servers, we need to ensure only the required TCP ports are open using the simple `geerlingguy.firewall` role. Next we install Memcached using the `geerlingguy.memcached` role.

In our `vars.yml` file (again, alongside `main.yml`), add the following:

⁸⁶<https://github.com/geerlingguy/ansible-for-devops>

⁸⁷<https://github.com/geerlingguy/ansible-for-devops/blob/master/lamp-infrastructure/playbooks/www/templates/index.php.j2>

```

1  ---
2  firewall_allowed_tcp_ports:
3    - "22"
4  firewall_additional_rules:
5    - "iptables -A INPUT -p tcp --dport 11211 -s {{ groups['lamp-www'][0] }} -j ACCEPT"
6    - "iptables -A INPUT -p tcp --dport 11211 -s {{ groups['lamp-www'][1] }} -j ACCEPT"
7
8

```

We need port 22 open for remote access, and for Memcached, we're adding manual iptables rules to allow access on port 11211 for the web servers **only**. We add one rule per `lamp-www` server by drilling down into each item in the generated `groups` variable that Ansible uses to track all inventory groups currently available.



The principle of least privilege “requires that in a particular abstraction layer of a computing environment, every module ... must be able to access only the information and resources that are necessary for its legitimate purpose” (Source: [Wikipedia⁸⁸](#)). Always restrict services and ports to only those servers or users that need access!

MySQL

The MySQL configuration is more complex than the other servers because we need to configure MySQL users per-host and configure replication. Because we want to maintain an independent and flexible playbook, we also need to dynamically create some variables so MySQL will get the right server addresses in any potential environment.

Let's first create the main playbook, `playbooks/db/main.yml`:

```

1  ---
2  - hosts: lamp-db
3    sudo: yes
4
5  vars_files:
6    - vars.yml
7
8  pre_tasks:
9    - name: Create dynamic MySQL variables.
10      set_fact:
11        mysql_users:
12          - {
13            name: mycompany_user,

```

⁸⁸http://en.wikipedia.org/wiki/Principle_of_least_privilege

```
14      host: "{{ groups['lamp-www'][0] }}"
15      password: secret,
16      priv: "*.*:SELECT"
17    }
18    -
19    name: mycompany_user,
20    host: "{{ groups['lamp-www'][1] }}"
21    password: secret,
22    priv: "*.*:SELECT"
23  }
24  mysql_replication_master: "{{ groups['a4d.lamp.db.1'][0] }}"
25
26 roles:
27   - gearlingguy.firewall
28   - gearlingguy.mysql
```

Most of the playbook is straightforward, but in this instance, we're using `set_fact` as a `pre_task` (to be run before the `gearlingguy.firewall` and `gearlingguy.mysql` roles) to dynamically create variables for MySQL configuration.

`set_fact` allows us to define variables at runtime, so we can be guaranteed to have all server IP addresses available, even if the servers were freshly provisioned at the beginning of the playbook's run. We'll create two variables:

- `mysql_users` is a list of users the `gearlingguy.mysql` role will create when it runs. This variable will be used on all database servers so both of the two `lamp-www` servers get SELECT privileges on all databases.
- `mysql_replication_master` is used to indicate to the `gearlingguy.mysql` role which database server is the master; it will perform certain steps differently depending on whether the server being configured is a master or slave, and ensure that all the slaves are configured to replicate data from the master.

We'll need a few other normal variables to configure MySQL, so we'll add them alongside the `firewall` variable in `playbooks/db/vars.yml`:

```
1 ---
2   firewall_allowed_tcp_ports:
3     - "22"
4     - "3306"
5
6   mysql_replication_user: {name: 'replication', password: 'secret'}
7   mysql_databases:
8     - { name: mycompany_database, collation: utf8_general_ci, encoding: utf8 }
```

We're opening port 3306 to anyone, but according to the **principle of least privilege** discussed earlier, you would be justified in restricting this port to only the servers and users that need access to MySQL (similar to the memcached server configuration). In this case, the attack vector is mitigated because MySQL's own authentication layer is used through the `mysql_user` variable generated in `main.yml`.

We are defining two MySQL variables, `mysql_replication_user` to be used as for master and slave replication, and `mysql_databases` to define a list of databases that will be created (if they don't already exist) on the database servers.

With the configuration of the database servers complete, the server-specific playbooks are ready to go.

Main Playbook for Configuring All Servers

A simple playbook including each of the group-specific playbooks is all we need for the overall configuration to take place. Create `configure.yml` in the project's root directory, with the following contents:

```
1 ---
2   - include: playbooks/varnish/main.yml
3   - include: playbooks/www/main.yml
4   - include: playbooks/db/main.yml
5   - include: playbooks/memcached/main.yml
```

At this point, if you had some already-booted servers and statically defined inventory groups like `lamp-www`, `lamp-db`, etc., you could run `ansible-playbook configure.yml` and you'd have a full HA infrastructure at the ready!

But we're going to continue to make our playbooks more flexible and useful.

Getting the required roles

As mentioned in the Chapter 6, Ansible allows you to define all the required Ansible Galaxy roles for a given project in a `requirements.txt` file. Instead of having to remember to run `ansible-galaxy install -y [role1] [role2] [role3]` for each of the roles we're using, we can create `requirements.txt` in the root of our project, with the following contents:

```
1 gearlingguy.firewall
2 gearlingguy.repo-epel
3 gearlingguy.varnish
4 gearlingguy.apache
5 gearlingguy.php
6 gearlingguy.php-mysql
7 gearlingguy.php-memcached
8 gearlingguy.mysql
9 gearlingguy.memcached
```

To make sure all the required dependencies are installed, run `ansible-galaxy install -r requirements.txt` from within the project's root.

Vagrantfile for Local Infrastructure via VirtualBox

As with many other examples in this book, we can use Vagrant and VirtualBox to build and configure the infrastructure locally. This lets us test things as much as we want with zero cost, and usually results in faster testing cycles, since everything is orchestrated over a local private network on a (hopefully) beefy workstation.

Our basic Vagrantfile layout will be something like the following:

1.

```
14     v.customize ["modifyvm", :id, "--ioapic", "on"]
15   end
16
17   # Varnish.
18   config.vm.define "varnish" do |varnish|
19     varnish.vm.hostname = "varnish.dev"
20     varnish.vm.network :private_network, ip: "192.168.2.2"
21   end
22
23   # Apache.
24   config.vm.define "www1" do |www1|
25     www1.vm.hostname = "www1.dev"
26     www1.vm.network :private_network, ip: "192.168.2.3"
27
28     www1.vm.provision "shell",
29       inline: "sudo yum update -y"
30
31     www1.vm.provider :virtualbox do |v|
32       v.customize ["modifyvm", :id, "--memory", 256]
33     end
34   end
35
36   # Apache.
37   config.vm.define "www2" do |www2|
38     www2.vm.hostname = "www2.dev"
39     www2.vm.network :private_network, ip: "192.168.2.4"
40
41     www2.vm.provision "shell",
42       inline: "sudo yum update -y"
43
44     www2.vm.provider :virtualbox do |v|
45       v.customize ["modifyvm", :id, "--memory", 256]
46     end
47   end
48
49   # MySQL.
50   config.vm.define "db1" do |db1|
51     db1.vm.hostname = "db1.dev"
52     db1.vm.network :private_network, ip: "192.168.2.5"
53   end
54
55   # MySQL.
```

```

56 config.vm.define "db2" do |db2|
57   db2.vm.hostname = "db2.dev"
58   db2.vm.network :private_network, ip: "192.168.2.6"
59 end
60
61 # Memcached.
62 config.vm.define "memcached" do |memcached|
63   memcached.vm.hostname = "memcached.dev"
64   memcached.vm.network :private_network, ip: "192.168.2.7"
65
66 # Run Ansible provisioner once for all VMs at the end.
67 memcached.vm.provision "ansible" do |ansible|
68   ansible.playbook = "configure.yml"
69   ansible.inventory_path = "inventories/vagrant/inventory"
70   ansible.limit = "all"
71   ansible.extra_vars = {
72     ansible_ssh_user: 'vagrant',
73     ansible_ssh_private_key_file: "~/.vagrant.d/insecure_private_key"
74   }
75 end
76 end
77 end

```

Most of the Vagrantfile is straightforward, and similar to other examples used in this book. The last block of code, which defines the `ansible` provisioner configuration, contains three extra values that are important for our purposes:

```

1   ansible.inventory_path = "inventories/vagrant/inventory"
2   ansible.limit = "all"
3   ansible.extra_vars = {
4     ansible_ssh_user: 'vagrant',
5     ansible_ssh_private_key_file: "~/.vagrant.d/insecure_private_key"
6   }

```

1. `ansible.inventory_path` defines an inventory file to be used with the `ansible.playbook`. You could certainly create a dynamic inventory script for use with Vagrant, but because we know the IP addresses ahead of time, and are expecting a few specially-crafted inventory group names, it's simpler to build the inventory file for Vagrant provisioning by hand (we'll do this next).
2. `ansible.limit` is set to `all` so Vagrant knows it should run the Ansible playbook connected to all VMs, and not just the current VM. You could technically use `ansible.limit` with a provisioner configuration for each of the individual VMs, and just run the VM-specific

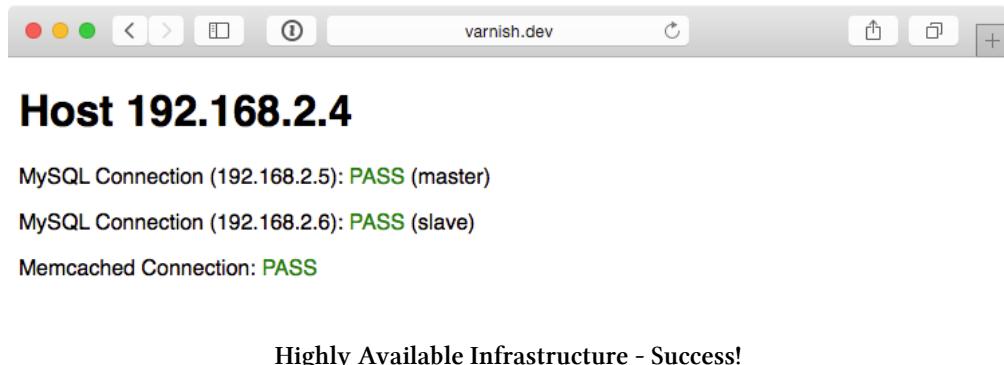
playbook through Vagrant, but our live production infrastructure will be using one playbook to configure all the servers, so we'll do the same locally.

3. `ansible.extra_vars` contains the vagrant SSH user configuration for Ansible. It's more standard to include these settings in a static inventory file or use Vagrant's automatically-generated inventory file, but it's easiest to set them once for all servers here.

Before running `vagrant up` to see the fruits of our labor, we need to create an inventory file for Vagrant at `inventories/vagrant/inventory`:

```
1 [lamp-varnish]
2 192.168.2.2
3
4 [lamp-www]
5 192.168.2.3
6 192.168.2.4
7
8 [a4d.lamp.db.1]
9 192.168.2.5
10
11 [lamp-db]
12 192.168.2.5
13 192.168.2.6
14
15 [lamp-memcached]
16 192.168.2.7
```

Now `cd` into the project's root directory, run `vagrant up`, and after ten or fifteen minutes, load `http://192.168.2.2/` in your browser. Voila!



You should see something like the above screenshot; the PHP app displays the current app server's IP address, the individual MySQL servers' status, and the Memcached server status. Refresh the page a few times to verify Varnish is distributing requests randomly between the two app servers.

We have local infrastructure development covered, and Ansible makes it easy to use the exact same configuration to build our infrastructure in the cloud.

Provisioner Configuration: DigitalOcean

In Chapter 7, we learned provisioning and configuring DigitalOcean droplets in an Ansible playbook is fairly simple. But we need to take provisioning a step further by provisioning multiple droplets (one for each server in our infrastructure) and dynamically grouping them so we can configure them after they are booted and online.

For the sake of flexibility, let's create a playbook for our DigitalOcean droplets in `provisioners/digitalocean.yml`. This will allow us to add other provisioner configurations later, alongside the `digitalocean.yml` playbook. As with our example in Chapter 7, we will use a local connection to provision cloud instances. Begin the playbook with:

```
1 ---  
2 - hosts: localhost  
3   connection: local  
4   gather_facts: false
```

Next we need to define some metadata to describe each of our droplets. For simplicity's sake, we'll inline the `droplets` variable in this playbook:

```
6 vars:  
7   droplets:  
8     - { name: a4d.lamp.varnish, group: "lamp-varnish" }  
9     - { name: a4d.lamp.www.1, group: "lamp-www" }  
10    - { name: a4d.lamp.www.2, group: "lamp-www" }  
11    - { name: a4d.lamp.db.1, group: "lamp-db" }  
12    - { name: a4d.lamp.db.2, group: "lamp-db" }  
13    - { name: a4d.lamp.memcached, group: "lamp-memcached" }
```

Each droplet is an object with two keys:

- `name`: The name of the Droplet for DigitalOcean's listings and Ansible's host inventory.
- `group`: The Ansible inventory group for the droplet.

Next we need to add a task to create the droplets, using the `droplets` list as a guide, and as part of the same task, register each droplet's information in a separate dictionary, `created_droplets`:

```
15 tasks:
16   - name: Provision DigitalOcean droplets.
17     digital_ocean:
18       state: "{{ item.state | default('present') }}"
19       command: droplet
20       name: "{{ item.name }}"
21       private_networking: yes
22       size_id: "{{ item.size | default(66) }}" # 512mb
23       image_id: "{{ item.image | default(6372108) }}" # CentOS 6 x64.
24       region_id: "{{ item.region | default(4) }}" # NYC2
25       ssh_key_ids: "{{ item.ssh_key | default('138954') }}" # gearlingguy
26       unique_name: yes
27     register: created_droplets
28     with_items: droplets
```

Many of the options (e.g. `size_id`) are defined as `{{ item.property | default('default_value') }}`, which allows us to use optional variables per droplet. For any of the defined droplets, we could add `size_id: 72` (or whatever valid value you'd like), and it would override the default value set in the task.



You could specify an SSH public key per droplet, or (as in this instance) use the same key for all hosts by providing a default. In this case, I added an SSH key to my DigitalOcean account, then used the DigitalOcean API to retrieve the key's numeric ID (as described in the previous chapter).

It's best to use key-based authentication and add at least one SSH key to your DigitalOcean account so Ansible can connect using keys instead of insecure passwords, especially since these instances will be created with only a root account.

We loop through all the defined `droplets` using `with_items: droplets`, and after each droplet is created add the droplet's metadata (name, IP address, etc.) to the `created_droplets` variable. Next, we'll loop through that variable to build our inventory on-the-fly so our configuration applies to the correct servers:

```
30      - name: Add DigitalOcean hosts to their respective inventory groups.
31        add_host:
32          name: "{{ item.1.droplet.ip_address }}"
33          groups: "do,{{ droplets[item.0].group }},{{ item.1.droplet.name }}"
34          # You can dynamically add inventory variables per-host.
35          ansible_ssh_user: root
36          mysql_replication_mole: >
37            "{{ 'master' if (item.1.droplet.name == 'a4d.lamp.db.1') }}"
38
```

```
43 - hosts: do
44   remote_user: root
45   gather_facts: no
46
47   tasks:
48     - name: Wait for port 22 to become available.
49       local_action: "wait_for port=22 host={{ inventory_hostname }}"
```

Once we know port 22 is reachable, we know the droplet is up and ready for configuration.

We're *almost* ready to provision and configure our entire infrastructure on DigitalOcean, but we need to create one last playbook to tie everything together. Create `provision.yml` in the project root with the following contents:

```
1 ---
2 - include: provisioners/digitalocean.yml
3 - include: configure.yml
```

That's it! Now, assuming you set the environment variables `DO_CLIENT_ID` and `DO_API_KEY`, you can run `$ ansible-playbook provision.yml` to provision and configure the infrastructure on DigitalOcean.

The entire process should take about 15 minutes, and once it's complete, you should see something like:

```
PLAY RECAP ****
107.170.27.137      : ok=19    changed=13    unreachable=0    failed=0
107.170.3.23        : ok=13    changed=8     unreachable=0    failed=0
107.170.51.216      : ok=40    changed=18    unreachable=0    failed=0
107.170.54.218      : ok=27    changed=16    unreachable=0    failed=0
162.243.20.29       : ok=24    changed=15    unreachable=0    failed=0
192.241.181.197     : ok=40    changed=18    unreachable=0    failed=0
localhost            : ok=2     changed=1     unreachable=0    failed=0
```

Visit the IP address of the varnish server and you should be greeted with a status page similar to the one generated by the Vagrant-based infrastructure:



Host 107.170.51.216

MySQL Connection (162.243.20.29): **PASS** (master)

MySQL Connection (107.170.54.218): **PASS** (slave)

Memcached Connection: **PASS**

Highly Available Infrastructure on DigitalOcean.

Because everything in this playbook is idempotent, running `$ ansible-playbook provision.yml` again should report no changes, and helps you verify that everything is running correctly.

Ansible will also rebuild and reconfigure any droplets that may be missing from your infrastructure. If you're daring, and want to test this feature, just log into your DigitalOcean account, delete one of the droplets just created by this playbook (maybe one of the two app servers), then run the playbook again.

Now that we've tested our infrastructure on DigitalOcean, we can destroy the droplets just as easily (change the `state` parameter in `provisioners/digitalocean.yml` to default to '`'absent'`' and run `$ ansible-playbook provision.yml` again).

Next up, we'll build the infrastructure a third time—on Amazon's infrastructure.

Provisioner Configuration: Amazon Web Services (EC2)

For Amazon Web Services, provisioning works slightly different. Amazon has a broader ecosystem of services surrounding EC2 instances, and for our particular example, we will need to configure security groups prior to provisioning instances.

To begin, create `aws.yml` inside the `provisioners` directory and begin the playbook the same ways as with DigitalOcean:

```
1 ---  
2 - hosts: localhost  
3   connection: local  
4   gather_facts: false
```

EC2 instances use security groups as an AWS-level firewall (which operates outside the individual instance's OS). We will need to define a list of `security_groups` alongside our EC2 instances. First, the `instances`:

```
6 vars:
7   instances:
8     - {
9       name: a4d.lamp.varnish,
10      group: "lamp-varnish",
11      security_group: ["default", "a4d_lamp_http"]
12    }
13    - {
14      name: a4d.lamp.www.1,
15      group: "lamp-www",
16      security_group: ["default", "a4d_lamp_http"]
17    }
18    - {
19      name: a4d.lamp.www.2,
20      group: "lamp-www",
21      security_group: ["default", "a4d_lamp_http"]
22    }
23    - {
24      name: a4d.lamp.db.1,
25      group: "lamp-db",
26      security_group: ["default", "a4d_lamp_db"]
27    }
28    - {
29      name: a4d.lamp.db.2,
30      group: "lamp-db",
31      security_group: ["default", "a4d_lamp_db"]
32    }
33    - {
34      name: a4d.lamp.memcached,
35      group: "lamp-memcached",
36      security_group: ["default", "a4d_lamp_memcached"]
37  }
```

Inside the `instances` variable, each instance is an object with three keys:

- `name`: The name of the instance, which we'll use to tag the instance and ensure only one instance is created per name.
- `group`: The Ansible inventory group in which the instance should belong.
- `security_group`: A list of security groups into which the instance will be placed. The `default` security group comes is added to your AWS account upon creation, and has one rule to allow outgoing traffic on any port to any IP address.



If you use AWS exclusively, it would be best to autoscaling groups and change the design of this infrastructure a bit. For this example, we just need to ensure that the six instances we explicitly define are created, so we're using particular names and an `exact_count` to enforce the 1:1 relationship.

With our instances defined, we'll next define a `security_groups` variable containing all the required security group configuration for each server:

```
39    security_groups:
40      - name: a4d_lamp_http
41        rules:
42          - { proto: tcp, from_port: 80, to_port: 80, cidr_ip: 0.0.0.0/0 }
43          - { proto: tcp, from_port: 22, to_port: 22, cidr_ip: 0.0.0.0/0 }
44        rules_egress: []
45      - name: a4d_lamp_db
46        rules:
47          - { proto: tcp, from_port: 3306, to_port: 3306, cidr_ip: 0.0.0.0/0 }
48          - { proto: tcp, from_port: 22, to_port: 22, cidr_ip: 0.0.0.0/0 }
49        rules_egress: []
50      - name: a4d_lamp_memcached
51        rules:
52          - { proto: tcp, from_port: 11211, to_port: 11211, cidr_ip: 0.0.0.0/0 }
53          - { proto: tcp, from_port: 22, to_port: 22, cidr_ip: 0.0.0.0/0 }
54        rules_egress: []
```

Each security group has a `name` (which was used to identify the security group in the `instances` list), `rules` (a list of firewall rules like protocol, ports, and IP ranges to limit *incoming* traffic), and `rules_egress` (a list of firewall rules to limit *outgoing* traffic).

We need three security groups: `a4d_lamp_http` to open port 80, `a4d_lamp_db` to open port 3306, and `a4d_lamp_memcached` to open port 11211.

Now that we have all the data we need to set up security groups and instances, the first task needs to create or verify the existence of the security groups:

```

56 tasks:
57   - name: Configure EC2 Security Groups.
58     ec2_group:
59       name: "{{ item.name }}"
60       description: Example EC2 security group for A4D.
61       region: "{{ item.region | default('us-west-2') }}" # Oregon
62       state: present
63       rules: "{{ item.rules }}"
64       rules_egress: "{{ item.rules_egress }}"
65     with_items: security_groups

```

The `ec2_group` requires a name, region, and rules for each security group. Security groups will be created if they don't exist, modified to match the supplied values if they do exist, or verified if they exist and match the given values.

With the security groups configured, we can provision the defined EC2 instances by looping through instances with the `ec2` module:

```

67   - name: Provision EC2 instances.
68     ec2:
69       key_name: "{{ item.ssh_key | default('jeff_mba_home') }}"
70       instance_tags:
71         inventory_group: "{{ item.group | default('') }}"
72         inventory_host: "{{ item.name | default('') }}"
73       group: "{{ item.security_group | default('') }}"
74       instance_type: "{{ item.type | default('t2.micro') }}" # Free Tier
75       image: "{{ item.image | default('ami-11125e21') }}" # RHEL6 x64 hvm
76       region: "{{ item.region | default('us-west-2') }}" # Oregon
77       wait: yes
78       wait_timeout: 500
79       exact_count: 1
80       count_tag:
81         inventory_group: "{{ item.group | default('') }}"
82         inventory_host: "{{ item.name | default('') }}"
83     register: created_instances
84     with_items: instances

```

This example is slightly more complex than the DigitalOcean example, and a few parts warrant a deeper look:

- EC2 allows SSH keys to be defined by name—in my case, I have a key `jeff_mba_home` in my AWS account. You should set the `key_name` default to a key that you have in your account.

- Instance tags are tags that AWS will attach to your instance, for categorization purposes. By giving a list of keys and values, I can then use that list later in the count_tag parameter.
- t2.micro was used as the default instance type, since it falls within EC2's free tier usage. If you just set up an account and keep all AWS resource usage within free tier limits, you won't be billed anything.
- exact_count and count_tag work together to ensure AWS provisions only one of each of the instances we defined. The count_tag tells the ec2 module to match the given group + host and then exact_count tells the module to only provision 1 instance. If you wanted to *remove* all your instances, you could set exact_count to 0 and run the playbook again.

Each provisioned instance will have its metadata added to the registered created_instances variable, which we'll use to build Ansible inventory groups for the server configuration playbooks.

```

86   - name: Add EC2 instances to their respective inventory groups.
87     add_host:
88       name: "{{ item.1.tagged_instances.0.public_ip }}"
89       groups: "aws,{{ item.1.item.group }},{{ item.1.item.name }}"
90       # You can dynamically add inventory variables per-host.
91       ansible_ssh_user: ec2-user
92       mysql_replication_role: >
93         {{ 'master' if (item.1.item.name == 'a4d.lamp.db.1')
94           else 'slave' }}
95       mysql_server_id: "{{ item.0 }}"
96       when: item.1.instances is defined
97       with_indexed_items: created_instances.results

```

This add_host example is slightly simpler than the one for DigitalOcean, because AWS attaches metadata to EC2 instances which we can re-use when building groups or hostnames (e.g. item.1.item.group). We don't have to use list indexes to fetch group names from the original instances variable.

We still use with_indexed_items so we can use the index to generate a unique ID per server for use in building the MySQL master-slave replication.

The final step in provisioning the EC2 instances is to ensure we can connect to them before continuing, and to set selinux into permissive mode so the configuration we supply will work correctly.

```

86 # Run some general configuration on all AWS hosts.
87 - hosts: aws
88   gather_facts: false
89
90   tasks:
91     - name: Wait for port 22 to become available.
92       local_action: "wait_for port=22 host={{ inventory_hostname }}"
93
94     - name: Set selinux into 'permissive' mode.
95       selinux: policy=targeted state=permissive
96       sudo: yes

```

Since we defined `ansible_ssh_user` as `ec2-user` in the dynamically-generated inventory above, we need to ensure the `selinux` task runs with `sudo` explicitly.

Now, modify the `provision.yml` file in the root of the project folder, and change the provisioners include to look like the following:

```

1 ---
2 - include: provisioners/aws.yml
3 - include: configure.yml

```

Assuming the environment variables `AWS_ACCESS_KEY_ID` and `AWS_SECRET_ACCESS_KEY` are set in your current terminal session, you can run `$ ansible-playbook provision.yml` to provision and configure the infrastructure on AWS.

The entire process should take about 15 minutes, and once it's complete, you should see something like:

```

PLAY RECAP ****
54.148.100.44      : ok=24    changed=16    unreachable=0    failed=0
54.148.120.23      : ok=40    changed=19    unreachable=0    failed=0
54.148.41.134      : ok=40    changed=19    unreachable=0    failed=0
54.148.56.137      : ok=13    changed=9     unreachable=0    failed=0
54.69.160.32       : ok=27    changed=17    unreachable=0    failed=0
54.69.86.187       : ok=19    changed=14    unreachable=0    failed=0
localhost           : ok=3     changed=1     unreachable=0    failed=0

```

Visit the IP address of the varnish server (the first server configured) and you should be greeted with a status page similar to the one generated by the Vagrant and DigitalOcean-based infrastructure:



Host 54.148.120.23

MySQL Connection (54.148.100.44): **PASS** (master)

MySQL Connection (54.69.160.32): **PASS** (slave)

Memcached Connection: **PASS**

Highly Available Infrastructure on AWS EC2.

As with the earlier examples, running `ansible-playbook provision.yml` again should produce no changes, because everything in this playbook is idempotent. And if one of your instances were terminated, running the playbook again would recreate and reconfigure the instance in a few minutes.

To terminate all the provisioned instances, you can change the `exact_count` in the `ec2` task to `0`, and run `$ ansible-playbook provision.yml` again.

Summary

In the above example, an entire highly-available PHP application infrastructure was defined in a series of short Ansible playbooks, and then provisioning configuration was created to build the infrastructure on either local VMs, DigitalOcean droplets, or AWS EC2 instances.

Once you start working on building infrastructure this way—abstracting individual servers, then abstracting cloud provisioning—you’ll start to see some of Ansible’s true power in being more than just a configuration management tool. Imagine being able to create your own multi-datacenter, multi-provider infrastructure with Ansible and some basic configuration.

While Amazon, DigitalOcean, Rackspace and other hosting providers have their own tooling and unique infrastructure merits, the agility and flexibility afforded by building infrastructure in a provider-agnostic fashion lets you treat hosting providers as commodities, and gives you freedom to build more reliable, performant, and simple application infrastructure.

Even if you plan on running everything within one hosting provider’s network (or in a private cloud, or even on a few bare metal servers), Ansible provides deep stack-specific integration so you can do whatever you need to do and manage the provider’s services within your playbooks.



You can find the entire contents of this example in the [Ansible for DevOps GitHub repository⁸⁹](#), in the `lamp-infrastructure` directory.

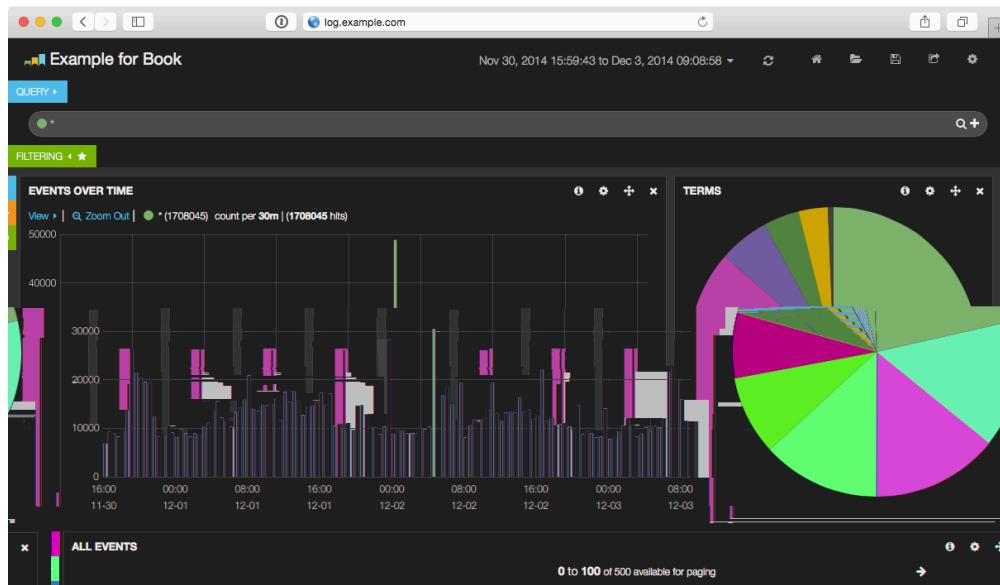
⁸⁹<https://github.com/geerlingguy/ansible-for-devops>

ELK Logging with Ansible

Though application, database, and backup servers may be some of the most mission-critical components of a well-rounded infrastructure, one area that is equally important is a decent logging system.

In the old days, when one or two servers could handle an entire website or application, you could work with built-in logfiles and rsyslog to troubleshoot an issue or check trends in performance, errors, or overall traffic. With a typical modern infrastructure—like the example above, with six separate servers—it pays dividends to find a better solution for application, server, and firewall/authentication logging. Plain text files, logrotate, and grep don't cut it anymore.

Among various modern logging and reporting toolsets, the ‘ELK’ stack (Elasticsearch, Logstash, and Kibana) has come to the fore as one of the best-performing and easiest-to-configure open source centralized logging solutions.



An example Kibana logging dashboard.

In our example, we'll configure a single ELK server to handle aggregation, searching, and graphical display of logged data from a variety of other servers, and give some common configuration examples to send common system logs, webserver logs, etc.

ELK Playbook

Just like our previous example, we're going to let a few roles from Ansible Galaxy do the heavy lifting of actually installing and configuring Elasticsearch, Logstash, and Kibana. If you're interested in reading through the roles that do this work, feel free to peruse them after you've downloaded them.

In this example, rather than walking through each role and variable in detail, I'm going to highlight the important parts, but then jump immediately into how you can use this base server to aggregate logs, then how to point your other servers' log files to it using Logstash Forwarder.

Here's our main playbook, saved as provisioning/elk/playbook.yml:

```
1 - hosts: logs
2   gather_facts: yes
3
4   vars_files:
5     - vars/main.yml
6
7   pre_tasks:
8     - name: Update apt cache if needed.
9       apt: update_cache=yes cache_valid_time=86400
10
11  roles:
12    - gearlingguy.java
13    - gearlingguy.nginx
14    - gearlingguy.elasticsearch
15    - gearlingguy.elasticsearch-curator
16    - gearlingguy.kibana
17    - gearlingguy.logstash
18    - gearlingguy.logstash-forwarder
```

This assumes you have a logs group in your inventory with at least one server listed. The playbook includes a vars file located in provisioning/elk/vars/main.yml, so create that file, and then put the following inside:

```
1 ---
2 java_packages:
3   - openjdk-7-jdk
4
5 nginx_user: www-data
6 nginx_worker_connections: 1024
7 nginx_remove_default_vhost: true
8
9 kibana_server_name: logs
10 kibana_username: kibana
11 kibana_password: password
12
13 logstash_monitor_local_syslog: false
14 logstash_forwarder_files:
```

```
15  - paths:
16    - /var/log/auth.log
17  fields:
18    type: syslog
```

You'll want to use a different password besides 'password' for `kibana_password`. Other options are straightforward, with the exception of the two `logstash_*` variables.

The first variable tells the `geerlingguy.logstash` role to ignore the local syslog file (in this case, we're only interested in logging authorization attempts through the local `auth.log`).

The second variable gives the `geerlingguy.logstash-forwarder` role a list of files to monitor, along with metadata to tell logstash what kind of file is being monitored. In this case, we are only worried about the `auth.log` file, and we know it's a syslog-style file. (Logstash needs to know what kind of file you're monitoring so it can parse the logged messages correctly).

If you want to get this ELK server up and running quickly, you can create a local VM using Vagrant like you have in most other examples in the book. Create a `Vagrantfile` in the same directory as the provisioning folder, with the following contents:

```
1  # -*- mode: ruby -*-
2  # vi: set ft=ruby :
3
4  VAGRANTFILE_API_VERSION = "2"
5
6  Vagrant.configure(VAGRANTFILE_API_VERSION) do |config|
7    config.vm.box = "geerlingguy/ubuntu1204"
8
9    config.vm.provider :virtualbox do |v|
10      v.customize ["modifyvm", :id, "--natdnshostresolver1", "on"]
11      v.customize ["modifyvm", :id, "--memory", 1024]
12      v.customize ["modifyvm", :id, "--cpus", 2]
13      v.customize ["modifyvm", :id, "--ioapic", "on"]
14    end
15
16    # ELK server.
17    config.vm.define "logs" do |logs|
18      logs.vm.hostname = "logs"
19      logs.vm.network :private_network, ip: "192.168.9.90"
20
21      logs.vm.provision :ansible do |ansible|
22        ansible.playbook = "provisioning/elk/playbook.yml"
23        ansible.inventory_path = "provisioning/elk/inventory"
24        ansible.sudo = true
```

```

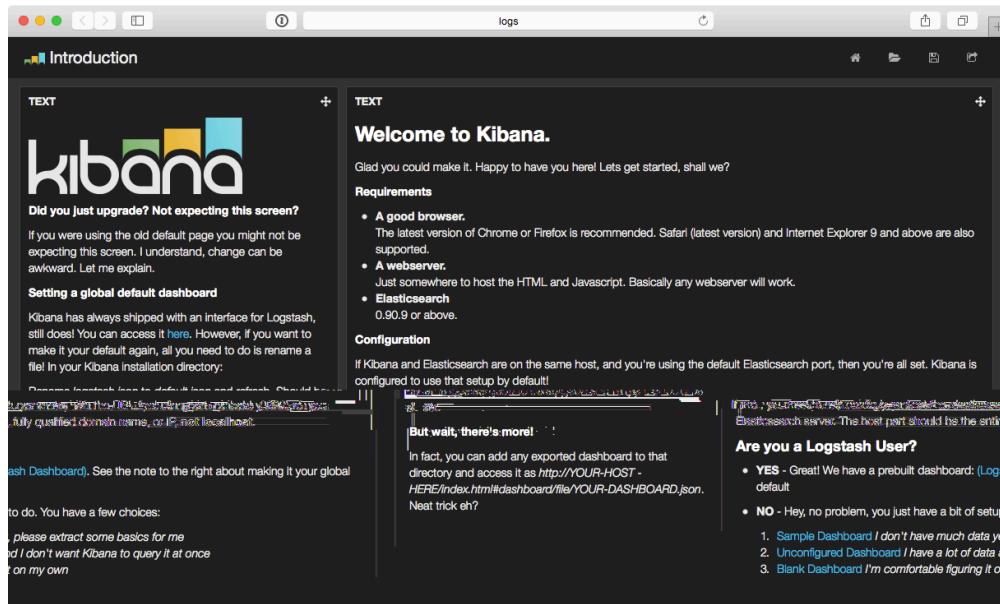
25   end
26 end
27
28 end

```

This Vagrant configuration expects an inventory file at provisioning/elk/inventory, so quickly create one with the following contents:

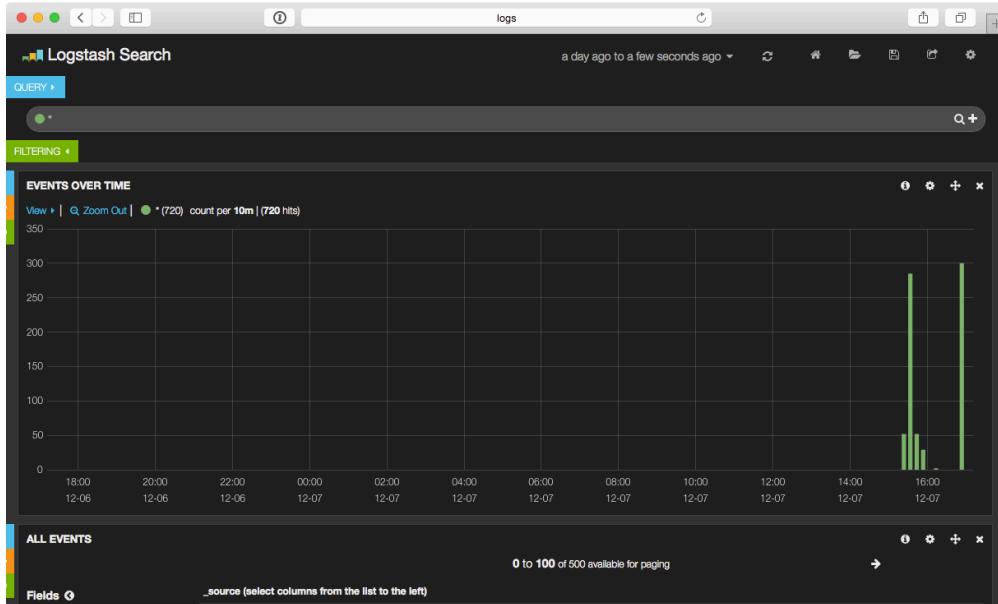
```
1 logs ansible_ssh_host=192.168.9.90 ansible_ssh_port=22
```

Now, run vagrant up. The build should take about five minutes, and upon completion, if you add a line like logs 192.168.9.90 to your /etc/hosts file, you can visit <http://logs/> in your browser and see Kibana's default homepage:



Kibana's default homepage.

Kibana helpfully links to an example dashboard for Logstash (under the “Are you a Logstash User?” section), and if you select it, you should see a live dashboard that shows logged activity for the past day:



Kibana's default Logstash dashboard.

This example won't dive too deep into customizing Kibana's dashboard customization, since there are many guides to using Kibana available freely, including [Kibana's official guide⁹⁰](#). For our purposes, we'll use the default dashboard.



This example uses Kibana 3.x, but a stable release of Kibana 4.x is on the horizon (as of early 2015). Some of the screenshots may show a different interface than the latest release, but this book will likely be updated with newer screenshots and updated guides once the 4.x release comes out.

Forwarding Logs from Other Servers

It's great that we have the ELK stack running; Elasticsearch will store and make available log data with one search index per day, Logstash will listen for log entries, Logstash Forwarder will send entries in `/var/log/auth.log` to Logstash, and Kibana will organize the logged data with useful visualizations.

Configuring additional servers to direct their logs to our new Logstash server is fairly simple using Logstash Forwarder. The basic steps we'll follow are:

1. Set up another server in the Vagrantfile.
2. Set up an Ansible playbook to install and configure Logstash Forwarder alongside the application running on the server.

⁹⁰<http://www.elasticsearch.org/guide/en/kibana/current/index.html>

3. Boot the server and watch as the logs are forwarded to the main ELK server.

Let's begin by creating a new Nginx web server. It's useful to monitor webserver access logs for a variety of reasons, not the least of which is to watch for traffic spikes and increases in non-200 responses for certain resources. Add the following server definition inside the Vagrantfile, just after the end of the ELK server definition:

```
28  # Web server.
29  config.vm.define "webs" do |webs|
30    webs.vm.hostname = "webs"
31    webs.vm.network :private_network, ip: "192.168.9.91"
32
33    webs.vm.provision :ansible do |ansible|
34      ansible.playbook = "provisioning/web/playbook.yml"
35      ansible.inventory_path = "provisioning/web/inventory"
36      ansible.sudo = true
37    end
38  end
```

We'll next set up the simple playbook to install and configure both Nginx and Logstash Forwarder, at provisioning/web/playbook.yml:

```
1  - hosts: webs
2    gather_facts: yes
3
4    vars_files:
5      - vars/main.yml
6
7    pre_tasks:
8      - name: Update apt cache if needed.
9        apt: update_cache=yes cache_valid_time=86400
10
11   roles:
12     - geerlingguy.nginx
13     - geerlingguy.logstash-forwarder
14
15   tasks:
16     - name: Set up virtual host for testing.
17       copy:
18         src: files/example.conf
19         dest: /etc/nginx/conf.d/example.conf
20         owner: root
```

```

21     group: root
22     mode: 0644
23     notify: restart nginx

```

This playbook installs the `geerlingguy.nginx` and `geerlingguy.logstash-forwarder` roles, and in the tasks, there is an additional task to configure one virtualhost in a Nginx configuration directory, via the file `example.conf`. Create that file now (at the path `provisioning/web/files/example.conf`), and define one Nginx virtualhost for our testing:

```

1 server {
2     listen 80 default_server;
3
4     root /usr/share/nginx/www;
5     index index.html index.htm;
6
7     access_log /var/log/nginx/access.log combined;
8     error_log /var/log/nginx/error.log debug;
9 }

```

Since this is the only server definition, and it's set as the `default_server` on port 80, all requests will be directed to it. We routed the `access_log` to `/var/log/nginx/access.log`, and told Nginx to write log entries using the `combined` format, which is what our Logstash server will expect for nginx access logs.

Next, set up the required variables to tell the `nginx` and `logstash-forwarder` roles how to configure their respective services. Inside `provisioning/web/vars/main.yml`:

```

1 ---
2 nginx_user: www-data
3 nginx_worker_connections: 1024
4 nginx_remove_default_vhost: true
5
6 logstash_forwarder_logstash_server: 192.168.9.90
7 logstash_forwarder_logstash_server_port: 5000
8
9 logstash_forwarder_files:
10   - paths:
11     - /var/log/secure
12   fields:
13     type: syslog
14   - paths:
15     - /var/log/nginx/access.log
16   fields:
17     type: nginx

```

The `nginx` variables ensure Nginx will run optimally on our Ubuntu server, and remove the default virtualhost entry. The `logstash_forwarder` variables tell `geerlingguy.logstash-forwarder` what logs to forward to our central log server:

- `logstash_forwarder_logstash_server` and `_port`: Defines the server IP or domain and port to which logs should be transported.
- `logstash_forwarder_files`: Defines a list of `paths` and `fields`, which identify a file or list of files to be transported to the log server, along with a type for the files. In this case, the authentication log (`/var/log/secure`) is a `syslog`-formatted log file, and `/var/log/nginx/access.log` is of type `nginx` (which will be parsed correctly on the Logstash server since it's in the combined log format popularized by Apache).



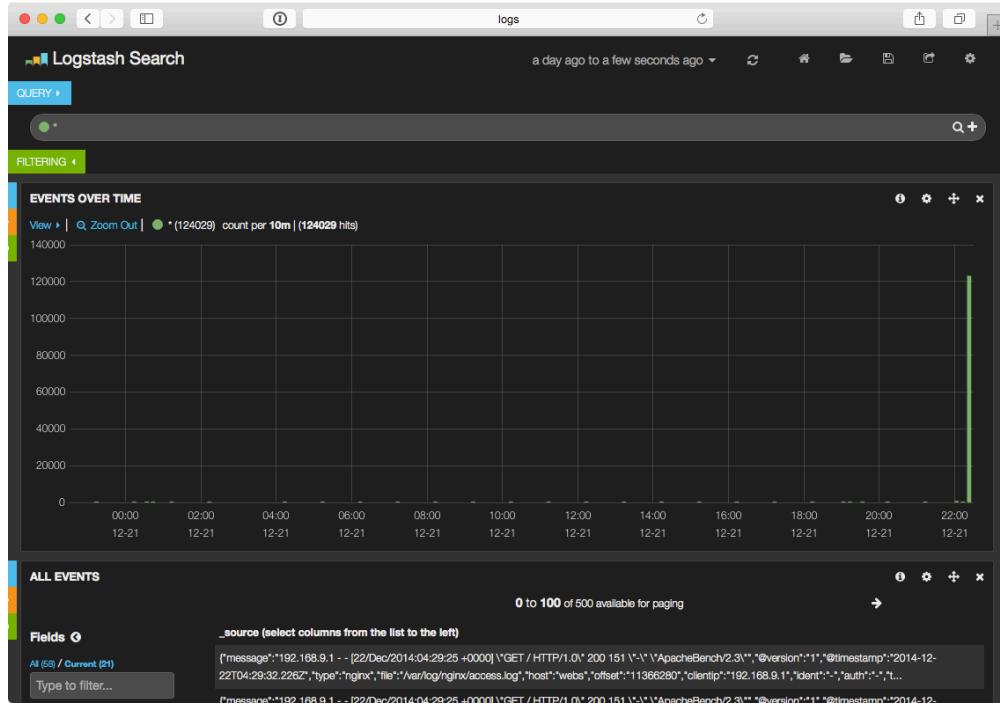
Note that this demonstration configuration is not using a custom certificate to authenticate logging connections. You should normally configure your own secure certificate and give the `logstash-forwarder` role the path to the certificate using the `logstash_forwarder_ssl_certificate_file` variable. If you use the example provided with the project, you could expose your logging infrastructure to the outside, plus you'll get a *****SECURITY RISK***** warning in the logs every time the `Logstash` role is run.

To allow Vagrant to pass the proper connection details to Ansible, create `provisioning/web/inventory` with the `webs` host details:

```
1 webs ansible_ssh_host=192.168.9.91 ansible_ssh_port=22
```

Run `vagrant up` again. Vagrant should verify that the first server (`logs`) is running, then create and run the Ansible provisioner on the newly-defined `webs` Nginx server.

You can load `http://192.168.9.91/` or `http://webs/` in your browser, and you should see a `Welcome to nginx!` message on the page. You can refresh the page a few times, then switch back over to `http://logs/` to view some new log entries on the ELK server:



Entries populating the Logstash Search Kibana dashboard.



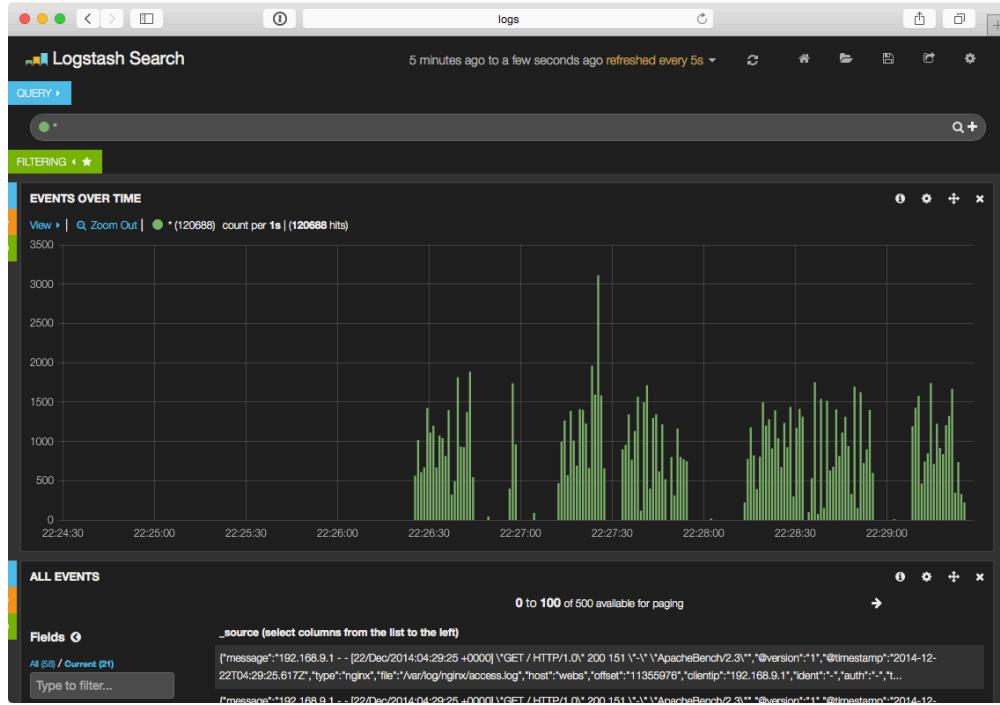
If you refresh the page a few times, and no entries show up in the Kibana Logstash dashboard, it could be that Nginx is buffering the log entries. In this case, keep refreshing a while (so you generate a few dozen or hundred entries), and Nginx will eventually write the entries to disk (thus allowing Logstash Forwarder to convey the logs to the Logstash server). Read more about Nginx log buffering in the [Nginx's ngx_http_log_module documentation⁹¹](#).

A few requests being logged through logstash forwarder isn't all that exciting. Let's use the popular ab tool available most anywhere to put some load on the web server. On a modest MacBook Air, running the command below resulted in Nginx serving around 1,200 requests per second.

```
ab -n 20000 -c 50 http://webs/
```

During the course of the load test, I set Kibana to show only the past 5 minutes of log data, automatically refreshed every 5 seconds, and I could monitor the requests on the ELK server just a few seconds after they were served by Nginx:

⁹¹http://nginx.org/en/docs/http/ngx_http_log_module.html



Monitoring a deluge of Nginx requests in near-realtime.

Logstash Forwarder uses a highly-efficient TCP-like protocol, Lumberjack, to transmit log entries securely between servers. With the right tuning and scaling, you can efficiently process and display thousands of requests per second across your infrastructure! For most, even the simple example demonstrated above would adequately cover an entire infrastructure's logging and log analysis needs.

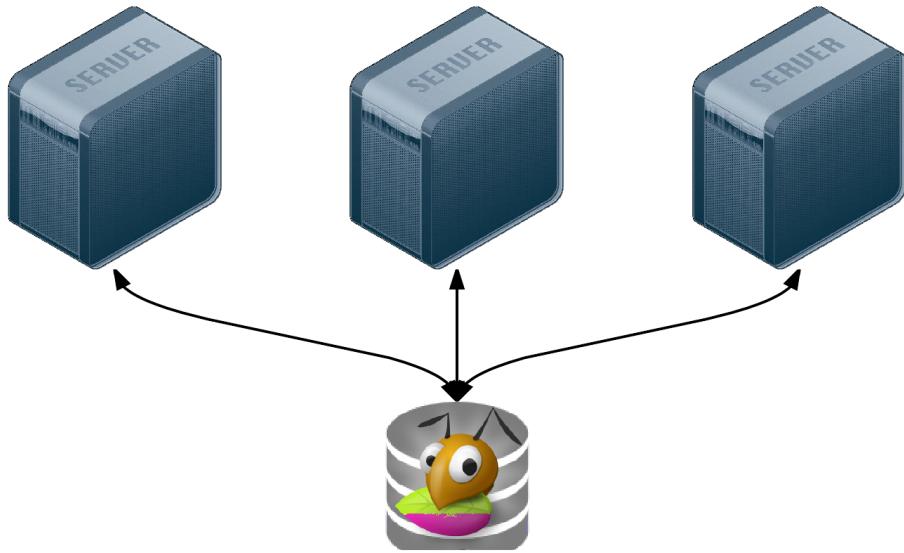
Summary

Log aggregation and analysis are two fields that see constant improvements and innovation. There are many SaaS products and proprietary solutions that can assist with logging, but few match the flexibility, security, and TCO of Elasticsearch, Logstash and Kibana.

Ansible is the simplest way to configure an ELK server and direct all your infrastructure's pertinent log data to the server.

GlusterFS Distributed File System Configuration with Ansible

Modern infrastructure often involves some amount of horizontal scaling; instead of having one giant server, with one storage volume, one database, one application instance, etc., most apps use two, four, ten, or dozens of servers.



GlusterFS is a distributed filesystem for servers.

Many applications can be scaled horizontally with ease, but what happens when you need shared resources, like files, application code, or other transient data, to be shared on all the servers? And how do you have this data scale out with your infrastructure, in a fast but reliable way? There are many different approaches to synchronizing or distributing files across servers:

- Set up rsync either on cron or via inotify to synchronize smaller sets of files on a regular basis.
- Store everything in a code repository (e.g. Git, SVN, etc.) and deploy files to each server using Ansible.
- Have one large volume on a file server and mount it via NFS or some other file sharing protocol.
- Have one master SAN that's mounted on each of the servers.
- Use a distributed file system, like Gluster, Lustre, Fraunhofer, or Ceph.

Some options are easier to set up than others, and all have benefits—and drawbacks. Rsync, git, or NFS offer simple initial setup, and low impact on filesystem performance (in many scenarios). But if you need more flexibility and scalability, less network overhead, and greater fault tolerance, you will have to consider something that requires more configuration (e.g. a distributed file system) and/or more hardware (e.g. a SAN).

GlusterFS is licensed under the AGPL license, has good documentation, and a fairly active support community (especially in the #gluster IRC channel). But to someone new to distributed file systems, it can be daunting to get set it up the first time.

Configuring Gluster - Basic Overview

To get Gluster working on a basic two-server setup (so you can have one folder that's synchronized and replicated across the two servers—allowing one server to go down completely, and the other to still have access to the files), you need to do the following:

1. Install Gluster server and client on each server, and start the server daemon.
2. (On both servers) Create a ‘brick’ directory (where Gluster will store files for a given volume).
3. (On both servers) Create a directory to be used as a mount point (a directory where you’ll have Gluster mount the shared volume).
4. (On both servers) Use `gluster peer probe` to have Gluster connect to the other server.
5. (On one server) Use `gluster volume create` to create a new Gluster volume.
6. (On one server) Use `gluster volume start` to start the new Gluster volume.
7. (On both servers) Mount the gluster volume (adding a record to `/etc/fstab` to make the mount permanent).

Additionally, you need to make sure you have the following ports open on both servers (so Gluster can communicate): TCP ports 111, 24007-24011, 49152-49153, and UDP port 111. (You need to add an additional TCP port in the 49xxx range for each extra server in your Gluster cluster.)

Configuring Gluster with Ansible

For demonstration purposes, we’ll set up a simple two-server infrastructure using Vagrant, and create a shared volume between the two, with two replicas (meaning all files will be replicated on each server). As your infrastructure grows, you can set other options for data consistency and transport according to your needs.

To build the two-server infrastructure locally, create a folder `gluster` containing the following `Vagrantfile`:

```
1 # -*- mode: ruby -*-
2 # vi: set ft=ruby :
3
4 Vagrant.configure("2") do |config|
5   # Base VM OS configuration.
6   config.vm.box = "geerlingguy/ubuntu1404"
7   config.vm.synced_folder '.', '/vagrant', disabled: true
8   config.ssh.insert_key = false
9
10  config.vm.provider :virtualbox do |v|
11    v.memory = 256
12    v.cpus = 1
```

```

13   end
14
15   # Define two VMs with static private IP addresses.
16   boxes = [
17     { :name => "gluster1", :ip => "192.168.29.2" },
18     { :name => "gluster2", :ip => "192.168.29.3" }
19   ]
20
21   # Provision each of the VMs.
22   boxes.each do |opts|
23     config.vm.define opts[:name] do |config|
24       config.vm.hostname = opts[:name]
25       config.vm.network :private_network, ip: opts[:ip]
26
27     # Provision both VMs using Ansible after the last VM is booted.
28     if opts[:name] == "gluster2"
29       config.vm.provision "ansible" do |ansible|
30         ansible.playbook = "playbooks/provision.yml"
31         ansible.inventory_path = "inventory"
32         ansible.limit = "all"
33       end
34     end
35   end
36 end
37
38 end

```

This configuration creates two servers, gluster1 and gluster2, and will run a playbook at playbooks/provision.yml on the servers defined in an inventory file in the same directory as the Vagrantfile.

Create the inventory file to help Ansible connect to the two servers:

```

1 [gluster]
2 192.168.29.2
3 192.168.29.3
4
5 [gluster:vars]
6 ansible_ssh_user=vagrant
7 ansible_ssh_private_key_file=~/vagrant.d/insecure_private_key

```

Now, create a playbook named provision.yml inside a playbooks directory:

```
1  ---
2  - hosts: gluster
3    sudo: yes
4
5  vars_files:
6    - vars.yml
7
8  roles:
9    - geerlingguy.firewall
10   - geerlingguy.glusterfs
11
12 tasks:
13   - name: Ensure Gluster brick and mount directories exist.
14     file: "path={{ item }} state=directory mode=0775"
15     with_items:
16       - "{{ gluster_brick_dir }}"
17       - "{{ gluster_mount_dir }}"
18
19   - name: Configure Gluster volume.
20     gluster_volume:
21       state: present
22       name: "{{ gluster_brick_name }}"
23       brick: "{{ gluster_brick_dir }}"
24       replicas: 2
25       cluster: "{{ groups.gluster | join(',') }}"
26       host: "{{ inventory_hostname }}"
27       force: yes
28       run_once: true
29
30   - name: Ensure Gluster volume is mounted.
31     mount:
32       name: "{{ gluster_mount_dir }}"
33       src: "{{ groups.gluster[0] }}:/{{ gluster_brick_name }}"
34       fstype: glusterfs
35       opts: "defaults,_netdev"
36       state: mounted
```

This playbook uses two roles to set up a firewall and install the required packages for GlusterFS to work. You can manually install both of the required roles with the command `ansible-galaxy install geerlingguy.firewall geerlingguy.glusterfs`, or add them to a `requirements.txt` file and install with `ansible-galaxy install -r requirements.txt`.

Gluster requires a ‘brick’ directory to use as a virtual filesystem, and our servers also need a directory

where the filesystem can be mounted, so the first `file` task ensures both directories exist (`gluster-brick_dir` and `gluster_mount_dir`). Since we need to use these directory paths more than once, we use variables which will be defined later, in `vars.yml`.

Ansible's `gluster_volume` module (added in Ansible 1.9) does all the hard work of probing peer servers, setting up the brick as a Gluster filesystem, and configuring the brick for replication. Some of the most important configuration parameters for the `gluster_volume` module include:

- `state`: Setting this to `present` makes sure the brick is present. It will also start the volume when it is first created by default, though this behavior can be overridden by the `start_on_create` option.
- `name` and `brick` give the Gluster brick a name and location on the server, respectively. In this example, the brick will be located on the boot volume, so we also have to add `force: yes`, or Gluster will complain about not having the brick on a separate volume.
- `replicas` tells Gluster how many replicas to ensure exist; this number can vary depending on how many servers you have in the brick's `cluster`, and how much data redundancy you require. Setting this 1:1 with the number of servers in your infrastructure means there's a full replica on each server, which can be good for read-heavy volumes, but worse for write-heavy volumes.
- `cluster` defines all the hosts which will contain the distributed filesystem. In this case, all the `gluster` servers in our Ansible inventory should be included, so we use a Jinja2 `join` filter to join all the addresses into a list.
- `host` sets the host for peer probing explicitly. If you don't set this, you can sometimes get errors on brick creation, depending on your network configuration.

We only need to run the `gluster_volume` module once for all the servers, so we add `run_once: true`.

The last task ensures the Gluster volume is mounted on each of the servers, in the `gluster_mount_dir`, using Ansible's `mount` module.

The last step is to define all the variables used in the playbook. Create a `vars.yml` file inside the `playbooks` directory, with the following variables defined:

```
1  ---
2  # Firewall configuration.
3  firewall_allowed_tcp_ports:
4      - 22
5      # For Gluster.
6      - 111
7      # Port-mapper for Gluster 3.4+.
8      # - 2049
9      # Gluster Daemon.
```

```
10    - 24007
11    # 24009+ for Gluster <= 3.3; 49152+ for Gluster 3.4+ (one port per server).
12    - 24009
13    - 24010
14    - 24011
15    # Gluster inline NFS server.
16    - 38465
17    - 38466
18    - 38467
19  firewall_allowed_udp_ports:
20    - 111
21
22  # Gluster configuration.
23  gluster_mount_dir: /mnt/gluster
24  gluster_brick_dir: /srv/gluster/brick
25  gluster_brick_name: gluster
```

This variables file should be pretty self-explanatory; all the ports required for Gluster are opened in the firewall, and the three Gluster-related variables we use in the playbook are defined.

Now that we have everything set up, the folder structure should look like this:

```
gluster/
  playbooks/
    provision.yml
    main.yml
  inventory
  Vagrantfile
```

Change directory into the `gluster` directory, and run `vagrant up`. After a few minutes, provisioning should have completed successfully. To ensure Gluster is working properly, you can run the following two commands, which should give information about Gluster's peer connections and the configured `gluster` volume:

```
$ ansible gluster -i inventory -a "gluster peer status" -s
192.168.29.2 | success | rc=0 >>
Number of Peers: 1

Hostname: 192.168.29.3
Port: 24007
Uuid: 1340bcf1-1ae6-4e55-9716-2642268792a4
State: Peer in Cluster (Connected)

192.168.29.3 | success | rc=0 >>
Number of Peers: 1

Hostname: 192.168.29.2
Port: 24007
Uuid: 63d4a5c8-6b27-4747-8cc1-16af466e4e10
State: Peer in Cluster (Connected)

$ ansible gluster -i inventory -a "gluster volume info" -s
192.168.29.3 | success | rc=0 >>

Volume Name: gluster
Type: Replicate
Volume ID: b75e9e45-d39b-478b-a642-ccd16b7d89d8
Status: Started
Number of Bricks: 1 x 2 = 2
Transport-type: tcp
Bricks:
Brick1: 192.168.29.2:/srv/gluster/brick
Brick2: 192.168.29.3:/srv/gluster/brick

192.168.29.2 | success | rc=0 >>

Volume Name: gluster
Type: Replicate
Volume ID: b75e9e45-d39b-478b-a642-ccd16b7d89d8
Status: Started
Number of Bricks: 1 x 2 = 2
Transport-type: tcp
Bricks:
Brick1: 192.168.29.2:/srv/gluster/brick
Brick2: 192.168.29.3:/srv/gluster/brick
```

You can also do the following to confirm that files are being replicated/distributed correctly:

1. Log into the first server: `vagrant ssh gluster1`
2. Create a file in the mounted gluster volume: `sudo touch /mnt/gluster/test`
3. Log out of the first server: `exit`
4. Log into the second server: `vagrant ssh gluster2`
5. List the contents of the gluster directory: `ls /mnt/gluster`

You should see the `test` file you created in step 2; this means Gluster is working correctly!

Summary

Deploying distributed file systems like Gluster can seem challenging, but Ansible simplifies the process, and more importantly, does so idempotently; each time you run the playbook again, it will ensure everything stays configured as you've set it.

This example Gluster configuration can be found in its entirety on GitHub, in the [Gluster example⁹²](#) in the Ansible Vagrant Examples project.

Mac Provisioning with Ansible and Homebrew

The next example will be specific to the Mac (since that's the author's platform of choice), but the principle behind it applies universally. How many times have you wanted to hit the 'reset' button on your day-to-day workstation or personal computer? How much time do you spend automating configuration and testing of applications and infrastructure at your day job, and how little do you spend automating your *own* local environment?

Over the past few years, as I've gone through four Macs (one personal, three employer-provided), I decided to start fresh on each new Mac (rather than transfer all my cruft from my old Mac to my new Mac through Apple's Migration Assistant). I had a problem, though; I had to spend at least 4-6 hours on each Mac, downloading, installing, and configuring everything. Another problem: since I actively used at least two separate Macs, I had to manually install and configure new software on both Macs whenever I wanted to try a new tool.

To restore order to this madness, I wrapped up all the configuration I could into a set of [dotfiles⁹³](#) and used git to synchronize the dotfiles to all my workstations.

However, even with the assistance of [Homebrew⁹⁴](#), a great package manager for OS X, there was still a lot of manual labor involved in installing and configuring my favorite apps and command line tools.

⁹²<https://github.com/geerlingguy/ansible-vagrant-examples/tree/master/gluster>

⁹³<https://github.com/geerlingguy/dotfiles>

⁹⁴<http://brew.sh/>

Running Ansible playbooks locally

We've seen examples of running playbooks with connection: local earlier, when provisioning virtual machines in the cloud through our local workstation; but you can perform *any* Ansible task using a local connection. This is how we'll configure our local workstation using Ansible.

I usually begin building a playbook with the basic scaffolding in place, and fill in details as I go. You can follow along by creating the playbook `main.yml` with:

```
1  ---
2  - hosts: localhost
3    user: jgeerling
4    connection: local
5
6    vars_files:
7      - vars/main.yml
8
9    roles: []
10
11   tasks: []
```

We'll store any variables we need in the included `vars/main.yml` file. The `user` is set to my local user account, in this case, `jgeerling`, so file permissions are set for my account, and tasks are run under my own account to minimize surprises.



If certain tasks need to be run with sudo privileges, you can add `sudo: yes` to the task, and either run the playbook with `--ask-sudo-pass` (in which case, Ansible will prompt you for your sudo password before running the playbook), or run the playbook normally, and wait for Ansible to prompt you for your sudo password.

Automating Homebrew package and app management

Since I use Homebrew (billed as “the missing package manager for OS X”) for most of my application installation and configuration, I created the role `geerlingguy.homebrew`, which installs homebrew, then installs all the applications and packages I configure in a few simple variables.

The next step, then, is to add the Homebrew role and configure the required variables. Inside `main.yml`, update the `roles` section:

```
9   roles:  
10    - geerlingguy.homebrew
```

Then add the following into `vars/main.yml`:

```
1  ---  
2  homebrew_installed_packages:  
3    - ansible  
4    - sqlite  
5    - mysql  
6    - php56  
7    - python  
8    - ssh-copy-id  
9    - cowsay  
10   - pv  
11   - drush  
12   - wget  
13   - brew-cask  
14  
15  homebrew_taps:  
16    - caskroom/cask  
17    - homebrew/binary  
18    - homebrew/dupes  
19    - homebrew/php  
20    - homebrew/versions  
21  
22  homebrew_cask_appdir: /Applications  
23  homebrew_cask_apps:  
24    - google-chrome  
25    - firefox  
26    - sequel-pro  
27    - sublime-text  
28    - vagrant  
29    - vagrant-manager  
30    - virtualbox
```

Homebrew has a few tricks up its sleeve, like being able to manage general packages like PHP, MySQL, Python, Pipe Viewer, etc. natively (using commands like `brew install [package]` and `brew uninstall package`), and can also install and manage general application installation for many Mac apps, like Chrome, Firefox, VLC, etc. using `brew cask`.

To anyone who's set up a new Mac the old-fashioned way—download 15 .dmg files, mount them, drag the applications to the Applications folder, eject them, delete the .dmg files—Homebrew's simplicity and speed are a godsend. This Ansible playbook has so far automated that process completely,

so you don't even need to run the Homebrew commands manually! The `geerlingguy.homebrew` role uses Ansible's built-in `homebrew` module to manage package installation, and some custom tasks to manage cask applications.

Configuring Mac OS X through dotfiles

Just like there's a `homebrew` role on Galaxy made for configuring and installing packages via Homebrew, there's a `dotfiles` role you can use to download and configure your local dotfiles.



Dotfiles are named as such because they are, simply, files that begin with a `.` placed in your home directory. Many programs and shell environments read local configuration from dotfiles, so dotfiles are a simple, efficient, and easily-synchronized method of customizing your development environment for maximum efficiency.

In this example, we'll use the author's dotfiles, but you can tell the role to use whatever set of dotfiles you want.

Add another role to the roles list:

```
9   roles:
10     - geerlingguy.homebrew
11     - geerlingguy.dotfiles
```

Then, add the following three variables to your `vars/main.yml` file:

```
2 dotfiles_repo: https://github.com/geerlingguy/dotfiles.git
3 dotfiles_repo_local_destination: ~/repositories/dotfiles
4 dotfiles_files:
5   - .bash_profile
6   - .gitignore
7   - .inputrc
8   - .osx
9   - .vimrc
```

The first variable gives the git repository URL for the dotfiles to be cloned. The second gives a local path for the repository to be stored, and the final variable tells the role which dotfiles it should use from the specified repository.

The `dotfiles` role clones the specified dotfiles repository locally, then symlinks every one of the dotfiles specified in `dotfiles_files` into your home folder (removing any existing dotfiles of the same name).

If you want to run the `.osx` dotfile, which adjusts many system and application settings, add in a new task under the `tasks` section in the main playbook:

```
1 tasks:
2   - name: Run .osx dotfiles.
3     shell: ~/osx --no-restart
4     changed_when: false
```

In this case, the `.osx` dotfile allows a `--no-restart` flag to be passed to prevent the script from restarting certain apps and services including Terminal—which is good, since you’d likely be running the playbook from within Terminal.

At this point, you already have the majority of your local environment set up. Copying additional settings and tweaking things further is an exercise in adjusting your dotfiles or including another playbook that copies or links preference files into the right places.

I’m constantly tweaking my own development workstation, and for the most part, all my configuration is wrapped up in my [Mac Development Ansible Playbook](#)⁹⁵, available on GitHub. I’d encourage you to fork that project, as well as my dotfiles, if you’d like to get started automating the build of your own development workstation. Even if you don’t use a Mac, most of the structure is similar; just substitute a different package manager, and start automating everything!

Summary

Ansible is the best way to automate infrastructure provisioning and configuration. Ansible can also be used to configure your own workstation or workstations, saving you time and frustration in doing so yourself. Unfortunately, you can’t yet provision yourself a new top-of-the-line workstation with Ansible!

You can find the full playbook I’m currently using to configure my Macs on GitHub: [Mac Development Ansible Playbook](#)⁹⁶.

Docker-based Infrastructure with Ansible

Docker is a highly optimized platform for building and running containers on local machines and servers in a highly efficient manner. You can think of Docker containers as sort-of lightweight virtual machines. This book won’t go into the details of how Docker and Linux containers work, but will provide an introduction to how Ansible can integrate with Docker to build, manage, and deploy containers.



Prior to running example Docker commands or building and managing containers using Ansible, you’ll need to make sure Docker is installed on either your workstation or a VM or server where you’ll be testing everything. Please see the [installation guide for Docker](#)⁹⁷ for help installing Docker on whatever platform you’re using.

⁹⁵<https://github.com/geerlingguy/mac-dev-playbook>

⁹⁶<https://github.com/geerlingguy/mac-dev-playbook>

⁹⁷<https://docs.docker.com/installation/>

A brief introduction to Docker containers

Starting with an extremely simple example, let's build a docker image from a Dockerfile. In this case, we just want to show how Dockerfiles work, and how we can use Ansible to build the image in the same way you could using the command line with `docker build`.

Let's start with a really simple Dockerfile:

```
1 # Build an example Docker container image.
2 FROM busybox
3 MAINTAINER Jeff Geerling <geerlingguy@mac.com>
4
5 # Run a command when the container starts.
6 CMD ["/bin/true"]
```

This Docker container doesn't do much, but that's okay; we just want to build it and verify that it's present and working—first with Docker, then with Ansible.

Save the above file as `Dockerfile` inside a new directory, and then on the command line, run the following command to build the container:

```
$ docker build -t test .
```

After a few seconds, the docker image should be built, and if you list all local images with `docker image`, you should see your new test image (along with the busybox image, which was used as a base):

```
$ docker images
REPOSITORY TAG IMAGE ID CREATED VIRTUAL SIZE
test      latest 50d6e6479bc7 About a minute ago 2.433 MB
busybox   latest 4986bf8c1536 2 weeks ago    2.433 MB
```

If you want to run the container image you just created, enter the following:

```
$ docker run --name=test test
```

This creates a docker container with the name `test`, and starts the container. Since the only thing our container does is calls `/bin/true`, the container will run the command, then exit. You can see the current status of all your containers (whether or not they're actively running) with the `docker ps -a` command:

```
$ docker ps -a
CONTAINER ID  IMAGE      [...] CREATED      STATUS
bae0972c26d4  test:latest  [...]  3 seconds ago  Exited (0) 2 seconds ago
```

You can control the container using either the container ID (in this case, `bae0972c26d4`) or the name (`test`); start with `docker start [container]`, stop with `docker stop [container]`, delete/remove with `docker rm [container]`.

If you delete the container (`docker rm test`) and delete the image you built (`docker rmi test`), you can experiment with the Dockerfile by changing it and rebuilding the image (with `docker build`), and running the resulting image (with `docker run`). As an example, if you change the command from `/bin/true` to `/bin/false`, then run build and run the container, `docker ps -a` will show that the container exited with the status code `1` instead of `0`.

For our purposes, this is a simple enough introduction to how Docker works. To summarize:

- Dockerfiles contain the instructions Docker uses to build containers.
- `docker build` builds Dockerfiles and generates container images.
- `docker images` lists all images present on the system.
- `docker run` runs created images.
- `docker ps -a` lists all containers, both running and stopped.

When developing Dockerfiles to containerize your own applications, you will likely want to get familiar with the Docker CLI and how the process works from a manual perspective. But when building the final images and running them on your servers, Ansible can help ease the process.

Using Ansible to build and manage containers

Ansible has a built-in [Docker module⁹⁸](#) that integrates nicely with Docker for container management. We're going to use it to automate the building and running of the container managed by the Dockerfile we just created.

Move the Dockerfile you had into a subdirectory, and create a new Ansible playbook (call it `main.yml`) in the project root directory. The directory layout should look like:

```
docker/
  main.yml
  test/
    Dockerfile
```

Inside the new playbook, add the following:

⁹⁸http://docs.ansible.com/docker_module.html

```
1  ---
2  - hosts: localhost
3    connection: local
4
5  tasks:
6    - name: Build Docker image from Dockerfiles.
7      docker_image:
8        name: test
9        path: test
10       state: build
```

The playbook uses the `docker_image` module to build an image. Provide a name for the image, the path to the Dockerfile (in this case, inside the `test` directory), and tell Ansible via the `state` parameter whether the image should be present, absent, or built (via `build`).



Ansible's Docker integration may require you to install an extra Docker python library on the system running the Ansible playbook. For example, on ArchLinux, if you get the error "failed to import Python module", you will need to install the `python2-docker-py` package.



The `docker_image` module is listed as being deprecated as of early 2015. The module's functionality will soon be moved into the main `docker` module, but until that time, this playbook should work as-is.

Run the playbook (`$ ansible-playbook main.yml`), and then list all the Docker images (`$ docker images`). If all was successful, you should see a fresh `test` image in the list.

Run `docker ps -a` again, though, and you'll see that the new `test` image was never run and is absent from the output. Let's remedy that by adding another task to our Ansible playbook:

```
12 - name: Run the test container.
13   docker:
14     image: test:latest
15     name: test
16     state: running
```

If you run the playbook again, Ansible will run the docker container. Check the list of containers with `docker ps -a`, and you'll note that the `test` container is again present.

You can remove the container and the image via ansible by changing the `state` parameter to `absent` for both tasks.



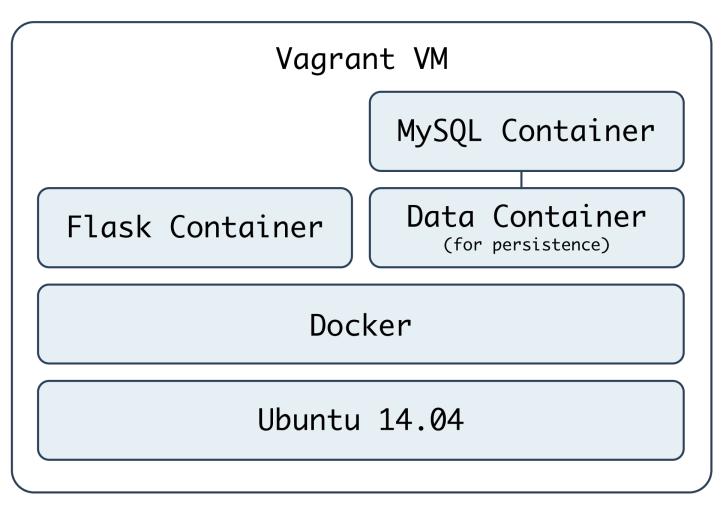
This playbook assumes you have both Docker and Ansible installed on whatever host you're using to test Docker containers. If this is not the case, you may need to modify the example so the Ansible playbook is targeting the correct hosts and using the right connection settings. Additionally, if the user account under which you run the playbook can't run docker commands, you may need to use sudo with this playbook.



The code example above can be found in the [Ansible for DevOps GitHub repository](#)⁹⁹.

Building a Flask app with Ansible and Docker

Let's build a more useful Docker-powered environment, with a container that runs our application (built with Flask, a lightweight Python web framework), and a container that runs a database (MySQL), along with a data container. We need a separate data container to persist the MySQL database, because data changed inside the MySQL container is lost every time the container stops.



Docker stack for Flask App

We'll create a VM using Vagrant to run our Docker containers so the same Docker configuration can be tested on any machine capable of running Ansible and Vagrant. Create a `docker` folder, and inside it, the following `Vagrantfile`:

⁹⁹<https://github.com/geerlingguy/ansible-for-devops/tree/master/docker>

```

1 # -*- mode: ruby -*-
2 # vi: set ft=ruby :
3
4 VAGRANTFILE_API_VERSION = "2"
5
6 Vagrant.configure(VAGRANTFILE_API_VERSION) do |config|
7   config.vm.box = "geerlingguy/ubuntu1404"
8   config.vm.network :private_network, ip: "192.168.33.39"
9   config.ssh.insert_key = false
10
11  config.vm.provider :virtualbox do |v|
12    v.customize ["modifyvm", :id, "--name", "docker.dev"]
13    v.customize ["modifyvm", :id, "--natdnshostresolver1", "on"]
14    v.customize ["modifyvm", :id, "--memory", 1024]
15    v.customize ["modifyvm", :id, "--cpus", 2]
16    v.customize ["modifyvm", :id, "--ioapic", "on"]
17  end
18
19  # Enable provisioning with Ansible.
20  config.vm.provision "ansible" do |ansible|
21    ansible.playbook = "provisioning/main.yml"
22  end
23
24 end

```

We'll use Ubuntu 14.04 for this example, and we've specified an Ansible playbook (`provisioning/main.yml`) to set everything up. Inside `provisioning/main.yml`, we need to first install and configure Docker (which we'll do using the Ansible Galaxy role `angstwad.docker_ubuntu`), then run some additional setup tasks, and finally build and start the required Docker containers:

```

1 ---
2 - hosts: all
3   sudo: yes
4
5   roles:
6     - role: angstwad.docker_ubuntu
7
8   tasks:
9     - include: setup.yml
10    - include: docker.yml

```

We're using `sudo` for everything because Docker either requires root privileges, or requires the

current user account to be in the docker group. It's simplest for our purposes to set everything up with sudo.

Angstwad's docker_ubuntu role requires no additional settings or configuration, so we can move on to setup.yml (in the same provisioning directory alongside main.yml):

```
1 ---
2   - name: Install Pip.
3     apt: name=python-pip state=installed
4     sudo: yes
5
6   - name: Install Docker Python library.
7     pip: name=docker-py state=present
8     sudo: yes
```

Ansible needs the docker-py library in order to control Docker via Python, so we install pip, then use it to install docker-py.

Next is the meat of the playbook, docker.yml (also in the provisioning directory). The first task is building docker images for our data, application, and database containers:

```
1 ---
2   - name: Build Docker images from Dockerfiles.
3     docker_image:
4       name: "{{ item.name }}"
5       tag: "{{ item.tag }}"
6       path: "/vagrant/provisioning/{{ item.directory }}"
7       state: build
8     with_items:
9       - { name: data, tag: "data", directory: data }
10      - { name: www, tag: "flask", directory: www }
11      - { name: db, tag: mysql, directory: db }
```

Don't worry that we haven't created the actual Dockerfiles required to create the Docker images yet; we'll do that after we finish structuring everything with Ansible.

Like our earlier usage of docker_image, we supply a name, path, and state for each image. In this example, we're also adding a tag, which behaves like a git tag, allowing future Docker commands to use the images we created at a specific version. We'll be building three containers, data, www, and db, and we're pointing docker to the path /vagrant/provisioning/[directory], where [directory] contains the Dockerfile and any other helpful files to be used to build the Docker image.

After building the images, we will need to start each of them (or at least make sure a container is **present**, in the case of the data container—since you can use data volumes from non-running containers). We'll do that in three separate docker tasks:

```
13 # Data containers don't need to be running to be utilized.
14 - name: Run a Data container.
15   docker:
16     image: data:data
17     name: data
18     state: present
19
20 - name: Run a Flask container.
21   docker:
22     image: www:flask
23     name: www
24     state: running
25     command: python /opt/www/index.py
26     ports: "80:80"
27
28 - name: Run a MySQL container.
29   docker:
30     image: db:mysql
31     name: db
32     state: running
33     volumes_from: data
34     command: /opt/start-mysql.sh
35     ports: "3306:3306"
```

Each of these containers' configuration is a little more involved than the previous. In the case of the first container, it's just present; Ansible will ensure a data container is present.

For the Flask container, we need to make sure our app is running, and *continues* running, so in this case (unlike our earlier usage of `/bin/true` to run a container briefly and exit), we are providing an explicit command to run:

```
26     command: python /opt/www/index.py
```

Calling the script directly will launch the app in the foreground and log everything to stdout, making it easy to inspect what's going on with `docker logs [container]` if needed.

Additionally, we want to map the container's port 80 to the host's port 80, so external users can load pages over HTTP. This is done using the `ports` option, passing data just as you would using Docker's `--publish` syntax.

The Flask container will have a static web application running on it, and has no need for extra non-transient file storage, but the MySQL container will mount a data volume from the data container so it has a place to store data that won't vanish when the container dies and is restarted.

Thus, for the db container, we have two special options; the `volumes_from` option, which mounts volumes from the specified container (in this case, the data container), and the `command`, which calls a shell script to start MySQL. We'll get to why we're running a shell script and not launching a MySQL daemon directly in a bit.

Now that we have the playbook structured to build our simple Docker-based infrastructure, we'll build out each of the three Dockerfiles and related configuration to support the data, www, and db containers.

At this point, we should have a directory structure like:

```
docker/
  provisioning/
    data/
    db/
    www/
  docker.yml
  main.yml
  setup.yml
Vagrantfile
```



It's best practice to use lightweight base images without any extra frills instead of heavyweight 'VM-like' images. Additionally, lightweight server environments where containers are built and run, like CoreOS, don't need the baggage of a standard Linux distribution. If you need Ansible available for configuration and container management in such an environment, you also need to have Python and other dependencies installed. Check out these two resources in particular for tips and tricks with managing and configuring containers with Ansible on CoreOS servers: [Managing CoreOS with Ansible¹⁰⁰](#) and [Provisioning CoreOS with Ansible¹⁰¹](#).

Data storage container

For the data storage container, we don't need much; we just need to create a directory and set it as an exposed mount point using `VOLUME`:

¹⁰⁰<https://coreos.com/blog/managing-coreos-with-ansible/>

¹⁰¹<http://www.tazj.in/en/1410951452>

```
1 # Build a simple MySQL data volume Docker container.
2 FROM busybox
3 MAINTAINER Jeff Geerling <geerlingguy@mac.com>
4
5 # Create data volume for MySQL.
6 RUN mkdir /var/lib/mysql
7 VOLUME /var/lib/mysql
```

We create a directory (line 6) and expose the directory as a volume (line 7) which can be mounted by the host or other containers. Save the above into a new file, `docker/provisioning/data/Dockerfile`.



This container builds on top of the official `busybox` base image. Busybox is an extremely simple distribution that's linux-like, but doesn't contain every option or application generally found in popular distributions like Debian, Ubuntu, or RedHat. Since we only need to create and share a directory, we don't need any additional 'baggage' inside the container. In the Docker world, it's best to use the most minimal base images possible, and only install and run the bare necessities inside each container to support the container's app.

Flask container

[Flask](#)¹⁰² is a lightweight Python web framework “based on Werkzeug, Jinja 2 and good intentions”. It’s a great web framework for small, fast, and robust websites and apps, or even a simple API. For our purposes, we need to build a Flask app that connects to a MySQL database and displays the status of the connection on a simple web page (very much like our PHP example, in the earlier Highly-Available Infrastructure example).

Here’s the code for the Flask app (save it as `docker/provisioning/www/index.py.j2`):

```
1 # Infrastructure test page.
2 from flask import Flask
3 from flask import Markup
4 from flask import render_template
5 from flask.ext.sqlalchemy import SQLAlchemy
6
7 app = Flask(__name__)
8
9 # Configure MySQL connection.
10 db = SQLAlchemy()
```

¹⁰²<http://flask.pocoo.org/>

```
11 db_uri = 'mysql://admin:admin@{{ host_ip_address }}/information_schema'
12 app.config['SQLALCHEMY_DATABASE_URI'] = db_uri
13 db.init_app(app)
14
15 @app.route("/")
16 def test():
17     mysql_result = False
18     try:
19         if db.session.query("1").from_statement("SELECT 1").all():
20             mysql_result = True
21     except:
22         pass
23
24     if mysql_result:
25         result = Markup('<span style="color: green;">PASS</span>')
26     else:
27         result = Markup('<span style="color: red;">FAIL</span>')
28
29     # Return the page with the result.
30     return render_template('index.html', result=result)
31
32 if __name__ == "__main__":
33     app.run(host="0.0.0.0", port=80)
```

This simple app defines one route (/), listens on every interface on port 80, and shows a MySQL connection status page rendered by the template index.html. There's nothing particularly complicated in this application, but there is one Jinja2 variable ({{ host_ip_address }}) which an Ansible playbook will replace during deployment), and the app has a few dependencies (like flask-sqlalchemy) which will need to be installed via the Dockerfile.

Since we are using a Jinja2 template to render the page, let's create that template in docker/provisioning/www/templates/index.html (Flask automatically picks up any templates inside a templates directory):

```
1 <!DOCTYPE html>
2 <html>
3 <head>
4     <title>Flask + MySQL Docker Example</title>
5     <style>* { font-family: Helvetica, Arial, sans-serif }</style>
6 </head>
7 <body>
8     <h1>Flask + MySQL Docker Example</h1>
9     <p>MySQL Connection: {{ result }}</p>
```

```
10 </body>
11 </html>
```

In this case, the `.html` template contains a Jinja2 variable (`{{ result }}`), and Flask will fill in that variable with the status of the MySQL connection.

Now that we have the app defined, we need to build the container to run the app. Here's a Dockerfile that will install all the required dependencies, then copy a simple Ansible playbook and the app itself into place, so we can do the more complicated configuration (like copying a template with variable replacement) through Ansible:

```
1 # A simple Flask app container.
2 FROM ansible/ubuntu14.04-ansible
3 MAINTAINER Jeff Geerling <geerlingguy@mac.com>
4
5 # Install Flask app dependencies.
6 RUN apt-get install -y libmysqlclient-dev python-dev
7 RUN pip install flask flask-sqlalchemy mysql-python
8
9 # Install playbook and run it.
10 COPY playbook.yml /etc/ansible/playbook.yml
11 COPY index.py.j2 /etc/ansible/index.py.j2
12 COPY templates /etc/ansible/templates
13 RUN mkdir -m 755 /opt/www
14 RUN ansible-playbook /etc/ansible/playbook.yml --connection=local
15
16 EXPOSE 80
```

Instead of installing apt and pip packages using Ansible, we'll install them using `RUN` commands in the Dockerfile. This allows those commands to be cached by Docker. Generally, more complicated package installation and configuration is easier and more maintainable inside Ansible, but in the case of simple package installation, having Docker cache the steps so future `docker build` commands take seconds instead of minutes is worth the verbosity of the Dockerfile.

At the end of the Dockerfile, we run a playbook (which should be located in the same directory as the Dockerfile), and expose port 80 so the app can be accessed via HTTP by the outside world. We'll create the app deployment playbook next.



Purists might cringe at the sight of an Ansible playbook inside a Dockerfile, and for good reason! Commands like the `ansible-playbook` command cover up configuration that might normally be done (and cached) within Docker. Additionally, using the `ansible/ubuntu14.04-ansible` base image (which includes Ansible) requires an initial download that's 50+ MB larger than a comparable `debian` or `ubuntu` image without Ansible. However, for brevity and ease of maintenance, we're using Ansible to manage all the app configuration inside the container (otherwise we'd need to run a bunch of verbose and incomprehensible shell commands to replace Ansible's `template` functionality).

For the Flask app to function properly, we'll need to get the `host_ip_address`, then replace the variable in the `index.py.j2` template. Create the Flask deployment playbook at `docker/provisioning/www/playbook.yml`:

```
1  ---
2  - hosts: localhost
3    sudo: yes
4
5  tasks:
6    - name: Get host IP address.
7      shell: "/sbin/ip route|awk '/default/ { print $3 }'"
8      register: host_ip
9      changed_when: false
10
11   - name: Set host_ip_address variable.
12     set_fact:
13       host_ip_address: "{{ host_ip.stdout }}"
14
15   - name: Copy Flask app into place.
16     template:
17       src: /etc/ansible/index.py.j2
18       dest: /opt/www/index.py
19       mode: 0755
20
21   - name: Copy Flask templates into place.
22     copy:
23       src: /etc/ansible/templates
24       dest: /opt/www
25       mode: 0755
```

The shell command that registers the `host_ip` (which is used in the next task to generate the `host_ip_address` variable) is a simple way to retrieve the IP while still letting Docker do its own virtual network management.

The last two tasks copy the flask app and templates directory into place.

The docker/provisioning/www directory should now contain the following:

```
www/
  templates/
    index.html
  Dockerfile
  index.py.j2
  playbook.yml
```

MySQL container

We've configured MySQL a few times throughout this book, so little time will be spent discussing how MySQL is set up. We'll instead dive into how MySQL is configured to work inside a docker container, with a persistent data volume from the previously-configured data container.

First, we'll create a really simple Ansible playbook to install and configure MySQL using the `geerlingguy.mysql` role:

```
1  ---
2  - hosts: localhost
3    sudo: yes
4
5  vars:
6    mysql_users:
7      - name: admin
8        host: "%"
9        password: admin
10       priv: "*.*:ALL"
11
12 roles:
13   - geerlingguy.mysql
```

This playbook is quite simple; it just sets up one MySQL user using the `mysql_users` variable, and then runs `geerlingguy.mysql`. Save it as `docker/provisioning/db/playbook.yml`.

Next, we need to account for the fact that there are two conditions under which MySQL will be started:

1. When Docker builds the container initially (using `docker build` through Ansible's `docker-image` module).
2. When we launch the container and pass in the data volume (using `docker run` through Ansible's `docker` module).

In the latter case, the data volume's `/var/lib/mysql` directory will supplant the container's own directory, but it will be empty! Therefore, instead of just launching the MySQL daemon as we launched the Flask app in the `www` container, we need to build a small shell script to run on container start to detect if MySQL has already been setup inside `/var/lib/mysql`, and if not, reconfigure MySQL so the data is there.

Here's a simple script to do just that—using the playbook we just created to do most of the heavy lifting. Save this as `docker/provisioning/db/start-mysql.sh`:

```
1 #!/bin/bash
2
3 # If connecting to a new data volume, we need to reconfigure MySQL.
4 if [[ ! -d /var/lib/mysql/mysql ]]; then
5     rm -f ~/.my.cnf
6     mysql_install_db
7     ansible-playbook /etc/ansible/playbook.yml --connection=local
8     mysqladmin shutdown
9 fi
10
11 exec /usr/bin/mysqld_safe
```

This bash script checks if there's already a `mysql` directory inside MySQL's default data directory, and if not (as is the case when we run the container with the data volume), it will remove any existing `.my.cnf` connection file, run `mysql_install_db` to initialize MySQL, then run the playbook, and shut down MySQL.

Once that's all done (or if the persistent data volume has already been set up previously), MySQL is started with the `mysqld_safe` startup script which, according to the MySQL documentation¹⁰³, is “the recommended way to start a mysqld server on Unix”.

Next comes the Dockerfile, where we'll make sure the `playbook.yml` playbook and `start-mysql.sh` script are put in the right places, and expose the MySQL port so other containers can connect to MySQL.

¹⁰³<http://dev.mysql.com/doc/refman/5.6/en/mysqld-safe.html>

```
1 # A simple MySQL container.
2 FROM ansible/ubuntu14.04-ansible
3 MAINTAINER Jeff Geerling <geerlingguy@mac.com>
4
5 # Install required Ansible roles.
6 RUN ansible-galaxy install geerlingguy.mysql
7
8 # Copy startup script.
9 COPY start-mysql.sh /opt/start-mysql.sh
10 RUN chmod +x /opt/start-mysql.sh
11
12 # Install playbook and run it.
13 COPY playbook.yml /etc/ansible/playbook.yml
14 RUN ansible-playbook /etc/ansible/playbook.yml --connection=local
15
16 EXPOSE 3306
```

Just as with the Flask app container, we're using a base image with Ubuntu 14.04 and Ansible. This time, since we're doing a bit more configuration via the playbook, we also need to install the `geerlingguy.mysql` role via Ansible Galaxy.

The `start-mysql.sh` script needs to be in the location where we're calling it with command: `/opt/start-mysql.sh` in the `docker.yml` file we set up much earlier, so we copy it in place, then give `+x` permissions so Docker can execute the file.

Finally, the Ansible playbook that configures MySQL is copied into place, then run, and port 3306 is exposed.

The `docker/provisioning/db` directory should now contain the following:

```
db/
  Dockerfile
  playbook.yml
  start-mysql.sh
```

Ship it!

Now that everything's in place, you should be able to cd into the main `docker` directory, and run `vagrant up`. After 10 minutes or so, Vagrant should show that Ansible provisioning was successful, and if you visit `http://192.168.33.39/` in your browser, you should see something like the following:



If you see “MySQL Connection: PASS”, congratulations, everything worked! If it shows ‘FAIL’, you might need to give the MySQL a little extra time to finish its reconfiguration, since it has to rebuild the database on first launch. If the page doesn’t show up at all, you might want to compare your code with the [Docker LAMP example¹⁰⁴](#) on GitHub.

Summary

The entire [Docker LAMP example¹⁰⁵](#) is available on GitHub, if you want to clone it and try it locally.

The Docker examples in this book barely scratch the surface of what makes Docker a fascinating and useful application deployment tool. As of the writing of this book, Docker is still in its infancy, so there are dozens of ways to manage the building of Dockerfiles, the deployment of images, and the running and linking of containers. Ansible is a solid contender in this space, and can even be used within a Dockerfile to simplify complex container configurations.

```
/ Any sufficiently advanced technology is \
| indistinguishable from magic.           |
\ (Arthur C. Clarke)                   /
```

```
\   ^__^
 \  (oo)\_____
  (__)\       )\/\
    ||----w |
    ||     ||
```

¹⁰⁴<https://github.com/geerlingguy/ansible-vagrant-examples/tree/master/docker>

¹⁰⁵<https://github.com/geerlingguy/ansible-vagrant-examples/tree/master/docker>

Chapter 9 - Deployments with Ansible

Deploying application code to servers is one of the hardest, but most rewarding, tasks of any development team. Most shops using traditional deployment techniques (manual steps, shell scripts, and prayers) dread deployments, especially for complex, monolithic apps.

Deployments are less daunting when you adopt modern deployment processes and use the right amount of automation. In the best case, deployments become so boring and routine they barely register as a blip on your team's radar.

Consider Etsy, a company whose engineers are deploying code to production [up to 40 times per day¹⁰⁶](#), with no manual intervention from the operations team. The operations team is free to work on more creative endeavors, and the developers see their code go live in near-real-time!

Etsy's production deployment schedule is enabled by a strong DevOps-oriented culture (with robust code repository management, continuous integration, well-tested code, feature flags, etc.). While it may not be immediately possible to start deploying *your* application to production 20 times a day, you can move a long way towards effortless deployments by automating deployments with Ansible.

Deployment strategies

There are dozens of ways to deploy code to servers. For the simplest of applications, all that's involved might be switching to a new tag in a code repository on the server and restarting a service.

For more complex applications, you might do a full Blue-Green deployment, where you build an entire new infrastructure alongside your current production infrastructure, run tests on the new infrastructure, then automatically cut over to the new instances. This may be overkill for many applications (especially if <100% uptime is acceptable), but it is becoming more and more common—and Ansible can automate the entire process.

In this chapter, we will be covering the following deployment strategies:

1. Single-server deployments.
2. Zero-downtime multi-server deployments.
3. Capistrano-style and blue-green deployments.

These are three of the most common deployment techniques, and they cover many common use cases. There are other ways you can strengthen your deployment processes, often involving application-level and organizational change, but those deployment aspects are out of the scope of this book.

¹⁰⁶<http://www.slideshare.net/mikebrittain/principles-and-practices-in-continuous-deployment-at-etsy>

Simple single-server deployments

The vast majority of small applications and websites are easily run on a single virtual machine or dedicated server. Using Ansible to provision and manage the configuration on the server is a no-brainer. Even though you only have to manage **one** server, it's better to encapsulate all the setup so you don't end up with a **snowflake server**.

In this instance, we are managing a very simple Ruby on Rails site that allows users to perform CRUD operations on articles (very simple database records with a title and body).

The code repository for this app is located on GitHub at <https://github.com/geerlingguy/demo-rails-app>.

To make testing simple, we'll begin by creating a new Vagrant VM using the following Vagrantfile:

```
1 # -*- mode: ruby -*-
2 # vi: set ft=ruby :
3
4 Vagrant.configure(2) do |config|
5   config.vm.box = "geerlingguy/ubuntu1404"
6
7   config.vm.provider "virtualbox" do |v|
8     v.name = "rails-demo"
9     v.memory = 1024
10    v.cpus = 2
11  end
12
13  config.vm.hostname = "rails-demo"
14  config.vm.network :private_network, ip: "192.168.33.7"
15
16  config.vm.provision "ansible" do |ansible|
17    ansible.playbook = "playbooks/main.yml"
18    ansible.sudo = true
19  end
20
21 end
```

In this case, we have a very simple VM that will be accessible at the IP address 192.168.33.7, and when provisioned, it will run the Ansible playbook defined in playbooks/main.yml.

Provisioning a simple Ruby on Rails server

To prepare for our application deployment, we need to do the following:

1. Install git (our application is version controlled in a git repository).
2. Install Node.js (asset compilation requires it's Javascript runtime).
3. Install Ruby (our application requires version 2.2.0 or later).
4. Install Passenger with Nginx (we need a fast web server to run our rails application).
5. Install any other dependencies, and prepare the server for deployment.

To that end, let's create a new playbook just for the provisioning tasks (we'll worry about deployment later), in a new file, `playbooks/provision.yml`:

```
1  ---
2  - hosts: all
3    sudo: yes
4
5    vars_files:
6      - vars.yml
7
8    roles:
9      - gearlingguy.git
10     - gearlingguy.nodejs
11     - gearlingguy.ruby
12     - gearlingguy.passenger
13
14   tasks:
15     - name: Install app dependencies.
16       apt: "name={{ item }} state=present"
17       with_items:
18         - libsqlite3-dev
19         - libreadline-dev
20
21     - name: Ensure app directory exists and is writeable.
22       file:
23         path: "{{ app_directory }}"
24         state: directory
25         owner: "{{ app_user }}"
26         group: "{{ app_user }}"
27         mode: 0755
```

This is a fairly simple playbook. We'll need to define a few variables to make sure the `gearlingguy.ruby` role installs the correct version of Ruby (at least 2.2.0), and the `gearlingguy.passenger` role is configured to serve our app correctly.

There are also a few other variables we will need, like `app_directory` and `app_user`, so let's create the variables file now, at `playbooks/vars.yml`:

```
1 # Variables for our app.
2 app_directory: /opt/demo-rails-app
3 app_user: www-data
4
5 # Variables for Passenger and Nginx.
6 passenger_server_name: 0.0.0.0
7 passenger_app_root: /opt/demo-rails-app/public
8 passenger_app_env: production
9 passenger_ruby: /usr/local/bin/ruby
10
11 # Variables for Ruby installation.
12 ruby_install_from_source: true
13 ruby_download_url: http://cache.ruby-lang.org/pub/ruby/2.2/ruby-2.2.0.tar.gz
14 ruby_version: 2.2.0
```

The passenger variables tell Passenger to run a server available on every network interface, and to launch our app (which will be located in `/opt/demo-rails-app/public`) with production settings (the app's environment), using the `ruby` binary we have installed in `/usr/local/bin/ruby`.

The Ruby variables tell the `ruby` role to install Ruby 2.2.0 from source, since the packages available through Ubuntu's standard apt repositories only contain older versions.

The playbook specified in our Vagrantfile, `playbooks/main.yml`, doesn't yet exist. Let's create that playbook and include the above `provision.yml` playbook so our server will be provisioned successfully. We'll separate out the deployment steps into another playbook and include that separately. Inside `playbooks/main.yml`:

```
1 ---
2 - include: provision.yml
```

Deploying a Rails app to the server

All the dependencies for our app's deployment were configured in `provision.yml`, so we're ready to build a playbook to perform all the deployment tasks.

Add a line to the `main.yml` file to include a new `deploy.yml` playbook:

```
1 ---
2 - include: provision.yml
3 - include: deploy.yml
```

Now we're ready to create a the `deploy.yml` playbook, which will do the following:

1. Use git to check out the latest production release of the Rails app.
2. Copy over a `secrets.yml` template that holds some secure app data required for running the app.
3. Make sure all the gems required for the app are installed (via Bundler).
4. Create the database (if it doesn't already exist).
5. Run `rake` tasks to make sure the database schema is up-to-date and all assets (like JS and CSS) are compiled.
6. Make sure the app files' ownership is set correctly so Passenger and Nginx can serve them without error.
7. If any changes or updates were made, restart Passenger and Nginx.

Most of these tasks will use Ansible's modules, but for a few, we'll just wrap the normal deployment-related commands in `shell` since there aren't pre-existing modules to take care of them for us:

```
1  ---
2  - hosts: all
3    sudo: yes
4
5  vars_files:
6    - vars.yml
7
8  roles:
9    - geerlingguy.passenger
10
11 tasks:
12   - name: Ensure demo application is at correct release.
13     git:
14       repo: https://github.com/geerlingguy/demo-rails-app.git
15       version: "{{ app_version }}"
16       dest: "{{ app_directory }}"
17       accept_hostkey: true
18       register: app_updated
19       notify: restart nginx
20
21   - name: Ensure secrets file is present.
22     template:
23       src: templates/secrets.yml.j2
24       dest: "{{ app_directory }}/config/secrets.yml"
25       owner: "{{ app_user }}"
26       group: "{{ app_user }}"
27       mode: 0664
28     notify: restart nginx
```

```

29
30     - name: Install required dependencies with bundler.
31         shell: "bundle install --path vendor/bundle chdir={{ app_directory }}"
32         when: app_updated.changed == true
33         notify: restart nginx
34
35     - name: Check if database exists.
36         stat: "path={{ app_directory }}/db/{{ app_environment.RAILS_ENV }}.sqlite3"
37         register: app_db_exists
38
39     - name: Create database.
40         shell: "bundle exec rake db:create chdir={{ app_directory }}"
41         when: app_db_exists.stat.exists == false
42         notify: restart nginx
43
44     - name: Perform deployment-related rake tasks.
45         shell: "{{ item }}" chdir={{ app_directory }}
46         with_items:
47             - bundle exec rake db:migrate
48             - bundle exec rake assets:precompile
49         environment: app_environment
50         when: app_updated.changed == true
51         notify: restart nginx
52
53     - name: Ensure demo application has correct user for files.
54         file:
55             path: "{{ app_directory }}"
56             state: directory
57             owner: "{{ app_user }}"
58             group: "{{ app_user }}"
59             recurse: yes
60         notify: restart nginx

```

The first thing you'll notice (besides the fact that we've included the `vars.yml` file again, since we need those variables in this playbook as well) is that we've added the `geerlingguy.passenger` role in this playbook. Since we'll be using one of the handlers defined in that playbook (`restart nginx`), we need to include the role explicitly. We could've added a separate handler specific to this playbook, but it's more maintainable to reuse handlers from roles if necessary.

Let's walk through the tasks, one-by-one:

1. (Lines 12-19) We put all the application files in place by checking out the git repository at the version `app_version` into the directory `app_directory`. We set `accept_hostkey` to true so

that, the first time we deploy the app, this task doesn't hang since we haven't yet accepted the Git server's hostkey.

2. (Lines 21-28) We copy a `secrets.yml` file to the application's configuration directory. There are different ways to deploy app secrets, but this is the simplest and easiest, and allows us to store the app secrets in an Ansible Vault-protected vars file if we so desire.
3. (Lines 30-33) If the `app_updated` variable shows that a change occurred as part of the first `git` task, we'll run a `bundler` command to ensure all the latest bundled dependencies are installed in the `vendor/bundle` directory.
4. (Lines 35-42) Create the application database with `rake db:create` if it doesn't already exist. Since this application uses a simple SQLite database, it's a matter of checking if the `.sqlite3` file exists, and if not, running the `db:create` task.
5. (Lines 44-51) If the `app_updated` variable shows that a change occurred as part of the first `git` task, we'll also run a couple `rake` tasks to make sure the database schema is up to date, and all assets (like scripts and stylesheets) are compiled.
6. (Lines 53-60) Make sure all app files have the correct permissions for Passenger/Nginx to serve them correctly.

Because many of the tasks result in filesystem changes that could change the behavior of the application, they all notify the `restart nginx` handler provided by the `geerlingguy.passenger` role, so Passenger reloads the configuration and restarts the app.

There are a few new variables we need to add to `vars.yml`, and we also need to add the `secrets.yml.j2` template mentioned in the task that copies it into place.

First, we'll create the secrets file, inside `playbooks/templates/secrets.yml.j2`:

```
1 development:  
2     secret_key_base: {{ app_secrets.dev }}  
3  
4 test:  
5     secret_key_base: {{ app_secrets.test }}  
6  
7 production:  
8     secret_key_base: {{ app_secrets.prod }}
```

We'll be using a dictionary variable for `app_secrets`, so let's add that and all the other new variables to `playbooks/vars.yml`:

```
1  ---
2  # Variables for our app.
3  app_version: 1.2.2
4  app_directory: /opt/demo-rails-app
5  app_user: www-data
6  app_secrets:
7      dev: fe562ec1e21eecc5af4d83f6a157a7
8      test: 4408f36dd290766d2f368fdfcedf4d
9      prod: 9bf801da1a24c9a103ea86a1438caa
10 app_environment:
11     RAILS_ENV: production
12
13 # Variables for Passenger and Nginx.
14 passenger_server_name: 0.0.0.0
15 passenger_app_root: /opt/demo-rails-app/public
16 passenger_app_env: production
17 passenger_ruby: /usr/local/bin/ruby
18
19 # Variables for Ruby installation.
20 ruby_install_from_source: true
21 ruby_download_url: http://cache.ruby-lang.org/pub/ruby/2.2/ruby-2.2.0.tar.gz
22 ruby_version: 2.2.0
```

Note the addition of the following variables to support our `deploy.yml` playbook:

- `app_version`: This is the git tag or branch tip to be deployed to the server.
- `app_secrets`: A dictionary of Rails app secrets, which are used to verify the integrity of signed app cookies. You can generate new, unique strings for these variables using `rake secret`.
- `app_environment`: Environment settings required for certain commands (like `bundle exec` and `rake`) to run with the correct Rails application environment.

Provisioning and Deploying the Rails App

Since we now have our `provision.yml` and `deploy.yml` playbooks completed, and both are included in the `main.yml` playbook Vagrant will run, we can finally bring up the new VM using Vagrant, and see if our application works!

The structure of your project folder should look like this:

```
deployments/
playbooks/
templates/
    secrets.yml.j2
deploy.yml
main.yml
provision.yml
vars.yml
Vagrantfile
```

Before we can run the playbook, we need to make sure all the role dependencies are present. If you were building everything from scratch, you might have a `roles` directory with all the roles inside, but in this case, since we're using roles from Ansible Galaxy, it's best to not include the role files directly with our playbook, but instead, add a `requirements.txt` file to the project and install the roles automatically with Galaxy.

Inside `requirements.txt`:

```
1 geerlingguy.git
2 geerlingguy.ruby
3 geerlingguy.nodejs
4 geerlingguy.passenger
```

Now, in the same directory as that file, run the command `$ ansible-galaxy install -r requirements.txt`, and after a minute, all the required roles will be downloaded to your default Ansible roles directory, if they're not already present.

Change directory back to the main directory containing the `Vagrantfile`, and run `vagrant up`. Assuming everything runs correctly, you should see the playbook complete successfully after a few minutes:

```
TASK: [Ensure demo application has correct user for files.] ****
changed: [default]
```

```
NOTIFIED: [geerlingguy.passenger | restart nginx] ****
changed: [default]
```

```
PLAY RECAP ****
default : ok=46    changed=28    unreachable=0    failed=0
```

Now, jump over to a web browser and load `http://192.168.33.7/`. You should see something like the following:



Demonstration Ruby on Rails Application

[Add article](#)

Title	Text	Operations
<i>There are currently no articles.</i>		

This demonstration is modeled after the official [Getting Started](#) Rails Guide.

Demonstration Rails app running successfully.

Try creating, updating, and deleting a few articles to make sure the database and all app functionality is working correctly:



Demonstration Ruby on Rails Application

[Add article](#)

Title	Text	Operations
Morbi mattis ullamcorper velit	Fusce risus nisl, viverra et, tempor et, pretium in, sapien. Proin sapien ipsum, porta a, auctor quis, euismod ut, mi. Praesent adipiscing. Maecenas egestas arcu quis ligula mattis placerat. Aenean posuere, tortor sed cursus feugiat, nunc augue blandit nunc, eu sollicitudin urna dolor sagittis lacus. Vivamus consectetuer hendrerit lacus. Ut a nisl in ante tempus hendrerit. Nunc sed turpis. Nullam accumsan lorem in dui. Nulla sit amet est. Nam adipiscing. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Fusce id purus. Ut varius tincidunt libero. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Donec vitae orci sed dolor rutrum auctor.	View Edit Delete
Praesent vestibulum dapibus nibh	Duis vel nibh at velit scelerisque suscipit. Etiam ut purus mattis mauris sodales aliquam. Suspendisse feugiat. Curabitur blandit mollis lacus. Proin magna. Fusce risus nisl, viverra et, tempor et, pretium in, sapien. Cras id dui. Nulla facilisi. Curabitur nisi. Mauris turpis nunc, blandit et, volutpat molestie, porta ut, ligula. Praesent nec nisl a purus blandit viverra. Etiam ultricies nisi vel augue.	View Edit Delete
Curabitur at lacus ac velit	Praesent porttitor, nulla vitae posuere iaculis, arcu nisl dignissim dolor, a pretium mi sem ut ipsum. Donec interdum, metus et hendrerit aliquet, dolor diam sagittis ligula, eget egestas libero turpis vel mi. Fusce vulputate eleifend sapien. Etiam vitae tortor. In dui magna, posuere eget, vestibulum et, tempor auctor, justo. Vivamus elementum semper nisi. In auctor lobortis lacus. Suspendisse faucibus, nunc et pellentesque egestas, lacus ante convallis tellus, vitae iaculis lacus elit id tortor. Donec posuere vulputate arcu. Suspendisse non nisl sit amet velit hendrerit rutrum. Quisque id mi. Vestibulum rutrum, mi nec elementum vehicula, eros quam gravida nisl, id fringilla neque ante vel mi. Nam eget dui. Nullam nulla eros, ultricies sit amet, nonummy id, imperdiet feugiat, pede. In auctor lobortis lacus.	View Edit Delete

This demonstration is modeled after the official [Getting Started](#) Rails Guide.

A simple app to perform CRUD operations on Articles.

The app seems to function perfectly, but it could use some improvements. After more development work, we have a new version of to deploy. We could update the `app_version` variable in `vars.yml` and run `vagrant provision` to run the entire provisioning and deployment playbook again, but to save a little time, and to utilize the more flexible playbook layout (with provisioning and deployment concerns separated), we can run the `deploy.yml` playbook separately.

Deploying application updates

First, to test whether we can deploy without provisioning, we will need to create an inventory file to tell Ansible how to connect directly to the Vagrant-managed VM.

Create the file `playbooks/inventory-ansible` with the following contents:

```
1 [rails]
2 192.168.33.7
3
4 [rails:vars]
5 ansible_ssh_user=vagrant
6 ansible_ssh_private_key_file=~/vagrant/.d/insecure_private_key
```



If you were creating this playbook for a server or VM running outside of Vagrant's control, you'd probably have already created an inventory file or added the server to your global inventory, but when we're working with Vagrant, it's often convenient to use Vagrant's own dynamically-managed inventory. Running playbooks outside of Vagrant's `up/provision` functionality requires us to create a separate inventory file.

Test the ability to run the `deploy.yml` playbook by running the following command inside the `playbooks` directory:

```
$ ansible-playbook deploy.yml -i inventory-ansible
```

Hopefully the playbook completed its run successfully. It may have reported a change in the “Ensure demo application has correct user for files” task, and if so, it will have restarted Passenger. Run it again, and ansible should report no changes:

```
PLAY RECAP ****
192.168.33.7 : ok=16    changed=0    unreachable=0    failed=0
```

Hopefully you've noticed that running the `deploy.yml` playbook standalone is much faster than running the `provision` and `deploy` playbooks together (deployment only takes 16 tasks, while both playbooks add up to 70+ tasks!). In the future, we can deploy application updates using only the `deploy.yml` playbook and changing the `app_version` either in `vars.yml` or by specifying the version on the command line in the `ansible-playbook` command.



It's generally preferred to change variables in `vars` files that are versioned with your playbooks, rather than specify them through inventory files, environment variables, or on the command line. This way the entire state of your infrastructure is encapsulated in your playbook files, which ideally should be version controlled and managed similarly to the application they deploy. Plus, who wants to enter any more information on the command line than is absolutely required?

Our application is a fairly generic web application that has updates to application code (which require a webserver reload), styles (which need recompiling), and possibly the database schema (which needs `rake migrate` tasks to be run). Any time `app_version` is changed inside `playbooks/vars.yml`, the deploy playbook will automatically run all the required tasks to get our app running with the latest code.

Update `app_version` to `1.3.0`, and then run the following command again:

```
$ ansible-playbook deploy.yml -i inventory-ansible
```

After a minute or so, the deployment should complete, and once that's done, you'll see the much improved new version of the Demonstration Ruby on Rails Application:



Rails app - version 1.3.0 with a responsive UI.

Simple application update deployments will involve incrementing the `app_version` to the latest git tag, then running the `deploy.yml` playbook again. You can always run the `main.yml` playbook to ensure the entire server stack is in the correct state, but it's faster to just deploy the app updates.

Zero-downtime multi-server deployments

If you need to run an application on multiple servers for horizontal scalability or redundancy, deployments can be cumbersome, resulting in downtime and complicated deployment processes—but not when you use Ansible!

[Server Check.in¹⁰⁷](#) is a simple server and website monitoring service that has a microservices-based architecture; there is a website, an API application, and a server checking application.

The server checking application needs to run on a variety of servers hosted around the world by

```

13   end
14
15   # Define four VMs with static private IP addresses.
16   boxes = [
17     { :name => "nodejs1", :ip => "192.168.3.2" },
18     { :name => "nodejs2", :ip => "192.168.3.3" },
19     { :name => "nodejs3", :ip => "192.168.3.4" },
20     { :name => "nodejs4", :ip => "192.168.3.5" }
21   ]
22
23   # Provision each of the VMs.
24   boxes.each do |opts|
25     config.vm.define opts[:name] do |config|
26       config.vm.hostname = opts[:name]
27       config.vm.network :private_network, ip: opts[:ip]
28
29       # Provision all the VMs using Ansible after the last VM is booted.
30       if opts[:name] == "nodejs4"
31         config.vm.provision "ansible" do |ansible|
32           ansible.playbook = "playbooks/main.yml"
33           ansible.inventory_path = "inventory"
34           ansible.limit = "all"
35         end
36       end
37     end
38   end
39
40 end

```

The above `Vagrantfile` defines four VMs that each use 256MB of RAM and have a unique hostname and IP address (defined by the `boxes` variable). Our Node.js app doesn't require much in the way of processing power or memory.

In the provision section of the playbook, we told Vagrant to provision the all the VMs with Ansible, using the inventory file `inventory`, and the playbook `playbooks/main.yml`. Create these two files in the same folder as your `Vagrantfile`:

```

deployments-rolling/
  playbooks/
    main.yml
  inventory
  Vagrantfile

```

Inside the `inventory` file, we just need to define a list of all the Node.js API app VMs by IP address:

```
1 [nodejs-api]
2 192.168.3.2
3 192.168.3.3
4 192.168.3.4
5 192.168.3.5
6
7 [nodejs-api:vars]
8 ansible_ssh_user=vagrant
9 ansible_ssh_private_key_file=~/vagrant.d/insecure_private_key
```

Inside the `main.yml` playbook, we'll call out two separate playbooks—one for the initial provisioning (installing Node.js and making sure the server is configured correctly), and another for deployment (ensuring our Node.js API app is present and running):

```
1 ---
2 - include: provision.yml
3 - include: deploy.yml
```

Go ahead and create the `provision.yml` and `deploy.yml` playbooks, starting with `provision.yml`:

```
1 ---
2 - hosts: nodejs-api
3   sudo: yes
4
5   vars:
6     nodejs_forever: true
7     firewall_allowed_tcp_ports:
8       - "22"
9       - "8080"
10
11   roles:
12     - geerlingguy.firewall
13     - geerlingguy.nodejs
```

This extremely simple playbook runs on all the servers defined in our inventory file, and runs two roles on the servers: `geerlingguy.firewall` (which installs and configures a firewall, in this case opening ports 22 for SSH and 8080 for our app) and `geerlingguy.nodejs` (which installs Node.js, NPM, and `forever`, which we'll use to run our app as a daemon).

Since we're using two roles from Ansible Galaxy, it's best practice to also include those roles in a requirements file so CI tools and others using this playbook can easily install all the required roles.

Create a `requirements.txt` file in the root folder and add the following:

```
1 geerlingguy.firewall  
2 geerlingguy.nodejs
```

Now, whenever someone new to the project wants to run the playbook, all that person needs to do is run `ansible-galaxy install -r requirements.txt` to install all the required roles.

At this point, your project directory should be structured like the following:

```
deployments-rolling/  
  playbooks/  
    deploy.yml  
    main.yml  
    provision.yml  
  inventory  
  requirements.txt  
  Vagrantfile
```

Before we can run `vagrant up` and see our infrastructure in action, we need to build out the `deploy.yml` playbook, which will ensure our app is present and running correctly on all the servers.

Inside `deploy.yml`, add the following:

```
1 ---  
2 - hosts: nodejs-api  
3   gather_facts: no  
4   sudo: yes  
5  
6   vars_files:  
7     - vars.yml
```

Use `sudo` for this playbook to keep things simple, and set `gather_facts` to `no` to save a little time during deployments, since our simple app doesn't require any of the gathered system facts to run.

Since we have a few variables to define, and we'd like to track them separately for easier file revision history, we'll define the variables in a `vars.yml` file in the same directory as the `deploy.yml` playbook:

```
1 ---  
2 app_repository: https://github.com/geerlingguy/demo-nodejs-api.git  
3 app_version: "1.0.0"  
4 app_directory: /opt/demo-nodejs-api
```

Once you've saved the `vars.yml` file, continue building out `deploy.yml`, starting with a task to clone the app's repository (which we just defined in `vars.yml`):

```
9  tasks:
10 - name: Ensure Node.js API app is present.
11   git:
12     repo: "{{ app_repository }}"
13     version: "{{ app_version }}"
14     dest: "{{ app_directory }}"
15     accept_hostkey: true
16     register: app_updated
17     notify: restart forever apps
```

Using variables for the `git` module's `repo` and `version` affords flexibility; app version changes might happen frequently, and it's easier to manage that in a separate `vars.yml` file.

We also want to `notify` a `restart forever apps` handler whenever the codebase is changed. We'll define the `restart forever apps` handler later in the playbook.

```
18 - name: Stop all running instances of the app.
19   command: "forever stopall"
20   when: app_updated.changed
21
22 - name: Ensure Node.js API app dependencies are present.
23   npm: "path={{ app_directory }}"
24   when: app_updated.changed
25
26 - name: Run Node.js API app tests.
27   command: "npm test chdir={{ app_directory }}"
28   when: app_updated.changed
```

Once the app is present on the server, we need to use `npm` to install dependencies (using Ansible's `npm` module), then run the app's test suite using `npm test`. To save time, we only stop the application, update dependencies, and run tests if the application has changed (using the `app_updated` variable we registered when checking out the application code).

Running the tests for the app during every deployment ensures the app is present and in a functioning state. Having a thorough unit and integration test suite that runs on every deployment is almost prerequisite to a frequent or continuously-integrated project! Running the tests during deployments also helps with ensuring zero-downtime deployments, as we'll see later.

```

25      - name: Get list of all running Node.js apps.
26        command: forever list
27        register: forever_list
28        changed_when: false
29
30      - name: Ensure Node.js API app is started.
31        command: "forever start {{ app_directory }}/app.js"
32        when: "forever_list.stdout.find('app.js') == -1"

```

Once the app is present and running correctly, we need to make sure it's started. There's a command to get the list of all running apps (using `forever`), then a command to start the app if it's not already running.

```

34      - name: Add cron entry to start Node.js API app on reboot.
35        cron:
36          name: "Start Node.js API app"
37          special_time: reboot
38          job: "forever start {{ app_directory }}/app.js"

```

The final task adds a cron job to make sure the app is started after the server reboots. Since we're managing the deamonization of our app using `forever` instead of the OS's init system, it's simplest to make sure the app starts on system boot using a reboot cron job.

Remember when we added the line `notify: restart forever apps` to the task that ensured the app was present on the server? It's time to define that handler, which runs the command `forever restartall` (which does exactly what it says):

```

40  handlers:
41    - name: restart forever apps
42      command: "forever restartall"

```

At this point, the Ansible playbooks and Vagrant configuration should be complete. The playbook will clone the `demo-nodejs-api` project, run its tests to make sure everything's working correctly, then start the app using `forever` and make sure it's started whenever the the server reboots.

You can run the command below to test all the new servers and make sure the app is running correctly:

```
$ for i in {2..5}; \
  do curl -w "\n" "http://192.168.3.$i:8080/hello/john"; \
done
```

If all the servers are online, you should see the text "hello john" repeated four times (once for each server):

```
"hello john"  
"hello john"  
"hello john"  
"hello john"
```

You can run `vagrant provision` to run the entire provisioning and deployment process again, or just run `ansible-playbook -i inventory playbooks/deploy.yml` to run the deployment playbook again. In either case, you should see no changes, and Ansible should verify that everything's ok.

You now have a fleet of Node.js API servers similar to Server Check.in's server checking infrastructure—except it doesn't do much yet! Luckily, the project has seen some new feature development since the initial `1.0.0` version you just deployed. We now need a way to get the new version deployed to and running on all the servers while maintaining 100% uptime for the API as a whole.

Ensuring zero downtime with serial and integration tests

Now, after a little extra time in development, we have new features to deploy in a `1.0.1` version. You could run the exact same `ansible-playbook` command as above, adding in `--extra-vars "app_version=1.0.1"`, but best practice is to update the variable in your included variables file, since that change can be tracked in version control and (hopefully) be used for automated deployments.

Change the `app_version` in `playbooks/vars.yml` to `1.0.1`, and run the deployment playbook again:

```
ansible-playbook -i inventory playbooks/deploy.yml
```

Uh oh—after we deployed the new version, our tests started failing! Since we deployed to all four servers asynchronously, all four application servers are offline, and our boss and customers are going to be very angry.

In this case, rolling back is simply a matter of reverting to `1.0.0` and redeploying (go ahead and do that now, so you keep at least a few 9's of uptime!), but imagine if part of the application update changed a database schema or did something else that required a lot more work to roll back changes; you'd be in a world of hurt!

Ansible has two particular settings that will help protect you when you deploy to many servers while maintaining your infrastructure's overall integrity during a failed deployment.

Open the deployment playbook (`playbooks/deploy.yml`) and modify the initial settings to match the following:

```
1  ---
2  - hosts: nodejs-api
3    gather_facts: no
4    sudo: yes
5    serial: 2
```

Note the addition of `serial: 1`. This tells Ansible to run the entire playbook on two servers at a time. If you update `app_version` to `1.0.1` again, and run the playbook, you should see it run on two of the four servers, and once it hits the test failure, the playbook execution will stop—leaving your other two servers up (and saving you a few hours on a conference bridge explaining the outage).

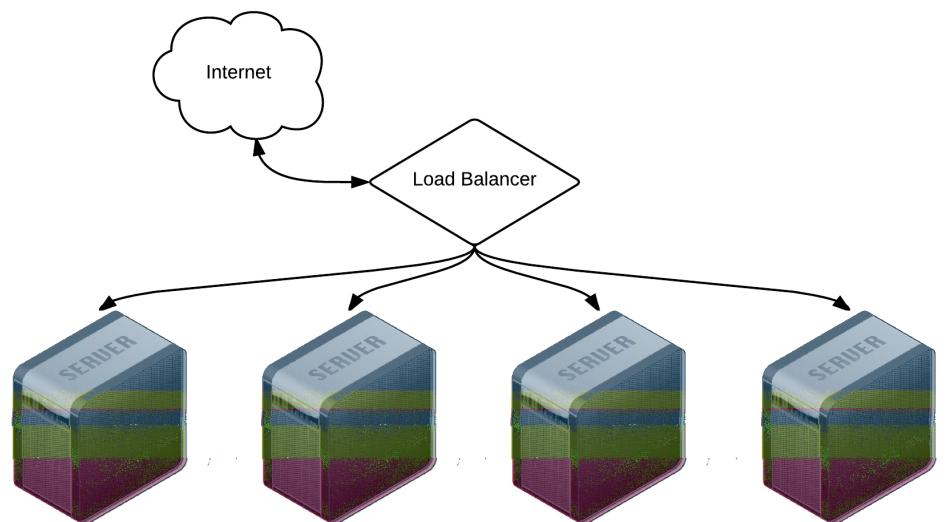
You could again revert back to `1.0.0`, but in the time that you were deploying the failed version, developers finished a new version that got all tests passing again, `1.0.2`. Go ahead and update `app_version` and run the playbook again.

```
PLAY RECAP ****
192.168.3.2
```

Deploying to app servers behind a load balancer

In the case of Server Check.in, there are two separate API layers that manage the complexity of ensuring all server checks happen, regardless of whether certain servers are up or down. The ‘load balancing’ occurs on the application layer instead of as a separate infrastructure layer (this is extremely helpful when dealing with global latency and network reliability variation).

For many applications, especially those with app servers close together (e.g. in the same data center) the infrastructure layer follows a more traditional layout, with a load balancer to handle the API request distribution:



Four servers behind a load balancer.

For a simple demonstration of zero-downtime deployment with a load balancer, let’s build a local infrastructure with one HAProxy load balancer and two Apache webservers.

First, create a new project folder `deployments-balancer`, and within it, create the following `Vagrantfile`:

```

1 # -*- mode: ruby -*-
2 # vi: set ft=ruby :
3
4 Vagrant.configure("2") do |config|
5   # Base VM OS configuration.
6   config.vm.box = "geerlingguy/ubuntu1404"
7   config.vm.synced_folder '.', '/vagrant', disabled: true
8   config.ssh.insert_key = false
9
10  config.vm.provider :virtualbox do |v|

```

```
11     v.memory = 256
12     v.cpus = 1
13   end
14
15 # Define four VMs with static private IP addresses.
16 boxes = [
17   { :name => "bal1", :ip => "192.168.4.2" },
18   { :name => "app1", :ip => "192.168.4.3" },
19   { :name => "app2", :ip => "192.168.4.4" }
20 ]
21
22 # Provision each of the VMs.
23 boxes.each do |opts|
24   config.vm.define opts[:name] do |config|
25     config.vm.hostname = opts[:name]
26     config.vm.network :private_network, ip: opts[:ip]
27
28   # Provision all the VMs using Ansible after the last VM is booted.
29   if opts[:name] == "app2"
30     config.vm.provision "ansible" do |ansible|
31       ansible.playbook = "playbooks/provision.yml"
32       ansible.inventory_path = "inventory"
33       ansible.limit = "all"
34     end
35   end
36 end
37 end
38
39 end
```

This Vagrantfile will create three servers running Ubuntu 14.04: `bal1` (the balancer), and `app1` and `app2` (the application servers). We referenced an Ansible playbook at `playbooks/provision.yml` (to install the required software on the servers), as well as a custom inventory file at `inventory`. First, create the inventory file (`inventory`, in the same directory as the Vagrantfile), with the appropriate groupings and connection variables:

```
1 [balancer]
2 192.168.4.2
3
4 [app]
5 192.168.4.3
6 192.168.4.4
7
8 [deployments:children]
9 balancer
10 app
11
12 [deployments:vars]
13 ansible_ssh_user=vagrant
14 ansible_ssh_private_key_file=~/.vagrant.d/insecure_private_key
```

With this inventory, we can operate on just the balancer, just the app servers, or all the servers together (in the deployments group). Next, create a simple playbook (at playbooks/provision.yml) to provision the servers:

```
1 ---
2   - hosts: balancer
3     sudo: yes
4
5   vars:
6     firewall_allowed_tcp_ports:
7       - "22"
8       - "80"
9     haproxy_backend_servers:
10      - name: 192.168.4.3
11        address: 192.168.4.3:80
12      - name: 192.168.4.4
13        address: 192.168.4.4:80
14
15   roles:
16     - geerlingguy.firewall
17     - geerlingguy.haproxy
18
19   - hosts: app
20     sudo: yes
21
22   vars:
23     firewall_allowed_tcp_ports:
```

```

24      - "22"
25      - "80"
26
27  roles:
28    - geerlingguy.firewall
29    - geerlingguy.apache

```

These two plays set up a firewall on both servers, and configure HAProxy on the load balancer, and Apache (with its default configuration) on the app servers. The only required configuration to get this infrastructure working is `haproxy_backend_servers`. We let the `geerlingguy.firewall`, `geerlingguy.haproxy`, and `geerlingguy.apache` roles do all the hard work for us.

Now, to make sure we have all these roles installed, create a requirements file to install the roles from Ansible Galaxy. Create `requirements.txt` in the same directory as the `Vagrantfile`, with the following contents:

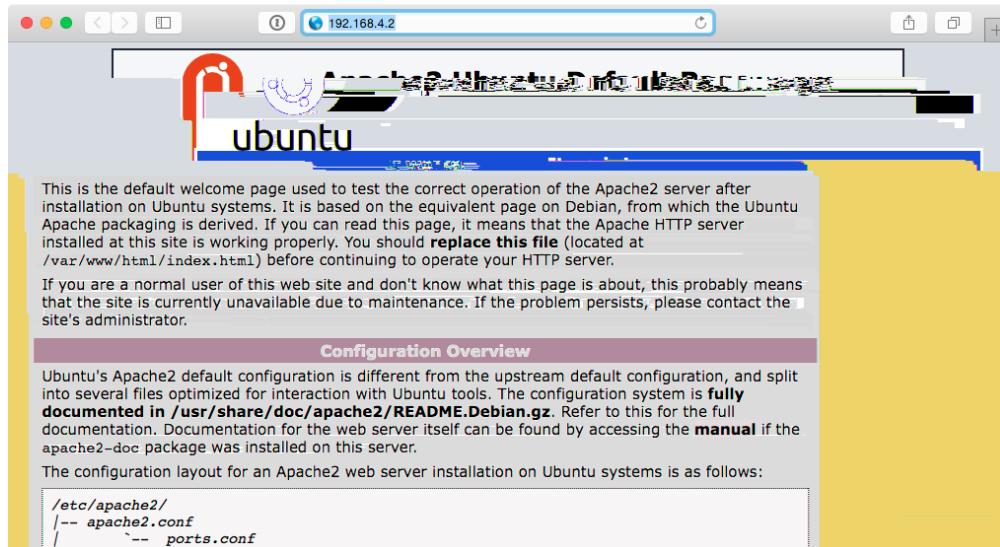
```

1 geerlingguy.firewall
2 geerlingguy.haproxy
3 geerlingguy.apache

```

To install the required roles, run `sudo ansible-galaxy install -r requirements.txt`.

At this point, if you want to bring up your local load-balanced infrastructure, run `vagrant up` in the `deployments-balancer` directory, and wait a few minutes. Once everything is up and running, visit `http://192.168.4.2/`, and you should see the default Ubuntu Apache2 landing page:



HAProxy is serving requests through the Apache backend servers.

You can verify that round-robin load balancing is working by running the following command:

```
1 $ for i in {1..5}; do curl -Is http://192.168.4.2/ | grep Cookie; done
2 Set-Cookie: SERVERID=192.168.4.4; path=/
3 Set-Cookie: SERVERID=192.168.4.3; path=/
4 Set-Cookie: SERVERID=192.168.4.4; path=/
5 Set-Cookie: SERVERID=192.168.4.3; path=/
6 Set-Cookie: SERVERID=192.168.4.4; path=/
```

You should see that the load balancer is distributing requests between the two backend app servers.

When you want to deploy new code to the application servers, you need to do it in a way that guarantees the load balancer will always have an app server from which requests can be served, so you want to use `serial` to do the deployment on each server (or groups of servers) in sequence. And to make sure the servers are properly removed from HAProxy, then added again post-deploy, you can use `pre_tasks` and `post_tasks`.

Create another playbook alongside `provision.yml` called `deploy.yml`, with the following contents:

```
1 ---
2   - hosts: app
3     sudo: yes
4     serial: 1
5
6   pre_tasks:
7     - name: Disable the backend server in HAProxy.
8       haproxy:
9         state: disabled
10        host: '{{ inventory_hostname }}'
11        socket: /var/lib/haproxy/stats
12        backend: habackend
13        delegate_to: "{{ item }}"
14        with_items: groups.balancer
15
16   tasks:
17     - debug: msg="Deployment would be done here."
18
19   post_tasks:
20     - name: Wait for backend to come back up.
21       wait_for:
22         host: '{{ inventory_hostname }}'
23         port: 80
24         state: started
25         timeout: 60
26
```

```
27      - name: Enable the backend server in HAProxy.
28        haproxy:
29          state: enabled
30          host: '{{ inventory_hostname }}'
31          socket: /var/lib/haproxy/stats
32          backend: habackend
33        delegate_to: "{{ item }}"
34        with_items: groups.balancer
```

This playbook doesn't do much in terms of actual deployment, but it does illustrate how to do a zero-downtime rolling update over two or more application servers:

1. In `pre_tasks`, the `haproxy` module disables the current app server (using the `inventory_hostname` variable) on all the load balancers in the `balancer` group, using `with_items`. The HAProxy task is delegated to each of the `balancer` servers (in our case, only one), since the task affects the load balancer, not the current app host.
2. In the `post_tasks`, we first `wait_for` port 80 to be available, and once it is, the `haproxy` module re-enables the current app server on all the load balancers.

Run the playbook on the local infrastructure with the following command:

```
1 $ ansible-playbook -i inventory playbooks/deploy.yml
```

It should only take a few seconds to run, and once it's finished, all the servers should be back in the mix for the load balancer. If you want to quickly confirm that the deployment playbook is working as it should, you can add a task which always fails, immediately following the `debug` task:

```
15 [...]
16 tasks:
17   - debug: msg="Deployment would be done here."
18   - command: /bin/false
19
20 post_tasks:
21 [...]
```

If you run the deployment playbook again, wait for it to fail, then run the `curl` command again, you'll notice all the requests are being directed to the second app server:

```
1 $ for i in {1..5}; do curl -Is http://192.168.4.2/ | grep Cookie; done
2 Set-Cookie: SERVERID=192.168.4.4; path=/
3 Set-Cookie: SERVERID=192.168.4.4; path=/
4 Set-Cookie: SERVERID=192.168.4.4; path=/
5 Set-Cookie: SERVERID=192.168.4.4; path=/
6 Set-Cookie: SERVERID=192.168.4.4; path=/
```

You can fix the deployment by removing the `/bin/false` command. Run the playbook one more time to restore the infrastructure to a fully functional state.

This demonstration may seem basic, but the `pre_tasks` and `post_tasks` in the playbook are identical to what many large-scale production infrastructure deployments use!

Capistrano-style and blue-green deployments

Many developers who deal with Ruby applications are familiar with [Capistrano](#)¹⁰⁸, a task automation and application deployment application built with Ruby. Capistrano's basic style of deployment is to create dated release directories, then symlink the current release into a stable application directory, along with resources that are continuous among releases (like logs and uploaded files).

Capistrano does a lot more than that basic deployment model, but many people want to replicate that simple application deployment workflow (which is also fairly simple for rollbacks, since you just revert the symlink to the previous release directory!). This is fairly simple to do with Ansible, and rather than walk you through the entire process in this book, I'll point you to a few great resources that explain the process in detail, along with an Ansible Galaxy role that coordinates Capistrano-style deployments even more easily!

- Rebuilding Capistrano-like deployment with Ansible¹⁰⁹
- `project_deploy` role on Ansible Galaxy¹¹⁰
- Thoughts on deploying with Ansible¹¹¹ (background for the above role)
- Ansible `project-deploy`¹¹² (presentation about the above role)

Extending things a little further, many organizations use **blue-green** deployments. The basic concept involves bringing up a parallel production infrastructure, then switching over to it. The cutover may take only a few milliseconds and no active production infrastructure is ever offline during the deployment process.

¹⁰⁸<http://capistranorb.com/>

¹⁰⁹<http://blog.versioneye.com/2014/09/24/rebuilding-capistrano-like-deployment-with-ansible/>

¹¹⁰<https://galaxy.ansible.com/list#/roles/732>

¹¹¹<http://www.future500.nl/articles/2014/07/thoughts-on-deploying-with-ansible/>

¹¹²<http://www.slideshare.net/ramondelafuente/ansible-projectdeploy>

A few different technologies and concepts, like container-based infrastructure and microservices (which are faster to deploy), and better cloud autoscaling and load balancing options, have made blue-green deployments much easier than in the past.

This book won't go through a detailed example of this style of deployment, as the process is similar to other examples provided, the only difference being an additional task of switching a load balancer from the old to the new infrastructure once it's up and running. Ansible's blog has an excellent overview of AWS-based blue-green deployments: [Immutable Systems and Ansible¹¹³](#), and there are built-in modules to manage almost any type of load balancer you could use, including [F5's BIG-IP¹¹⁴](#), [HAProxy¹¹⁵](#), [Citrix NetScaler¹¹⁶](#), and [Amazon ELB¹¹⁷](#).

Additional Deployment Features

There are a few other Ansible modules and options which are helpful in the context of deployments: `run_once`¹¹⁸ and `delegate_to` are extremely helpful in scenarios like updating a database schema or clearing an application's cache, where you need a particular task to only run one time, on a particular server:

```
- command: /opt/app/upgrade-database-schema
  run_once: true
  delegate_to: app1.example.com
```

Using `run_once` with `delegate_to` is similar to the pattern of using `when: inventory_hostname == groups.groupname[0]`, but is a little more precise in describing what you're trying to achieve—running a command once on a specific host.

Another important aspect of a successful deployment is communication. If you're running playbooks as part of a CI/CD process, or in some other automated fashion, you can use one of the many built-in Ansible notification modules to share the deployment's progress via chat, email, or even text-to-speech on your Mac with the `osx_say` module! Ansible includes easy-to-use notification modules for:

- Campfire
- HipChat
- IRC
- Jabber

¹¹³<http://www.ansible.com/blog/immutable-systems>

¹¹⁴http://docs.ansible.com/list_of_network_modules.html#f5

¹¹⁵http://docs.ansible.com/haproxy_module.html

¹¹⁶http://docs.ansible.com/netscaler_module.html

¹¹⁷http://docs.ansible.com/ec2_elb_module.html

¹¹⁸http://docs.ansible.com/playbooks_delegation.html#run-once

- Email
- Slack
- Twilio
- Amazon SNS
- etc.

Many playbooks include notifications in both the `pre_tasks` and `post_tasks` sections, notifying admins in a chat channel when a deployment begins or ends. For example:

```
post_tasks:  
  - name: Tell everyone on IRC the deployment is complete.  
    irc:  
      channel: my-org  
      server: irc.example.com  
      msg: "Deployment complete!"  
      delegate_to: 127.0.0.1
```

For a great primer on Ansible notifications, see Ansible Inc's blog post: [Listen to your Servers Talk¹¹⁹](#).

Summary

Automating deployments with Ansible enables your development team to have their code on production servers more reliably and quickly, and it enables your operations team to spend less time on repetitive tasks, and more time improving your infrastructure.

This chapter outlined only a few of the most popular deployment techniques, but Ansible is flexible enough to handle almost any situation out of the box.

```
/ One machine can do the work of fifty  \  
| ordinary men. No machine can do the   |  
| work of one extraordinary man.        |  
\ (Elbert Hubbard)                   /  
-----  
 \  ^__^  
  \  (oo)\_____  
   (__)\       )\/\ \  
     ||----w |  
     ||     ||
```

¹¹⁹<http://www.ansible.com/blog/listen-to-your-servers-talk>

Chapter 10 - Server Security and Ansible

One of the first configuration steps that should be performed on any new server—especially any server with any exposure (direct or indirect) to the public Internet—is security configuration.

I debated adding this chapter earlier in the book, as the importance of a secure configuration (especially when automating server configuration, application deployments, etc.) cannot be understated. But as it is, I decided to focus on Ansible's core functionality before giving a general overview of security, especially pertaining to Linux servers.

There are nine basic measures that must be taken to make sure that servers are secure from unauthorized access or intercepted communications:

1. Use secure and encrypted communication.
2. Disable root login and use `sudo`.
3. Remove unused software, open only required ports.
4. Use the principle of least privilege.
5. Update the OS and installed software.
6. Use a properly-configured firewall.
7. Make sure log files are populated and rotated.
8. Monitor logins and block suspect IP addresses.
9. Use SELinux (Security-Enhanced Linux).

Your infrastructure is as weak as the weakest server; in many high-profile security breaches, one poorly-secured server acts as a gateway into the rest of the network. Don't let your servers be *those* servers! Good security also helps you achieve the holy grail of system administration—100% uptime.

In this chapter, you'll learn about Linux security and how Ansible can help secure your servers, following the basic topics above.

A brief history of SSH and remote access

In the beginning, computers were the size of large conference rooms. A punch card reader would merrily accept pieces of paper that instructed the computer to do something, and then a printer would etch the results into another piece of paper. Thousands of mechanical parts worked harmoniously (when they *did* work) to compute relatively simple commands.

As time progressed, computers became somewhat smaller, and interactive terminals became more user-friendly, but they were still wired directly into the computer being used. Mainframes came to the fore in the 1960s, originally used via typewriter and teletype interfaces, then via keyboards and small text displays. As networked computing became more mainstream in the 1970s and 1980s, remote terminal access was used to interact with the large central computers.

The first remote terminal interfaces assumed a high level of trust between the central computer and all those on the network, because the small, centralized networks used were physically isolated from one another.

Telnet

In the late 1960s, the Telnet protocol was defined and started being used over TCP networks (normally on port 23) for remote control over larger private networks, and eventually the public Internet.

Telnet's underlying technology (a text-based protocol to transfer data between different systems) was the basis for many foundational communications protocols in use today, including HTTP, FTP, and POP3. However, plain text streams are not secure, and even with the addition of TLS and SASL, Telnet was never very secure by default. With the advent of SSH (which we'll get to in a bit), the protocol has declined in popularity for most remote administration purposes.

Telnet still has uses like configuring devices over local serial connections, or checking if a particular service is operating correctly on a remote server (like an HTTP server on port 80, mysql on port 3306, or munin on port 4949), but it is not installed by default on modern Linux distributions.



Plain text communications over a network are only as secure as the network's weakest link. In the early days of computer networking, networks were usually isolated to a specific company or educational institution, so transmitting things like passwords or secrets in plain text using the TCP protocol wasn't such a bad idea. Every part of the network (cabling, switches, and routers) was contained inside a secured physical perimeter. When connections started moving to the public Internet, this changed.

TCP packets can be intercepted over the Internet, at any point between the client and server, and these packets can easily be read if not encrypted. Therefore, plain text protocols are highly insecure, and should never be used to transmit sensitive information or system control data. Even on highly secure networks with properly-configured firewalls, it's a bad idea to use insecure communication methods like plain text rlogin and telnet connections for authentication and remote control.

Try running `traceroute google.com` in your terminal. Look at each of the hops between you and Google's CDN. Do you know who controls each of the devices between your computer and Google? Do you trust these operators with all of your personal or corporate secrets? Probably not. Each of these connection points—and each network device and cable connecting them—is a weak point exposing you to a man-in-the-middle attack. Strong encryption is needed between your computer and the destination if you want to ensure data security.

rlogin, rsh and rcp

rlogin was introduced in BSD 4.2 in 1983, and has been distributed with many UNIX-like systems alongside Telnet until recently. rlogin was used widely during the 80s and much of the 90s.

Just like Telnet, a user could log into the remote system with a password, but rlogin additionally allowed automatic (passwordless) logins for users on trusted remote computers. rlogin also worked better than telnet for remote administration, as it worked correctly with certain characters and commands where telnet required extra translation.

However, like Telnet, rlogin still used plain text communications over TCP port 513 by default. On top of that, rlogin also didn't have many safeguards against clients spoofing their true identities. Some of rlogin's intrinsic flaws were highlighted in a 1998 report by Carnegie Mellon, [rlogin: The Untold Story](#)¹²⁰.

rsh ("remote shell") is a command line program used alongside rlogin to execute individual shell commands remotely, and rcp ("remote copy") is used for remote file copies. rsh and rcp inherited the same security problems as rlogin, since they use the same connection method (over different ports).

SSH

Secure Shell was created in 1995 by Finland native Tatu Ylönen, in response to a [password-sniffing attack](#)¹²¹ at his university. Seeing the flaws in plain text communication for secure information, Tatu created Secure Shell/SSH with a strong emphasis on encryption and security.

His version of SSH was developed for a few years as freeware with liberal licensing, but as his [SSH Communications Security Corporation](#)¹²² began limiting the license and commercializing SSH, alternative forks began to gain in popularity. The most popular fork, OSSH, by Swedish programmer Bjoern Groenvall, was chosen as a starting point by some developers from the OpenBSD project.

OpenBSD was (and still is!) a highly secure, free version of BSD UNIX, and the project's developers needed a secure remote communication protocol, so a few project members worked to [clean up and improve OSSH](#)¹²³ so it could be included in OpenBSD's 2.6 release in December 1999. From there, it was quickly ported and adopted for all major versions of Linux, and is now ubiquitous in the world of POSIX-compliant operating systems.

How does SSH work, and what makes it better than telnet or rlogin? It starts with the basic connection. SSH connection encryption works similarly to SSL for secure HTTP connections, but its authentication layer adds more security:

1. When you enter `ssh user@example.host` to connect to the `example.host` server as `user`, your client and the host exchange keys.

¹²⁰http://resources.sei.cmu.edu/asset_files/TechnicalReport/1998_005_001_16670.pdf

¹²¹http://en.wikipedia.org/wiki/Secure_Shell#Version_1.x

¹²²<http://www.ssh.com/>

¹²³<http://www.openbsd.org/openssh/history.html>

2. If you’re connecting to a host the first time, or if the host’s key has changed since last time you connected (this happens often when connecting via DNS rather than directly by IP), SSH will prompt you for your approval of the host key.
3. If you have a private key in your `~/ .ssh` folder that matches one of the keys in `~/ .ssh/authorized_keys` on the remote system, the connection will continue to step 4. Otherwise, if password authentication is allowed, SSH will prompt you for your password. There are other authentication methods as well, such as Kerberos, but they are less common and not covered in this book.
4. The transferred key is used to create a session key that’s used for the remainder of the connection, encrypting all communication with a cipher such as AES, 3DES, Blowfish or RC4 ('arcfour').
5. The connection remains encrypted and persists until you exit out of the remote connection (in the case of an interactive session), or until the operation being performed (an `scp` or `sftp` file transfer, for example) is complete.

SSH uses encrypted keys to identify the client and host (which adds a layer of security over `telnet` and `rlogin`’s defaults), and then sets up a per-session encrypted channel for further communication. This same connection method is used for interactive `ssh` sessions, as well as for services like:

- `scp` (secure copy), SSH’s counterpart to `rlogin`’s `rcp`.
- `sftp` (secure FTP), SSH’s client/server file transfer protocol.
- SSH port forwarding (so you can run services securely over remote servers).
- SSH X11 forwarding (so you can use X windows securely).

(A full list of features is available on OpenBSD’s site: [OpenSSH Features¹²⁴](http://www.openbsd.org/openssh/features.html)).

The full suite of SSH packages also includes helpful utilities like `ssh-keygen`, which generates public/private key pairs suitable for use when connecting via SSH. You can also install the utility `ssh-copy-id`, which speeds up the process of manually adding your identity file to a remote server.

SSH is fairly secure by default—certainly more so than `telnet` or `rlogin`’s default configuration—but for even greater security, there are a few extra settings you should use (all of these settings are configured in `/etc/ssh/sshd_config`, and require a restart of the `sshd` service to take effect):

1. **Disable password-based SSH authentication.** Even though passwords are sent in the clear, disabling password-based authentication makes it impossible for brute-force password attacks to even be *attempted* even if you have the additional (and recommended) layer of something like Fail2Ban running. Set `PasswordAuthentication no` in the configuration.

¹²⁴<http://www.openbsd.org/openssh/features.html>

2. **Disable root account remote login.** You shouldn't log in as the root user regardless (use sudo instead), but to reinforce this good habit, disable remote root user account login by setting PermitRootLogin no in the configuration. If you need to perform actions as root, either use sudo (preferred), or if it's absolutely necessary to work interactively as root, login with a normal account, then su to the root account.
3. **Explicitly allow/deny SSH for users.** You can enable or disable SSH access for particular users on your system with AllowUsers and DenyUsers. To allow only 'John' to log in, the rule would be AllowUsers John. To allow any user *except* John to log in, the rule would be DenyUsers John.
4. **Use a non-standard port.** You can change the default SSH port from 22 to something more obscure, like 2849, and prevent thousands of 'script kiddie' attacks that look for servers responding on port 22. While security through obscurity is no substitute for actually securing SSH overall, it can provide a slight extra layer of protection. To change the port, set Port [new-port-number] in the configuration.

We'll cover how Ansible can help configure some of these particular options in SSH in the next section.

The evolution of SSH and the future of remote access

It has been over a decade since OpenSSH became the *de facto* standard of remote access protocols, and in that time, Internet connectivity has changed dramatically. For reliable, low-latency LAN and Internet connections, SSH is still the king due to its simplicity, speed, and security. But in high-latency environments (think 3G or 4G mobile network connections, or satellite uplinks), using SSH can be a slow and painful experience.

In some circumstances, just *establishing a connection* can take some time. Additionally, once connected, the delay inherent in SSH's TCP interface (where every packet must reach its destination and be acknowledged before further input will be accepted) means entering commands or viewing progress over a high-latency connection is an exercise in frustration.

Mosh¹²⁵, "the mobile shell", a new alternative to SSH, uses SSH to establish an initial connection, then synchronizes the following local session with a remote session on the server via UDP.

Using UDP instead of TCP requires Mosh to do a little extra behind-the-scenes work to synchronize the local and remote sessions (instead of sending all local keystrokes over the wire serially via TCP, then waiting for stdout and stderr to be returned, like SSH).

Mosh also promises better UTF-8 support than SSH, and is well supported by all the major POSIX-like operating systems (and can even run inside Google Chrome!).

It will be interesting to see where the future leads with regard to remote terminal access, but one thing is for sure: Ansible will continue to support the most secure, fast, and reliable connection methods to help you build and manage your infrastructure!

¹²⁵<https://www.usenix.org/system/files/conference/atc12/atc12-final32.pdf>

Use secure and encrypted communication

We spent a lot of time discussing SSH's heritage and the way it works because it is, in many ways, the foundation of a secure infrastructure—in almost every circumstance, you will allow SSH remote access for your servers, so it's important you know how it works, and how to configure it to ensure you always administer the server securely, over an encrypted connection.

Let's look at the security settings configured in `/etc/ssh/sshd_config` (mentioned earlier), and how we can control them with Ansible.

For our secure server, we want to disable password-based SSH authentication (make sure you can already log in via your SSH key before you do this!), disable remote root login, and change the port over which SSH operates. Let's do it!

```
1  - hosts: example
2    tasks:
3      - name: Update SSH configuration to be more secure.
4        lineinfile:
5          dest: /etc/ssh/sshd_config
6          regexp: "{{ item.regexp }}"
7          line: "{{ item.line }}"
8          state: present
9        with_items:
10       - {
11         regexp: "^\$PasswordAuthentication",
12         line: "PasswordAuthentication no"
13       }
14       - {
15         regexp: "^\$PermitRootLogin",
16         line: "PermitRootLogin no"
17       }
18       - {
19         regexp: "^\$Port",
20         line: "Port 2849"
21       }
22     notify: restart ssh
23
24   handlers:
25     - name: restart ssh
26       service: name=ssh state=restarted
```

In this extremely simple playbook, we set three options in SSH configuration (`PasswordAuthentication no`, `PermitRootLogin no`, and `Port 2849`) using Ansible's `lineinfile` module, then use a handler

we define in the `handlers` section to restart the ssh service. (Note that the task and handler defined here would probably be in separate files in a real-world playbook).



Note that if you change certain SSH settings, like the port for SSH, you will need to make sure Ansible's inventory is updated. You can explicitly define the SSH port for a host with the option `ansible_ssh_port`

```
- name: Add sudo group rights for deployment user.
  lineinfile:
    dest: /etc/sudoers
    regexp: '^%johndoe'
    line: 'johndoe ALL=(ALL) NOPASSWD: ALL'
    state: present
```

If you're ever editing the sudoers file by hand, you should use `visudo`, which validates your changes and makes sure you don't break sudo when you save the changes. When using Ansible with `lineinfile`, you have to use caution when making changes, and make sure your syntax is correct.

Another way of changing the sudoers file, and ensuring the integrity of the file, is to create a sudoers file locally, and copy it using Ansible's `copy` module, with a validation command, like so:

```
- name: Copy validated sudoers file into place.
  copy:
    src: sudoers
    dest: /etc/sudoers
    validate: 'visudo -cf %s'
```

The `%s` is a placeholder for the file's path, and will be filled in by Ansible before the sudoers file is copied into its final destination. The same parameter can be passed into Ansible's `template` module, if you need to copy a filled-in template to the server instead of a static file.



The sudoers file syntax is very powerful and flexible, but also a bit obtuse. Read the entire [Sudoers Manual¹²⁶](#) for all the details, or check out the [sample sudoers file¹²⁷](#) for some practical examples.

Remove unused software, open only required ports

Before the widespread use of configuration management tools for servers, when snowflake servers were the norm, many servers would become bloated with extra software no longer in active use, open ports for old services that are no longer needed, and old configuration settings serving no purpose other than to act as a potential attack vector.

If you're not actively using a piece of software, or there's a cron task running that isn't required, get rid of it. If you're using Ansible for your entire infrastructure, this shouldn't be an issue, since you could just bring up new servers to replace old ones when you have major configuration and/or package changes. But if not, consider adding in a 'cleanup' role or at least a task to remove packages that shouldn't be installed, like:

¹²⁶<http://www.sudo.ws/sudoers.man.html>

¹²⁷<http://www.sudo.ws/sudo/sample.sudoers>

```
1 - name: Remove unused packages.  
2   apt: name={{ item }} state=absent purge=yes  
3   with_items:  
4     - apache2  
5     - nano  
6     - mailutils
```

With modules like `yum`, `apt`, `file`, and `mysql_db`, a `state=absent` parameter means Ansible will remove whatever packages, files or databases you want, and will check to make sure this is still the case during future runs of your playbook.

Opening only required ports (and, as a secondary) is something to be done by a simple set of firewall rules. This will be covered fully in the “Use a properly-configured firewall” section, but as an example, don’t leave port 25 open on your server unless your server will be used as an SMTP relay server. Further, make sure the services you have listening on your open ports are configured to only allow access from trusted clients.

Use the principle of least privilege

Users, applications, and processes should only be able to access information (files) and resources (memory, network ports, etc) that are necessary for their operation.

Many of the other basic security measures in this chapter are tangentially related to the principle of least privilege, but user account configuration and file permissions are two main areas that are directly related to the principle.

User account configuration

New user accounts, by default, have fairly limited permissions on a Linux server. They usually have a home folder, over which they have complete control, but any other folder or file on the system is only available for reading, writing, or execution if the folder has group permissions set.

Usually, users can gain access to other files and services through two methods:

1. Adding the user to another group with wider access privileges.
2. Allowing the user to use the `sudo` command to execute commands and access files as root or another user.

For the former method, please read the next section on file permissions to learn how to limit access. For the latter, please make sure you understand the use of sudoers as explained earlier in this chapter.

File permissions

Every Ansible module that deals with files has file ownership and permission parameters available, including `owner`, `group`, and `mode`. Almost every time you handle files (using `copy`, `template`, `file`, etc.), you should explicitly define the correct permissions and ownership. For example, for a configuration file (in our example, the GitLab configuration file) that should *only* be readable or writeable by the root user, set the following:

```
1 - name: Configure the GitLab global configuration file.
2   file:
3     path: /etc/gitlab/gitlab.rb
4     owner: root
5     group: root
6     mode: 0600
```



File permissions may seem a bit obtuse, and sometimes, they may cause headaches. But in reality, using octal numbers to represent file permissions is a helpful way to encapsulate a lot of configuration in three simple numbers. The main thing to remember is the following: for each of the file's `user`, `group` and for `everyone`(each of the three digits), use the following digits to represent permission levels:

```
7: rwx (read/write/execute)
6: rw- (read/write)
5: r-x (read/execute)
4: r-- (read)
3: -wx (write/execute)
2: -w- (write)
1: --x (execute)
0: --- (no permissions)
```

In simpler terms, 4 = read, 2 = write and 1 = execute. Therefore read (4) and write (2) is 6 in the octal representation, and read (4) and execute (1) is 5.

Less experienced admins are overly permissive, setting files and directories to 777 to fix issues they have with their applications. To allow one user (for example, your webserver user, `httpd` or `nginx`) access to a directory or some files, you should consider setting the directory's or files' `group` to the user's group instead of giving permissions to *every user on the system*.

For example, if you have a directory of web application files, the `user` (or in Ansible's terminology, "owner") might be your personal user account, or a deployment or service account on the server. Set the `group` for the files to a group the webserver user is in, and the webserver should now be able to access the files (assuming you have the same permissions set for the user and group, like 664).

Update the OS and installed software

Every year, hundreds of security updates are released for the packages running on your servers, some of them fixing critical bugs. If you don't keep your server software up to date, you will be extremely vulnerable, especially when large exposures like [Heartbleed](#)¹²⁸ are uncovered.

At a minimum, you should schedule regular patch maintenance and package upgrade windows, and make sure you test the upgrades and patches on non-critical servers to make sure your applications work *before* applying the same on your production infrastructure.

With Ansible, since you already have your entire infrastructure described via Ansible inventories, you should be able to use a command like the following to upgrade all installed packages on a RedHat-based system:

```
$ ansible webservers -m yum -a "name=* state=latest"
```

On a Debian-based system, the syntax is similar:

```
$ ansible webservers -m apt -a "upgrade=dist update_cache=yes"
```

The above commands will upgrade *everything* installed on your server. Sometimes, you only want to install security-related updates, or exclude certain packages. In those cases, you need to configure `yum` or `apt` to tell them what to do (edit `/etc/yum.conf` for `yum` on RedHat-based systems, or use `apt-mark hold [package-name]` to keep a certain package at its current version on Debian-based systems).

Automating updates

Fully automated daily or weekly package and system upgrades provide even greater security. Not every environment or corporation can accommodate frequent automated upgrades (especially if your application has been known to break due to past package updates, or relies on custom builds or specific package versions), but if you can do it for your servers, it will increase the depth of your infrastructure's security.



As mentioned in an earlier sidebar, GPG package signature checking is enabled by default for all package-related functionality. It's best to leave GPG checks in place, and import keys from trusted sources when necessary, *especially* when using automatic updates, if you want to prevent potentially insecure packages from being installed on your servers!

¹²⁸<http://heartbleed.com/>

Automating updates for RedHat-based systems

RedHat 6 and later (and modern versions of Fedora, and RedHat derivatives like CentOS) uses a simple cron-based package, `yum-cron`, for automatic updates. For basic, set-and-forget usage, install `yum-cron` and make sure it's started and set to run on system boot:

```
1 - name: Install yum-cron.  
2   yum: name=yum-cron state=installed  
3  
4 - name: Ensure yum-cron is running and enabled on boot.  
5   service: name=yum-cron state=started enabled=yes
```

Further configuration (such as packages to exclude from automatic updates) can be done in the `yum.conf` file, at `/etc/yum.conf`.

Automating updates for Debian-based systems

Debian and its derivatives typically use the `unattended-upgrades` package to configure automatic updates. Like `yum-cron`, it is easy to install, and its configuration is placed in a variety of files within `/etc/apt/apt.conf.d/`:

```
1 - name: Install unattended upgrades package.  
2   apt: name=unattended-upgrades state=installed  
3  
4 - name: Copy unattended-upgrades configuration files in place.  
5   template:  
6     src: ".../templates/{{ item }}.j2"  
7     dest: "/etc/apt/apt.conf.d/{{ item }}"  
8     owner: root  
9     group: root  
10    mode: 0644  
11  with_items:  
12    - 10periodic  
13    - 50unattended-upgrades
```

The template files copied in the second task should look something like the following:

```
1 # File: /etc/apt/apt.conf.d/10periodic
2 APT::Periodic::Update-Package-Lists "1";
3 APT::Periodic::Download-Upgradeable-Packages "1";
4 APT::Periodic::AutocleanInterval "7";
5 APT::Periodic::Unattended-Upgrade "1";
```

This file provides configuration for the `apt` script that runs as part of the unattended upgrades package, and tells `apt` whether to enable unattended upgrades.

```
1 # File: /etc/apt/apt.conf.d/50unattended-upgrades
2 Unattended-Upgrade::Automatic-Reboot "false";
3
4 Unattended-Upgrade::Allowed-Origins {
5     "Ubuntu lucid-security";
6 //     "Ubuntu lucid-updates";
7 };
```

This file provides further configuration for unattended upgrades, like whether to automatically restart the server for package and kernel upgrades that require a reboot (make sure, if you have this set to `false`, that you get notifications or check in on your servers so you know when they'll need a manual reboot!), or what `apt` sources should be checked for updated packages.

Use a properly-configured firewall

If you were building a secure bank vault, you wouldn't want to have a large array of doors and windows that lead into the vault. Rather, you'd build thick reinforced concrete walls, and maybe have one or two locked-down controlled-access doors.

Similarly, you shouldn't close any port that isn't explicitly required to remain open on all your servers—whether in a DMZ in your network or open the the entire Internet. There are dozens of different ways to manage firewalls nowadays, from `iptables` and helpful tools like `ufw` and `firewalld` that help make `iptables` configuration easier, to AWS security groups and other external firewall services.

Ansible includes built-in support for configuring server firewalls with `ufw` (common on newer Debian and Ubuntu distributions) and `firewalld` (common on newer Fedora, RedHat, and CentOS distributions).

Configuring a firewall with `ufw` on Debian or Ubuntu

Below is an entire firewall configuration that will lock down most everything on a Debian or Ubuntu server, allowing traffic only through ports 22 (SSH), 80 (HTTP), and 123 (NTP):

```

1  - name: Configure open ports with ufw.
2    ufw:
3      rule: "{{ item.rule }}"
4      port: "{{ item.port }}"
5      proto: "{{ item.proto }}"
6    with_items:
7      - { rule: 'allow', port: 22, proto: 'tcp' }
8      - { rule: 'allow', port: 80, proto: 'tcp' }
9      - { rule: 'allow', port: 123, proto: 'udp' }
10
11 - name: Configure default incoming/outgoing rules with ufw.
12   ufw:
13     direction: "{{ item.direction }}"
14     policy: "{{ item.policy }}"
15     state: enabled
16   with_items:
17     - { direction: outgoing, policy: allow }
18     - { direction: incoming, policy: deny }

```

If you run a playbook with the above rules, the log into the machine (or use the `ansible` command) and run `sudo ufw status verbose`, you should see the configuration has been updated to the following:

```

$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

```

To	Action	From
--	-----	----
22/tcp	ALLOW IN	Anywhere
80/tcp	ALLOW IN	Anywhere
123/udp	ALLOW IN	Anywhere
22/tcp (v6)	ALLOW IN	Anywhere (v6)
80/tcp (v6)	ALLOW IN	Anywhere (v6)
123/udp (v6)	ALLOW IN	Anywhere (v6)

Configuring a firewall with firewalld on RedHat, Fedora, or CentOS

The same firewall configuration can be done via `firewalld` for RedHat-based systems with similar ease:

```
1 - name: Configure open ports with firewalld.
2   firewalld:
3     state: "{{ item.state }}"
4     port: "{{ item.port }}"
5     zone: external
6     immediate: yes
7     permanent: yes
8   with_items:
9     - { state: 'enabled', port: '22/tcp' }
10    - { state: 'enabled', port: '80/tcp' }
11    - { state: 'enabled', port: '123/udp' }
```



The `immediate` parameter was added in Ansible 1.9, and is required to make the rules effective immediately when the `permanent` parameter is set to yes. If you are running an older version of Ansible, you will need to restart to see your changes, or set `permanent` to no.



Note that `firewalld` doesn't have a simple/explicit command to allow setting default inbound/outbound policies, but you can still use `iptables` commands or manage the firewall via XML files inside `/etc/firewalld`.

If you run `sudo firewall-cmd --zone=external --list-all`, you should see the open ports:

```
$ sudo firewall-cmd --zone=external --list-all
external
  interfaces:
  sources:
  services: ssh
  ports: 123/udp 80/tcp 22/tcp
  masquerade: yes
  forward-ports:
  icmp-blocks:
  rich rules:
```

Some still prefer configuring firewalls with `iptables` (which can be obtuse, but is almost infinitely malleable). This approach is used in the `geerlingguy.firewall` role on Ansible Galaxy, which translates simple variables like `firewall_allowed_tcp_ports` and `firewall_forwarded_tcp_ports` into `iptables` rules, and provides a simple `firewall` service for loading firewall rules.

It doesn't really matter what method you use to control access to your server, but the *principle of least privilege* applies here, as in most security-related discussions: only allow access on ports that

are absolutely necessary for the functionality of your server, and restrict the use of those ports to only the hosts or subnets that need access to the services listening on the ports.



When you're building up a firewall, make sure that you don't accidentally lock down ports or IP addresses that will lock you out of the server entirely, otherwise you'll have to connect to the server through a local terminal connection and start over!

Make sure log files are populated and rotated

Checking server logs is one of the most effective ways to not only see what attacks have taken place on a server, but also to see trends over time and predict high-traffic periods, potential attack vectors, and potential catastrophe.

But logs are completely worthless if they aren't being populated with effective data, aren't being monitored in any way, or are *the cause* of an outage! There are too many root cause analyses that conclude, "the server's disk was full because log file **x** took up all the free space".

I have my eyes on you, 218.78.214.9...

```
1 sshd[19731]: input_userauth_request: invalid user db2admin
2 sshd[19731]: Received disconnect from 218.78.214.9: 11: Bye Bye
3 sshd[19732]: Invalid user jenkins from 218.78.214.9
4 sshd[19733]: input_userauth_request: invalid user jenkins
5 sshd[19733]: Received disconnect from 218.78.214.9: 11: Bye Bye
6 sshd[19734]: Invalid user jenkins from 218.78.214.9
7 sshd[19735]: input_userauth_request: invalid user jenkins
8 sshd[19735]: Received disconnect from 218.78.214.9: 11: Bye Bye
9 sshd[19736]: Invalid user minecraft from 218.78.214.9
10 sshd[19737]: input_userauth_request: invalid user minecraft
11 sshd[19737]: Received disconnect from 218.78.214.9: 11: Bye Bye
```

Only you will know what logs are the most important to monitor on your servers, but some of the most common ones are database slow query logs, webserver access and error logs, authorization logs, and cron logs. You can use tools like the ELK stack (demonstrated in a cookbook in Chapter 8), Munin, Nagios, or even a hosted service to make sure logs are populated and monitored.

Additionally, you should always make sure log files are rotated and archived (according to your infrastructure's needs) using a tool like `logrotate`, and you should have monitoring enabled on log file sizes so you have an early warning when a particular log file or directory grows a bit too large. There are a number of `logrotate` roles on Ansible Galaxy (e.g. [Nick Hammond's `logrotate` role¹²⁹](#)) that make rotation configuration simple.

¹²⁹<https://galaxy.ansible.com/list#/roles/1117>

Monitor logins and block suspect IP addresses

If you've ever set up a new server on the public internet and enabled SSH on port 22 with password-based login enabled, you know how quickly the deluge of script-based logins begins. Many honeypot servers detect hundreds or thousands of such attempts per hours.

Suffice it to say, if you allow password-based login (for SSH, for your web app, or for anything else for that matter), you need to implement some form of monitoring and rate limiting. At a most basic level (and this may be all you need), you should install a tool like [Fail2Ban](#)¹³⁰, which monitors log files and bans IP addresses when it detects too many unsuccessful login attempts in a given period of time.

For the most basic level of security, you should install Fail2Ban and use its default configuration, which will help you protect common application logins. Here's a simple set of tasks you could add to your playbook to install Fail2Ban and make sure it's started on either Debian or RedHat-based distributions:

```
1 - name: Install fail2ban (RedHat).
2   yum: name=fail2ban state=present enablerrepo=epel
3   when: ansible_os_family == 'RedHat'
4
5 - name: Install fail2ban (Debian).
6   apt: name=fail2ban state=present
7   when: ansible_os_family == 'Debian'
8
9 - name: Ensure fail2ban is running and enabled on boot.
10  service: name=fail2ban state=started enabled=yes
```

Fail2Ban configuration is managed in a series of .conf files inside /etc/fail2ban, and most of the simpler configuration can be done by overriding defaults in a local override file, /etc/-fail2ban/jail.local. See the [Fail2Ban manual](#)¹³¹ for more information.

Use SELinux (Security-Enhanced Linux) or AppArmor

SELinux and AppArmor are two different tools which allow you to construct security sandboxes for memory and filesystem access, so, for example, one application can't easily access another application's resources. It's a little like user and group file permissions, but allowing far finer detail—with far more complexity.

You'd be forgiven if you disabled SELinux or AppArmor in the past; both require extra work to set up and configure for your particular servers, especially if you're using less popular distribution

¹³⁰http://www.fail2ban.org/wiki/index.php/Main_Page

¹³¹http://www.fail2ban.org/wiki/index.php/MANUAL_0_8

packages (extremely popular packages like Apache and MySQL are extremely well supported out-of-the-box on most distributions).

However, both of these tools are excellent ways to add *defense in depth* to your infrastructure. You should already have decent configurations for firewalls, file permissions, users and groups, OS updates, etc. But if you're running a web-facing application—especially one that runs on a server with any other applications—it's great to have the extra protection SELinux or AppArmor provides from applications accessing things they shouldn't.

SELinux is usually installed and enabled by default on Fedora, RedHat and CentOS systems, is available and supported on most other Linux platforms, and is widely supported through Ansible modules, so we'll cover SELinux in a bit more depth.

To enable SELinux in targeted mode (which is the most secure mode without being almost impossible to work with), make sure the Python SELinux library is installed, then use Ansible's `selinux` module:

```
- name: Install Python SELinux library.  
  yum: name=libselinux-python state=installed  
  
- Ensure SELinux is enabled in `targeted` mode.  
  selinux: policy=targeted state=enforcing
```

Ansible also has a `seboolean` module that allows setting SELinux booleans. A very common setting for web servers involves setting the `httpd_can_network_connect` boolean:

```
- name: Ensure httpd can connect to the network.  
  seboolean: name=httpd_can_network_connect state=yes persistent=yes
```

The Ansible `file` module also integrates well with SELinux, as you can set the four security context fields for a file or directory, one per parameter:

1. `selevel`
2. `serole`
3. `setype`
4. `seuser`

Building custom SELinux policies for more complex scenarios is out of the scope of this chapter, but you should be able to use tools like `setroubleshoot`, `setroubleshoot-server`, `getsebool`, and `aureport` to see what is being blocked, what booleans are available (and/or enabled currently), and even get helpful notifications when SELinux denies access to an application. Read [Getting started with SELinux¹³²](#) for an excellent and concise introduction.

¹³²<https://major.io/2012/01/25/getting-started-with-selinux/>

Next time you're tempted to disable SELinux instead of fixing the underlying problem, spend a little time seeing if you can keep SELinux's additional layer of protection by setting the correct boolean or configuring your filesystem correctly.

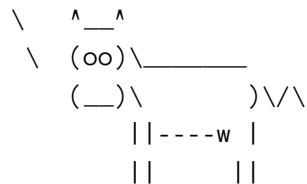
Summary and further reading

This chapter contains a broad overview of some Linux security best practices, and how Ansible can help you conform to them. There is a wealth of good information on the Internet to help you secure your servers, including articles and publications like the following:

- [Linode Library: Linux Security Basics¹³³](#)
- [My First Five Minutes on a Server¹³⁴](#)
- [20 Linux Server Hardening Security Tips¹³⁵](#)
- [Unix and Linux System Administration Handbook¹³⁶](#)

Also, much of the security configuration in this chapter is encapsulated in a simple Ansible role on Ansible Galaxy, which you can use for your own servers: [security role by gearlingguy¹³⁷](#).

```
/ Bad planning on your part does not \
| constitute an emergency on my part. |
\ (Proverb) /
```



¹³³<https://library.linode.com/security/basics>

¹³⁴<http://plusbryan.com/my-first-5-minutes-on-a-server-or-essential-security-for-linux-servers>

¹³⁵<http://www.cyberciti.biz/tips/linux-security.html>

¹³⁶<http://www.admin.com/>

¹³⁷<https://galaxy.ansible.com/list#/roles/1030>

Chapter 11 - Automating Your Automation - Ansible Tower and CI/CD

At this point, you should be able to convert almost any bit of your infrastructure's configuration into Ansible playbooks, roles, and inventories. And before deploying any infrastructure changes, you should test the changes in a non-production environment (just like you would with application releases). Manually running a playbook that configures your entire infrastructure, then making sure it does what you expect, is a good start towards order and stability.

Since all your infrastructure is defined in code, you can start automating all the aspects of infrastructure deployment, and even run unit, functional, and integration tests on your infrastructure, just like you do for your applications.

This section will cover different levels of infrastructure automation and testing, and highlight tools and techniques you can use to automate and streamline infrastructure operations.

Ansible Tower

Throughout this book, all the examples use Ansible's CLI to run playbooks and report back the results. For smaller teams, especially when everyone on the team is well-versed in how to use Ansible, YAML syntax, and follows security best practices with playbooks and variables files, using the CLI can be a sustainable approach.

But for many organizations, there are needs that stretch basic CLI use too far:

- The business needs detailed reporting of infrastructure deployments and failures, especially for audit purposes.
- Team-based infrastructure management requires varying levels of involvement in playbook management, inventory management, and key and password access.
- A thorough visual overview of the current and historical playbook runs and server health helps identify potential issues before they affect the bottom line.
- Playbook scheduling can help ensure infrastructure remains in a known state.

Ansible Tower checks off these items—and many more—and provides a great mechanism for team-based Ansible usage. The product is currently free for teams managing ten or fewer servers (it's

basically an ‘unlimited trial’ mode), and has flexible pricing for teams managing dozens to thousands of servers.

While this book includes a brief overview of Tower, and how you can get started with Tower, it is highly recommended that you read through Ansible, Inc’s extensive [Tower User Guide¹³⁸](#), which includes details this book won’t be covering such as LDAP integration and multiple-team playbook management workflows.

Getting and Installing Ansible Tower

Ansible has a very thorough [Ansible Tower User Guide¹³⁹](#), which details the installation and configuration of Ansible Tower. For the purposes of this chapter, since we just want to download and try out Tower locally, we are going to use Ansible’s official Vagrant box to quickly build an Ansible Tower VM.

Make sure you have [Vagrant¹⁴⁰](#) and [VirtualBox¹⁴¹](#) installed, then create a directory (e.g. tower) and do the following within the directory:

1. `vagrant init tower http://vms.ansible.com/ansible-tower-2.1.4-virtualbox.box`
(Create a new Vagrantfile using the Tower base box from Ansible).
2. `vagrant up` (Build the Tower VM).
3. `vagrant ssh` (Log into the VM, and Tower will display a message with connection information).



The above installation instructions and Vagrant box come from a blog post on Ansible’s official blog, [Ansible Tower and Vagrant¹⁴²](#).

You can now visit the URL provided by the login welcome message (something like `https://10.42.0.42/`), and after confirming a security exception for the Ansible Tower certificate, login with the credentials from step 3.

At this point, you will need to register a free trial license of Ansible Tower, which can be done following the instructions on the screen. The free trial allows you to use all of Tower’s features for up to 10 servers, and is great for experimenting and seeing how Tower fits into your workflow. After you get the license (it’s a block of JSON which you paste into the license field), you should get to Tower’s default dashboard page:

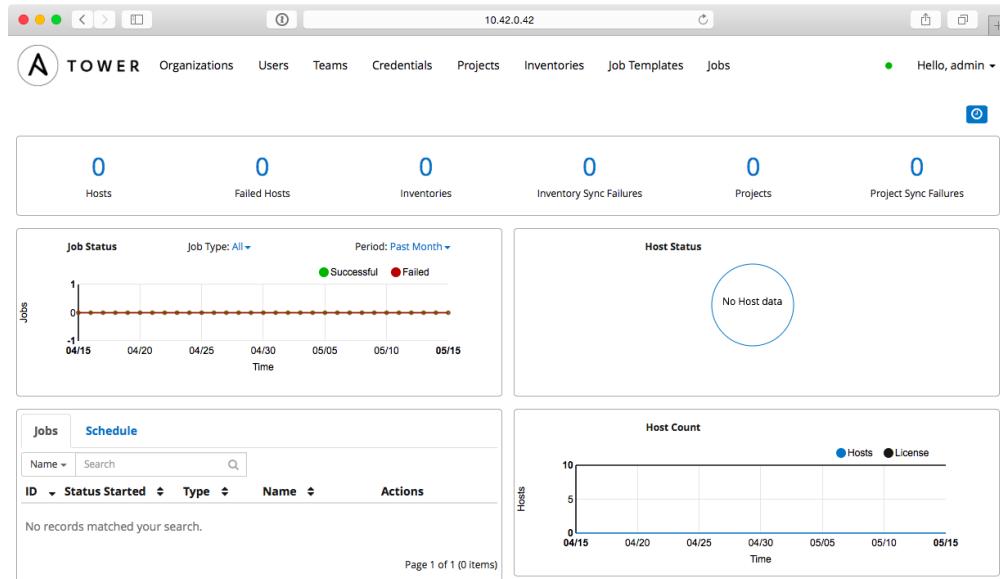
¹³⁸http://releases.ansible.com/ansible-tower/docs/tower_user_guide-latest.pdf

¹³⁹http://releases.ansible.com/ansible-tower/docs/tower_user_guide-latest.pdf

¹⁴⁰<https://www.vagrantup.com/downloads.html>

¹⁴¹<https://www.virtualbox.org/wiki/Downloads>

¹⁴²<http://www.ansible.com/blog/ansible-vagrant>



Ansible Tower's Dashboard

Using Ansible Tower

Ansible Tower is centered around the idea of organizing **Projects** (which run your playbooks via **Jobs**) and **Inventories** (which describe the servers on which your playbooks should be run) inside of **Organizations**. **Organizations** can then be set up with different levels of access based on **Users** and **Credentials** grouped in different **Teams**. It can be a little overwhelming at first, but once you get the initial structure configured, you'll see how powerful and flexible Tower's Project workflow is.

Let's get started with our first project!

The first step is to make sure you have a test playbook you can run using Ansible Tower. Generally, your playbooks should be stored in a source code repository (e.g. Git or Subversion), with Tower configured to check out the latest version of the playbook from the repository and run it. Since we're only going to run a simple example, we will create a playbook in Tower's default projects directory located in `/var/lib/awx/projects`:

1. Log into the Tower VM: `vagrant ssh`
2. Switch to the `awx` user: `sudo su - awx`
3. Go to Tower's default projects directory: `cd /var/lib/awx/projects`
4. Create a new project directory: `mkdir ansible-for-devops && cd ansible-for-devops`
5. Create a new playbook file, `main.yml`, within the new directory, with the following contents:

```
1  ---
2  - hosts: all
3    gather_facts: no
4    connection: local
5
6  tasks:
7    - name: Check the date on the server.
8      command: date
```

Switch back to your web browser and get everything set up to run the test playbook inside Ansible Tower's web UI:

1. Create a new **Organization** called 'Ansible for DevOps'.
2. Add a new User to the Organization, named John Doe, with the username johndoe and password johndoe1234.
3. Create a new **Team** called 'DevOps Engineers', in the 'Ansible for DevOps' Organization.
4. Under the Team's Credentials section, add in SSH credentials by selecting 'Machine' for the Credential type, and setting 'Name' to Vagrant, 'Type' to Machine, 'SSH Username' to vagrant, and 'SSH Password' to vagrant.
5. Under the Team's Projects section, add a new **Project**. Set the 'Name' to Tower Test, 'Organization' to Ansible for DevOps, 'SCM Type' to Manual, and 'Playbook Directory' to ansible-for-devops (Tower automatically detects all folders placed inside /var/lib/awx/projects, but you could also use an alternate Project Base Path if you want to store projects elsewhere).
6. Under the Inventories section, add an **Inventory**. Set the 'Name' to Tower Local, and 'Organization' set to Ansible for DevOps. Once the inventory is saved: 1. Add a 'Group' with the Name localhost. Click on the group once it's saved. 2. Add a 'Host' with the Host Name 127.0.0.1.



New **Credentials** have a somewhat dizzying array of options, and offer login and API key support for a variety of services, like SSH, AWS, Rackspace, VMWare vCenter, and SCM systems. If you can login to a system, Tower likely supports the login mechanism!

Now that we have all the structure for running playbooks configured, we need only create a **Job Template** so we can run the playbook on the localhost and see whether we've succeeded. Click on 'Job Templates', and create a new Job Template with the following configuration:

- Name: Tower Test
- Inventory: Tower Local
- Project: Tower Test
- Playbook: main.yml

- Machine Credential: Vagrant

Save the Job Template, then click the small Rocketship button to start a job using the template. You'll be redirected to a Job status page, which provides live updates of the job status, and then a summary of the playbook run when complete:

The screenshot shows the Ansible Tower interface for a job named "1 - Tower Test". The job status is listed as "successful". The timing section shows the job started at 05/16/15 12:55:41 and finished at 05/16/15 12:55:47, with an elapsed time of 00:00:05. The "Plays" section shows one play named "all" that started at 12:55:46 and took 00:00:00. The "Tasks" section shows one task named "Check the date on the ..." that started at 12:55:46 and took 00:00:00, resulting in a host status of "Changed". The "Events Summary" section on the right shows a host named "127.0.0.1" with 1 completed task, both of which were successful ("OK"). The "Host Summary" section also shows 1 host with 1 OK status.

Tower Test job completed successfully!

You can view the playbook run's standard output in real-time (or review it after the fact) with the 'View standard out' button. You can also stop a running job, delete a job's record, or relaunch a job with the same parameters using the respective buttons on the job's page.

The job's dashboard page is very useful for giving an overview of how many hosts were successful, how many tasks resulted in changes, and the timing of the different parts of the playbook run.

Other Tower Features of Note

In our simple walkthrough above, we used Tower to run a simple playbook on the local server; setting up Tower to run playbooks on real-world infrastructure or other local VMs is just as easy, and the tools Ansible Tower provides are very handy, especially when working in larger team environments.

This book won't walk through the entirety of Ansible Tower's documentation, but a few other simple features you should try out include:

- Setting up scheduled Job runs (especially with the 'Check' option instead of 'Run') for CI/CD.
- Integrating user accounts and Teams with LDAP users and groups for automatic team-based project management.

- Setting different levels of permissions for Users and Teams so certain users can edit certain jobs, others can only run certain jobs, and yet others can only view the results of job runs within an Organization.
- Configuring Ansible Vault credentials so you can easily and automatically use Vault-protected variables in your playbooks.
- Setting up Provisioning Callbacks so newly-provisioned servers can self-provision via a URL per Job Template.
- Surveys, which allow users to add extra information based on a ‘Survey’ of questions per job run.
- Inventory Scripts, which allow you to build inventory dynamically.
- Built-in Munin monitoring (to monitor the Tower server), available with the same admin credentials at [https://\[tower-hostname\]/munin](https://[tower-hostname]/munin).

Ansible Tower continues to improve rapidly, and is one of the best ways to run Ansible Playbooks from a central CI/CD-style server with team-based access and extremely detailed live and historical status reporting.

Tower Alternatives

Ansible Tower is purpose-built for use with Ansible playbooks, but there are many other ways to run playbooks on your servers with a solid workflow. If price is a major concern, and you don’t need all the bells and whistles Tower provides, you can use other popular tools like [Jenkins](#)¹⁴³, [Rundeck](#)¹⁴⁴, or [Go CI](#)¹⁴⁵.

All these tools provide flexibility and security for running Ansible Playbooks, and each one requires a different amount of setup and configuration before it will work well for common usage scenarios. One of the most popular and long-standing CI tools is Jenkins, so we’ll explore how to configure a similar Playbook run in Jenkins next.

Jenkins CI

Jenkins is a Java-based open source continuous integration tool. It was forked from the Hudson project in 2011, but has a long history as a robust build tool for most any software project.

Jenkins is easy to install and configure, with the Java SDK as its only requirement. You can install Jenkins on any modern OS, but for the purposes of this demonstration, we’ll build a local VM using Vagrant, install Jenkins inside the VM using Ansible, then use Jenkins to run an Ansible playbook.

¹⁴³<http://jenkins-ci.org/>

¹⁴⁴<http://rundeck.org/>

¹⁴⁵<http://www.go.cd/>

Build a local Jenkins server with Ansible

Create a new directory for the Jenkins VM named `jenkins`. Inside the directory, create a `Vagrantfile` to describe the machine and the Ansible provisioning to Vagrant, with the following contents:

```
1 VAGRANTFILE_API_VERSION = "2"
2
3 Vagrant.configure(VAGRANTFILE_API_VERSION) do |config|
4   config.vm.box = "geerlingguy/centos7"
5   config.vm.hostname = "jenkins.dev"
6   config.vm.network :private_network, ip: "192.168.76.76"
7   config.ssh.insert_key = false
8
9   config.vm.provider :virtualbox do |vb|
10    vb.customize ["modifyvm", :id, "--memory", "512"]
11  end
12
13 # Ansible provisioning.
14 config.vm.provision "ansible" do |ansible|
15   ansible.playbook = "provision.yml"
16   ansible.sudo = true
17 end
18 end
```

This `Vagrantfile` will create a new VM running CentOS 7, with the IP address `192.168.76.76` and the hostname `jenkins.dev`. Go ahead and add an entry for `192.168.76.76 jenkins.dev` to your hosts file, and then create a new `provision.yml` playbook so Vagrant can run it with Ansible (as described in the `config.vm.provision` block in the `Vagrantfile`). Put the following in the `provision.yml` file:

```
1 ---
2 - hosts: all
3
4 vars:
5   firewall_allowed_tcp_ports:
6     - "22"
7     - "8080"
8   jenkins_plugins:
9     - ansicolor
10
11 roles:
12   - geerlingguy.firewall
13   - geerlingguy.ansible
```

```
14      - geerlingguy.java  
15      - geerlingguy.jenkins
```

This playbook uses a set of roles from Ansible Galaxy to install all the required components for our Jenkins CI server. To make sure you have all the required roles installed on your host machine, add a `requirements.txt` file in the `jenkins` folder, containing all the roles being used in the playbook:

```
1 geerlingguy.firewall  
2 geerlingguy.ansible  
3 geerlingguy.java  
4 geerlingguy.jenkins
```

The `geerlingguy.ansible` role installs Ansible on the VM, so Jenkins can run Ansible playbooks and ad-hoc commands. The `geerlingguy.java` role is a dependency of `geerlingguy.jenkins`, and the `geerlingguy.firewall` role configures a simple firewall to limit access on ports besides 22 (for SSH) and 8080 (Jenkins' default port).

Finally, we tell the `geerlingguy.jenkins` role a set of plugins to install through the `jenkins_plugins` variable; in this case, we just want the `ansicolor` plugin, which gives us full color display in Jenkins' console logs (so our Ansible playbook output is easier to read).



There is an official [Ansible plugin for Jenkins](#)¹⁴⁶, which can be used to run Ansible Ad-Hoc tasks and Playbooks, but as of the writing of this book, the plugin was still in early development stages and is not yet the recommended way to run Ansible playbooks via Jenkins.

To build the VM and run the playbook, do the following (inside the `jenkins` folder):

1. Run `ansible-galaxy install -r requirements.txt` to install the required roles.
2. Run `vagrant up` to build the VM and install and configure Jenkins.

After a few minutes, the provisioning should complete, and you should be able to access Jenkins at `http://jenkins.dev:8080/` (if you configured the hostname in your hosts file).

Create an Ansible playbook on the Jenkins server

It's preferred to keep your playbooks and server configuration in a code repository (e.g. Git or SVN), but for simplicity's sake, this example requires a playbook stored locally on the Jenkins server, similar to the earlier Ansible Tower example.

¹⁴⁶<https://wiki.jenkins-ci.org/display/JENKINS/Ansible+Plugin>

1. Log into the Jenkins VM: `vagrant ssh`
2. Go to the `/opt` directory: `cd /opt`
3. Create a new project directory: `sudo mkdir ansible-for-devops && cd ansible-for-devops`
4. Create a new playbook file, `main.yml`, within the new directory, with the following contents (use `sudo` to create the file, e.g. `sudo vi main.yml`):

```
1 {lang=text}
2 ~~~
3 ---
4 - hosts: 127.0.0.1
5   gather_facts: no
6   connection: local
7
8   tasks:
9     - name: Check the date on the server.
10    command: date
11 ~~~
```

After you create the playbook, you will head over to the Jenkins UI to create a job to run the playbook. But if you want, you can quickly test the playbook while you're logged in, with `ansible-playbook main.yml`.

Create a Jenkins job to run an Ansible Playbook

Now that you have Jenkins running, you can configure a Jenkins job to run a playbook on the local server with Ansible. Visit <http://jenkins.dev:8080/>, and once the page loads, click the ‘New Item’ link to create a new ‘Freestyle project’ with a title ‘`ansible-local-test`’. Click ‘OK’ and when configuring the job, and set the following configuration:

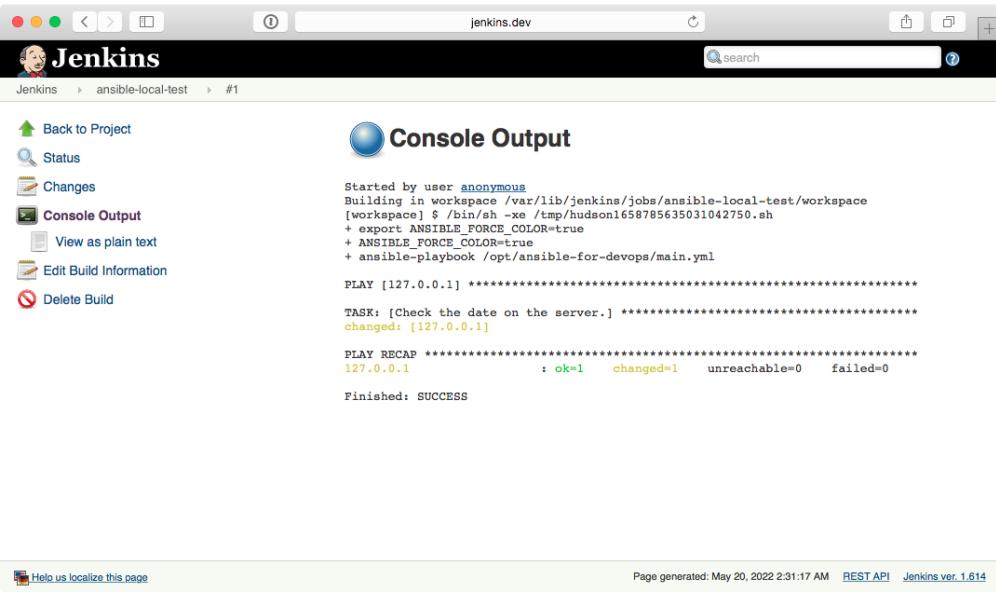
- Under ‘Build Environment’, check the ‘Color ANSI Console Output’ option. This allows Ansible’s helpful colored output to pass through the Jenkins console, so it is easier to read during and after the run.
- Under ‘Build’, click ‘Add Build Step’, then choose ‘Execute shell’. In the ‘Command’ field that appears, add the following code, which will run the local Ansible playbook:

```

1 # Force Ansible to output jobs with color.
2 export ANSIBLE_FORCE_COLOR=true
3
4 # Run the local test playbook.
5 ansible-playbook /opt/ansible-for-devops/main.yml

```

Click ‘Save’ to save the ‘Ansible Local Test’ job, and on the project’s page, click the ‘Build Now’ link to start a build. After a few seconds, you should see a new item in the ‘Build History’ block. Click on the (hopefully) blue circle to the left of ‘#1’, and it will take you to the console output of the job. It should look something like this:



The screenshot shows a Jenkins web interface. In the top navigation bar, the URL is 'jenkins.dev'. Below the header, there's a breadcrumb trail: 'Jenkins > ansible-local-test > #1'. On the left, a sidebar menu includes 'Back to Project', 'Status', 'Changes', 'Console Output' (which is selected and highlighted in blue), 'View as plain text', 'Edit Build Information', and 'Delete Build'. The main content area is titled 'Console Output'. It displays the command-line output of an Ansible playbook run. The output starts with the command 'ansible-playbook /opt/ansible-for-devops/main.yml'. It shows the execution of a task to check the date on the server, which changes from '127.0.0.1'. The play recap summary shows 'ok=1 changed=1 unreachable=0 failed=0'. At the bottom, a message says 'Finished: SUCCESS'. At the very bottom of the page, there's a footer with links to 'Help us localize this page', 'Page generated: May 20, 2022 2:31:17 AM', 'REST API', and 'Jenkins ver. 1.614'.

```

Started by user anonymous
Building in workspace /var/lib/jenkins/jobs/ansible-local-test/workspace
[workspace] $ /bin/sh -xe /tmp/hudson1658785635031042750.sh
+ export ANSIBLE_FORCE_COLOR=true
+ ANSIBLE_FORCE_COLOR=true
+ ansible-playbook /opt/ansible-for-devops/main.yml

PLAY [127.0.0.1] ****
TASK: [Check the date on the server.]
changed: [127.0.0.1]

PLAY RECAP ****
127.0.0.1 : ok=1    changed=1    unreachable=0    failed=0

Finished: SUCCESS

```

Jenkins job completed successfully!

This is an extremely simple example, but hopefully it’s enough to show you how easy it is to get at least some of your baseline CI/CD automation done using a free and open source tool. Most of the more difficult aspects of managing infrastructure through Jenkins surrounds the ability to manage SSH keys, certificates, and other credentials through Jenkins, but there is already plenty of documentation surrounding these things elsewhere online and in Jenkins documentation, so this will be left as an exercise for the reader.

The rest of this chapter focuses on ways to test and debug your playbooks and your infrastructure as a whole, and while many examples use Travis CI or plain command line options, anything you see can be automated with Jenkins jobs!

Unit, Integration, and Functional Testing

When determining how you should test your infrastructure, you need to understand the different kinds of testing, and then determine the kinds of testing on which you should focus more effort.

Unit testing, when applied to applications, is testing that applies to the smallest units of code (usually functions or class methods). In Ansible, unit testing would typically apply to individual playbooks. You could run individual playbooks in an isolated environment, but that's often not worth the effort. What *is* worth your effort is at least checking the playbook syntax, to make sure you didn't just commit a YAML file that will break an entire deployment because of a missing quotation mark, or a whitespace issue!

Integration testing, which is definitely more valuable when it comes to Ansible, is the testing of small groupings of individual units of code, to make sure they work correctly together. Breaking your infrastructure definition into many task-specific roles and playbooks allows you to do this; if you've structured your playbooks so they have no or limited dependencies, you could test each role individually in a fresh virtual machine, before you use the role as part of a full infrastructure deployment.

Functional testing involves the whole shebang. Basically, you set up a complete infrastructure environment, and then run tests against it to make sure **everything** was successfully installed, deployed, and configured. Ansible's own reporting is helpful in this kind of testing (and often, all that is necessary), and there are also external tools that can be used to test infrastructure even more deeply.

It is often possible to perform all the testing you need on your own local workstation, using Virtual Machines (as demonstrated in earlier chapters), using tools like VirtualBox or VMWare. And with most cloud services providing robust control APIs and hourly billing, it's often simple, inexpensive, and just as fast to test directly on cloud instances that mirror your production infrastructure!

We'll begin with some of the simplest tests you can run using Ansible, along with some common debugging techniques, then progress to full-fledged functional testing methods with an automated process.

Debugging and Asserting

For most playbooks, simply testing configuration changes and the result of commands being run as you go is all the testing you need. And having tests run *during your playbook runs* using some of Ansible's built-in utility modules means you have immediate assurance the system is in the state you want.

If at all possible, you should try to bake all simple test cases (e.g. simple comparison and state checks) into your playbooks directly. Ansible has three modules that simplify this process.

The `debug` module

When actively developing an Ansible playbook, or even for historical logging purposes (e.g. if you're running Ansible playbooks using Tower or another CI system), it's often handy to print values of variables or output of certain commands during the playbook run.

For this purpose, Ansible has a debug module, which prints variables or messages during playbook execution.

As an extremely basic example, here are two of the ways I normally use debug while building a playbook:

```
1 - hosts: 127.0.0.1
2   gather_facts: no
3   connection: local
4
5   tasks:
6     - name: Register the output of the 'uptime' command.
7       command: uptime
8       register: system_uptime
9
10    - name: Print the registered output of the 'uptime' command.
11      debug: var=system_uptime.stdout
12
13    - name: Print a simple message if a command resulted in a change.
14      debug: msg="Command resulted in a change!"
15      when: system_uptime.changed
```

Running this playbook gives the following output:

```
$ ansible-playbook debug.yml

PLAY [127.0.0.1] ****
TASK: [Register the output of the 'uptime' command.] ****
changed: [127.0.0.1]

TASK: [Print the registered output of the 'uptime' command.] ****
ok: [127.0.0.1] => {
    "var": {
        "system_uptime.stdout": "15:01  up 15:18, 2 users, load averages: 1.23 1.33 1.42"
    }
}

TASK: [Print a simple message if a command resulted in a change.] ****
ok: [127.0.0.1] => {
    "msg": "Command resulted in a change!"}
```

```
PLAY RECAP ****
127.0.0.1 : ok=3    changed=1    unreachable=0    failed=0
```

Debug messages are helpful when actively debugging a playbook or when you need extra verbosity in the playbook's output, but if you need to perform an explicit test on some variable, or bail out of a playbook for some reason, Ansible provides the `fail` module, and its even simpler cousin, `assert`.

The `fail` and `assert` modules

Both `fail` and `assert`, when triggered, will abort the playbook run, and the only difference is in the simplicity of their usage. To illustrate, let's look at an example:

```
1 - hosts: 127.0.0.1
2   gather_facts: no
3   connection: local
4
5   vars:
6     should_fail_via_fail: true
7     should_fail_via_assert: false
8     should_fail_via_complex_assert: false
9
10  tasks:
11    - name: Fail if conditions warrant a failure.
12      fail: msg="There was an epic failure."
13      when: should_fail_via_fail
14
15    - name: Stop playbook if an assertion isn't validated.
16      assert: that="should_fail_via_assert != true"
17
18    - name: Assertions can have contain conditions.
19      assert:
20        that:
21          - should_fail_via_fail != true
22          - should_fail_via_assert != true
23          - should_fail_via_complex_assert != true
```

Switch the boolean values of `should_fail_via_fail`, `should_fail_via_assert`, and `should_fail_via_complex_assert` to trigger each of the three `fail/assert` tasks, to see how they work.

For most test cases, `debug`, `fail`, and `assert` are all you need to ensure your infrastructure is in the correct state during a playbook run.

Checking syntax and performing dry runs

Two of the simplest checks you should include in an automated playbook testing workflow are `--syntax-check` (which checks the playbook syntax to find simple quoting, formatting, or whitespace errors) and `--check` (which will run your entire playbook in check mode).

Syntax checking is extremely straightforward, and only requires a few seconds for even larger, more complex playbooks with dozens or hundreds of includes. You should include an `ansible-playbook my-playbook.yml --syntax-check` in any kind of CI that you do, and it's good practice to run a syntax check right before you check in playbook changes in your version control system.

Running a playbook in check mode is a little bit more involved, as Ansible will actually run the entire playbook on your live infrastructure, but in a way that results in no changes. Instead, it will mark any tasks that *would've* resulted in a change so you can see what will happen when you *actually* run the playbook later.

This can be helpful for two purposes:

1. To prevent ‘configuration drift’, where a server might have some configuration that’s drifted away from your coded configuration. This could happen due to human intervention (though hopefully you don’t regularly log into your servers and make changes by hand anymore!) or due to other factors. But it’s good to know what configuration is incorrect without necessarily changing it.
2. To make sure changes you make to a playbook that shouldn’t break idempotency *don’t*, in fact, break idempotency. For example, if you’re making a change to build a configuration file differently, but with the same resulting file, running the playbook with `--check` can alert you to the fact that you might accidentally end up changing the file as a result of your change. Time to fix your playbook!

When using `--check` mode, there are sometimes tasks that you still want to run (e.g. command tasks that register variables used in later tasks). You can make sure those tasks are *always* run using the `always_run` option:

```
- name: A task that runs all the time, even in check mode.
  command: mytask --option1 --option2
  register: my_var
  always_run: true
```

Finally, for even more detailed information about what changes would occur, you can add the `--diff` option, and Ansible will output all the line-by-line changes that *would've* been made to your servers. This option will produce a lot of output if check mode makes a lot of changes, so it’s best to use this option conservatively, unless you want to scroll through a lot of text!

In addition to Ansible's robust but simple `--check-syntax` and `--check` modes, you might be interested in also running [Ansible Lint¹⁴⁷](#) on your playbooks. Ansible Lint allows you to check for deprecated syntax or inefficient task structures, and is highly configurable so you can set up the linting to follow the playbook standards you and your team choose.

Automated testing on GitHub using Travis CI

Automated testing using a continuous integration tool like Travis CI (which is free for public projects and integrated very well with GitHub) allows you to run tests against Ansible playbooks or roles you have hosted on GitHub with every commit.

There are four main things that should be tested when building and maintaining Ansible playbooks or roles:

1. The playbook or role's syntax (are all the .yml files formatted correctly?).
2. Whether the playbook or role will run through all the included tasks without failing.
3. The playbook or role's idempotence (if run again, it should not make any changes!).
4. The playbook or role's success (does the role do what it should be doing?).

Ultimately, the most important aspect is #4, because what's the point of a playbook or role if it doesn't do what you want it to do (e.g. start a web server, configure a database, deploy an app, etc.)?

We're going to assume, for the rest of this example, that you're testing a role you have on GitHub, though the example can be applied just as easily for standalone Ansible playbooks.

Setting up a role for testing

Since you're going to need a simple Ansible playbook and inventory file to test your role, you can create both inside a new 'tests' directory in your Ansible role:

```
1 # Directory structure:  
2 my_role/  
3   tests/  
4     test.yml <-- your test playbook  
5     inventory <-- an inventory file to use with the playbook
```

Inside the inventory file, add:

```
1 localhost
```

We just want to tell Ansible to run commands on the local machine (we'll use the `-connection=local` option when running the test playbook).

Inside `test.yml`, add:

¹⁴⁷<https://github.com/willthames/ansible-lint>

```
1 ---
2 - hosts: localhost
3   remote_user: root
4   roles:
5     - github-role-project-name
```

Substitute your own role name for `github-role-project-name` (e.g. `ansible-role-django`). This is a typical Ansible playbook, and we tell Ansible to run the tasks on localhost, with the root user (otherwise, you could run tasks with `travis` if you want, and use `sudo` on certain tasks). You can add `vars`, `vars_files`, etc. if you want, but we'll keep things simple, because for many smaller roles, the role is pre-packaged with sane defaults and all the other info it needs to run.

The next step is to add a `.travis.yml` file to your role so Travis CI will pick it up and use it for testing. Add that file to the root level of your role, and add the following to kick things off:

```
1 ---
2 language: python
3 python: "2.7"
4
5 before_install:
6   # Make sure everything's up to date.
7   - sudo apt-get update -qq
8
9 install:
10  # Install Ansible.
11  - pip install ansible
12
13  # Add ansible.cfg to pick up roles path.
14  - "printf '[defaults]\nroles_path = ../../' > ansible.cfg"
15
16 script:
17  # We'll add some commands to test the role here.
```

The only surprising part here is the `printf` line in the `install` section; I've added that line to create a quick and dirty `ansible.cfg` configuration file Ansible will use to set the `roles_path` one directory up from the current working directory. That way, we can include roles like `github-role-project-name`, or if we use `ansible-galaxy` to download dependencies (as another command in the `install` section), we can just use `- galaxy-role-name-here` to include that role in our `test.yml` playbook.

Now that we have the basic structure, it's time to start adding the commands to test our role.

Testing the role's syntax

This is the easiest test; `ansible-playbook` has a built in command that will check a playbook's syntax (including all the included files and roles), and return `0` if there are no problems, or an error code and some output if there were any syntax issues.

```
1 ansible-playbook -i tests/inventory tests/test.yml --syntax-check
```

Add this as a command in the `script` section of `.travis.yml`:

```
1 script:
2   # Check the role/playbook's syntax.
3   - ansible-playbook -i tests/inventory tests/test.yml --syntax-check
```

If there are any syntax errors, Travis will fail the build and output the errors in the log.

Role success - first run

The next aspect to check is whether the role runs correctly or fails on its first run.

```
1 # Run the role/playbook with ansible-playbook.
2 - "ansible-playbook -i tests/inventory tests/test.yml --connection=local --sudo"
```

This is a basic `ansible-playbook` command, which runs the playbook `test.yml` against the local host, using `--sudo`, and with the inventory file we added to the role's `tests` directory.

Ansible returns a non-zero exit code if the playbook run fails, so Travis will know whether the command succeeded or failed.

Role idempotence

Another important test is the idempotence test—does the role change anything if it runs a second time? It should not, since all tasks you perform via Ansible should be idempotent (ensuring a static/unchanging configuration on subsequent runs with the same settings).

```

1 # Run the role/playbook again, checking to make sure it's idempotent.
2 - >
3   ansible-playbook -i tests/inventory tests/test.yml --connection=local --sudo
4   | grep -q 'changed=0.*failed=0'
5   && (echo 'Idempotence test: pass' && exit 0)
6   || (echo 'Idempotence test: fail' && exit 1)

```

This command runs the exact same command as before, but pipes the results through grep, which checks to make sure ‘changed’ and ‘failed’ both report 0. If there were no changes or failures, the idempotence test passes (and Travis sees the 0 exit and is happy), but if there were any changes or failures, the test fails (and Travis sees the 1 exit and reports a build failure).

Role success - final result

The last thing I check is whether the role actually did what it was supposed to do. If it configured a web server, is the server responding on port 80 or 443 without any errors? If it configured a command line application, does that command line application work when invoked, and do the things it’s supposed to do?

```

1 # Request a page via the web server, to make sure it's running and responds.
2 - "curl http://localhost/"

```

In this example, I’m testing a web server by loading ‘localhost’; curl will exit with a 0 status (and dump the output of the web server’s response) if the server responds with a 200 OK status, or will exit with a non-zero status if the server responds with an error status (like 500) or is unavailable.

Taking this a step further, you could even run a deployed application or service’s own automated tests after ansible is finished with the deployment, thus testing your infrastructure and application in one go—but we’re getting ahead of ourselves here... that’s a topic for later!

Some notes about Travis CI

There are a few things you need to know about Travis CI, especially if you’re testing Ansible, which will rely heavily on the VM environment inside which it is running:

- **Ubuntu 12.04:** As of this writing, the only OS available via Travis CI is Ubuntu 12.04. Most of my roles work with Ubuntu/Debian/RedHat/CentOS, so it’s not an issue for me... but if your roles strictly target a non-Debian-flavored distro, you probably won’t get much mileage out of Travis. (There is an [open issue¹⁴⁸](https://github.com/travis-ci/travis-ci/issues/2046) to get Travis upgraded to Ubuntu 14.04, at least).

¹⁴⁸<https://github.com/travis-ci/travis-ci/issues/2046>

- **Preinstalled packages:** Travis CI comes with a bunch of services installed out of the box, like MySQL, Elasticsearch, Ruby, etc. In the `.travis.yml before_install` section, you may need to do some `apt-get remove --purge [package]` commands and/or other cleanup commands to make sure the VM is fresh for your Ansible role's run.
- **Networking/Disk/Memory:** Travis CI continuously shifts the VM specs you're using, so don't assume you'll have X amount of RAM, disk space, or network capacity. You can add commands like `cat /proc/cpuinfo`, `cat /proc/meminfo`, `free -m`, etc. in the `.travis.yml before_install` section if you need to figure out the resources available in your VM.

See much more information about the VM environment on the [Travis CI Build Environment page¹⁴⁹](#).

Real-world examples

This style of testing is integrated into many of the `geerlingguy.*` roles on Ansible Galaxy; here are a few example roles that use Travis CI integration in the way outlined above:

- <https://github.com/geerlingguy/ansible-role-apache>
- <https://github.com/geerlingguy/ansible-role-gitlab>
- <https://github.com/geerlingguy/ansible-role-mysql>

If you would like to run your tests using a slightly more simplified and more self-contained test running environment, you might be interested in the [rolespec¹⁵⁰](#) project, which formalizes and simplifies much of the code in the Travis CI examples shown above. Your tests will be dependent on another library for test runs, but doing this allows you to run the tests more easily in environments other than Travis CI.

Functional testing using serverspec

[Serverspec¹⁵¹](#) is a tool to help automate server tests using RSpec tests, which use a Ruby-like DSL to ensure your server configuration matches your expectations. In a sense, it's another way of building well-tested infrastructure.

Serverspec tests can be run locally, via SSH, through Docker's APIs, or through other means, without the need for an agent installed on your servers, so it's a lightweight tool for testing your infrastructure (just like Ansible is a lightweight tool for *managing* your infrastructure).

There's a lot of debate over whether well-written Ansible playbooks themselves (especially along with the dry-run `--check` mode) are adequate for well-tested infrastructure, but many teams are more comfortable maintaining infrastructure tests in Serverspec instead (especially if the team is already familiar with how Serverspec and Rspec works!).

¹⁴⁹<http://docs.travis-ci.com/user/ci-environment/>

¹⁵⁰<https://github.com/nickjj/rolespec>

¹⁵¹<http://serverspec.org/>

Consider this: a truly idempotent Ansible playbook is already a great testing tool if it uses Ansible's robust core modules and `fail`, `assert`, `wait_for` and other tests to ensure a specific state for your server. If you use Ansible's `user` module to ensure a given user exists and is in a given group, and run the same playbook with `--check` and get `ok` for that same task, isn't that a good enough test that your server is configured correctly?

This book will not provide a detailed guide for using Serverspec with your Ansible-managed servers, but here are a few resources in case you'd like to use it:

- A brief introduction to server testing with Serverspec¹⁵²
- Testing Ansible Roles with Test Kitchen, Serverspec and RSpec¹⁵³
- Testing infrastructure with serverspec¹⁵⁴

Summary

Tools to help manage, test, and run playbooks regularly and easily, such as Travis CI, Jenkins, and Ansible Tower, also help deliver certainty when applying changes to your infrastructure using Ansible. In addition the information contained in this chapter, read through the [Testing Strategies](#)¹⁵⁵ documentation in Ansible's documentation for a comprehensive overview of infrastructure testing and Ansible.

```
/ The first rule of any technology used \
| in a business is that automation      |
| applied to an efficient operation will|
| magnify the efficiency. The second is   |
| that automation applied to an          |
| inefficient operation will magnify the |
\ inefficiency. (Bill Gates)           /
```

\ ^__^
 \ (oo)_____
 (__)\)\/\
 ||----w |
 || ||

¹⁵²https://www.debian-administration.org/article/703/A_brief_introduction_to_server-testing_with_serverspec

¹⁵³<http://www.slideshare.net/MartinEtmajer/testing-ansible-roles-with-test-kitchen-serverspec-and-rspec-48185017>

¹⁵⁴<http://vincent.bernat.im/en/blog/2014-serverspec-test-infrastructure.html>

¹⁵⁵http://docs.ansible.com/test_strategies.html

Appendix A - Using Ansible on Windows workstations

Ansible works primarily over the SSH protocol, which is supported natively by most every server, workstation, and operating system on the planet, with one exception—Microsoft’s venerable Windows OS.

To use SSH on Windows, you need additional software. But Ansible also requires other utilities and subsystems only present on Linux or other UNIX-like operating systems. This poses a problem for many system administrators who are either forced to use or have chosen to use Windows as their primary OS.

This appendix will guide Windows users through the author’s preferred method of using Ansible on a Windows workstation.



Ansible 1.7 and later can be used to manage Windows hosts (see Ansible’s [Windows Support](#)¹⁵⁶ documentation), but it can’t be run from within Windows natively. You will still need to follow the instructions here to run the Ansible client on a Windows host, if you are stuck on Windows and want to use Ansible to manage other (Windows, Linux, Mac, etc.) hosts.

Prerequisites

Our goal is to have a virtual machine running Linux running on your computer. The easiest way to do this is to download and install Vagrant and VirtualBox (both 100% free!), and then use Vagrant to install Linux, and PuTTY to connect and use Ansible. Here are the links to download these applications:

1. [Vagrant](#)¹⁵⁷
2. [VirtualBox](#)¹⁵⁸
3. [PuTTY](#)¹⁵⁹

Once you’ve installed all three applications, you can use either the command prompt (`cmd`), Windows PowerShell, or a Linux terminal emulator like Cygwin to boot up a basic Linux VM with Vagrant (if you use Cygwin, which is not covered here, you could install its SSH component and use it for SSH, and avoid using PuTTY).

¹⁵⁶http://docs.ansible.com/intro_windows.html

¹⁵⁷<http://www.vagrantup.com/downloads.html>

¹⁵⁸<https://www.virtualbox.org/>

¹⁵⁹<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

Set up an Ubuntu Linux Virtual Machine

Open PowerShell (open the Start Menu or go to the Windows home and type in ‘PowerShell’), and change directory to a place where you will store some metadata about the virtual machine you’re about to boot. I like having a ‘VMs’ folder in my home directory to contain all my virtual machines:

```
# Change directory to your user directory.  
PS > cd C:/Users/[username]  
# Make a 'VMs' directory and cd to it.  
PS > md -Name VMs  
PS > cd VMs  
# Make a 'Ubuntu64' directory and cd to it.  
PS > md -Name ubuntu-precise-64  
PS > cd ubuntu-precise-64
```

Now, use vagrant to create the scaffolding for our new virtual machine:

```
PS > vagrant init precise64 http://files.vagrantup.com/precise64.box
```

Vagrant creates a ‘Vagrantfile’ describing a basic Ubuntu Precise (12.04) 64-bit virtual machine in the current directory, and is now ready for you to run `vagrant up` to download and build the machine. Run `vagrant up`, and wait for the box to be downloaded and installed:

```
PS > vagrant up
```

After a few minutes, the box will be downloaded and a new virtual machine set up inside VirtualBox. Vagrant will boot and configure the machine according to the defaults defined in the Vagrantfile. Once the VM is booted, and you’re back at the command prompt, it’s time to log into the VM.

Log into the Virtual Machine

Use `vagrant ssh-config` to grab the SSH connection details, which you will then enter into PuTTY to connect to the VM.

```
PS > vagrant ssh-config
```

It should show something like:

```
Host default
  Hostname 127.0.0.1
  User vagrant
  Port 2222
  UserKnownHostsFile /dev/null
  StrictHostKeyChecking no
  PasswordAuthentication no
  IdentityFile C:/Users/[username]/.vagrant.d/insecure_private_key
  IdentitiesOnly yes
  LogLevel FATAL
```

The lines we're interested in are the Hostname, User, Port, and IdentityFile.

Launch PuTTY, and enter the connection details:

- **Host Name (or IP address):** 127.0.0.1
- **Port:** 2222

Click Open to connect (you can save the connection details by entering a name in the 'Saved Sessions' field and clicking 'Save' to save the details), and if you receive a Security Alert concerning the server's host key, click 'Yes' to tell PuTTY to trust the host.

PuTTY will ask for login credentials; we'll use the default login for a Vagrant box (vagrant for both the username and password):

```
login as: vagrant
vagrant@127.0.0.1's password: vagrant
```

You should now be connected to the virtual machine, and see the message of the day:

```
Welcome to Ubuntu 12.04 LTS (GN/Linux 3.2.0-23-generic x86_64)
```

```
* Documentation: https://help.ubuntu.com/
Welcome to your Vagrant-built virtual machine.
Last login: <date> from <IP address>
vagrant@precise64:~$
```

If you see this prompt, you're logged in, and you can start administering the VM. The next (and final) step is to install Ansible.



This example uses PuTTY to log into the VM, but other applications like [Cygwin¹⁶⁰](#) or [Git for Windows¹⁶¹](#) work just as well, and may be easier to use. Since these alternatives have built-in SSH support, you don't need to do any extra connection configuration, or even launch the apps manually; just `cd` to the same location as the Vagrantfile, and enter `vagrant ssh!`

Install Ansible

Before installing Ansible, make sure your package list is up to date by updating apt-get:

```
$ sudo apt-get update
```

Ansible can be installed in a variety of ways, but the easiest is to use pip, a simple Python package manager. Python should already be installed on the system, but pip may not be, so let's install it, along with Python's development header files (which are in the `python-dev` package).

```
$ sudo apt-get install -y python-pip python-dev
```

After the installation is complete, installing Ansible is simple:

```
$ sudo pip install ansible
```

After Ansible and all its dependencies are downloaded and installed, make sure Ansible is running and working:

```
$ ansible --version
ansible 1.9.2
```



Upgrading Ansible is also easy with pip: Run `sudo pip install --upgrade ansible` to get the latest version.

¹⁶⁰<http://cygwin.com/install.html>

¹⁶¹<http://git-scm.com/download/win>

Summary

You should now have Ansible installed within a virtual machine running on your Windows workstation. You can control the virtual machine with Vagrant (`cd` to the location of the `Vagrantfile`), using `up` to boot or wake the VM, `halt` to shut down the VM, or `suspend` to sleep the VM. You can log into the VM using PuTTY and manually entering a username and password, or using Cygwin or Git's Windows shell and the `vagrant ssh` command.

Use Ansible from within the virtual machine just as you would on a Linux or Mac workstation directly. If you need to share files between your Windows environment and the VM, Vagrant conveniently maps `/vagrant` on the VM to the same folder where your `Vagrantfile` is located. You can also connect between the two via other methods (SSH, SMB, SFTP etc.) if you so desire.

Finally, there are also other ways to ‘hack’ Ansible into running natively within Windows (without a Linux VM), such as the `ansible-babun-bootstrap`¹⁶², but I still recommend running everything within a Linux VM as performance will be optimal and the number of environment-related problems you encounter will be greatly reduced!

¹⁶²<https://github.com/jonathanhle/ansible-babun-bootstrap>

Appendix B - Ansible Best Practices and Conventions

Ansible is a simple, flexible tool, and allows for a variety of organization methods and configuration syntaxes. You might like to have many tasks in one main file, or few tasks in many files. You might prefer defining variables in group variable files, host variable files, inventories, or elsewhere, or you might try to find ways of avoiding variables in inventories altogether.

There are few *universal* best practices in Ansible, but this appendix contains many helpful suggestions for organizing playbooks, writing tasks, using roles, and otherwise build infrastructure with Ansible.

In addition to this appendix (which contains mostly observations from the author's own daily use of Ansible), please read through the official [Ansible Best Practices¹⁶³](#) guide, which contains a wealth of hard-earned knowledge.

Playbook Organization

As playbooks are Ansible's bread and butter, it's important to organize them in a logical manner, so you can easily write, debug, and maintain them.

Write comments and use name liberally

Many tasks you write will be fairly obvious when you write them, but less so six months later when you are making changes. Just like application code, Ansible playbooks should be documented, at least minimally, so you can spend less time familiarizing yourself with what a particular task is supposed to do, and more time fixing problems or extending your playbooks.

In YAML, you can write a comment by starting a line with a hash (#). If your comment spans multiple lines, start each line with #.

It's also a good idea to use a name for every task you write, besides the most trivial. If you're using the git module to check out a specific tag, use a name to indicate what repository you're using, why a tag instead of a commit hash, etc. This way, whenever your playbook is run, you'll see the comment you wrote and be assured what's going on.

¹⁶³http://docs.ansible.com/playbooks_best_practices.html

```
- hosts: all

  tasks:

    # This task takes up to five minutes and is required so we will have
    # access to the images used in our application.
    - name: Copy the entire file repository to the application.
      copy:
        src: ...
```

This advice assumes, of course, that your comments actually indicate what's happening in your playbooks! Generally, I use full sentences with a period for all comments and names, but if you'd like to use a slightly different style, that's not an issue. Just try to be consistent, and remember that *bad comments are worse than no comments at all*.

Include related variables and tasks

If you find yourself writing a playbook that's over 50-100 lines and configures three or four different applications or services, it may help to separate each group of tasks into a separate file, and use `include` to place them in a playbook.

Additionally, variables are usually better left in their own file and included using `vars_files` rather than defined inline with a playbook.

```
- hosts: all

  vars_files:
    - vars/main.yml

  handlers:
    - include: handlers/handlers.yml

  tasks:
    - include: tasks/init.yml
    - include: tasks/database.yml
    - include: tasks/app.yml
```

Using a more hierarchical model like this allows you to see what your playbook is doing at a higher level, and also lets you manage each portion of a configuration or deployment separately. I generally split tasks into separate files once I reach 15-20 tasks in a given file.

Use Roles to bundle logical groupings of configuration

Along the same lines as using included files to better organize your playbooks and separate bits of configuration logically, Ansible roles can supercharge your ability to manage infrastructure well.

Using loosely-coupled roles to configure individual components of your servers (like databases, application deployments, the networking stack, monitoring packages, etc.) allows you to write configuration once, and use it on all your servers, regardless of their role.

Consider that you will probably configure something like NTP (Network Time Protocol) on every single server you manage, or at a minimum, set a timezone for the server. Instead of adding two or three tasks to every playbook you manage, set up a role (maybe call it `time` or `ntp`) that does this configuration, and use a few variables to allow different groups of servers to have customized settings.

Additionally, if you learn to build roles in a generic fashion, and for multiple platforms, you could even share it on Ansible Galaxy so others can use the role and help you make it more robust and efficient!

Use role defaults and vars correctly

Set all role default variables that should and likely will be overridden inside `defaults/main.yml`, and set variables that are useful to store as variables, but will likely never need to be overridden in `vars/main.yml`.

If you have a variable that needs to be overridden, but you need to include it in a platform-specific `vars` file (e.g. one `vars` file for Debian, one for RedHat), then create the variable in `vars/[file].yml` as `__varname`, and use `set_fact` to set the variable if the variable `varname` is not defined. This way playbooks using your role can still override one of these variables.

YAML Conventions and Best Practices

YAML is a human-readable, machine-parseable syntax that allows for almost any list, map, or array structure to be described using a few basic conventions, so it is a great fit for a configuration management tool. Consider the following method of defining a list (or ‘collection’) of widgets:

```
widget:  
  - foo  
  - bar  
  - fizz
```

This would translate into Python (using the PyYAML library employed by Ansible) as the following:

```
translated_yaml = {'widget': ['foo', 'bar', 'fizz']}
```

And what about a structured list/map in YAML?

```
widget:  
  foo: 12  
  bar: 13
```

The Python that would result:

```
translated_yaml = {'widget': {'foo': 12, 'bar': 13}}
```

A few things to note with both of the above examples:

- YAML will try to determine the type of an item automatically. So `foo` in the first example would be translated as a string, `true` or `false` would be a boolean, and `123` would be an integer. You can read the official documentation for further insight, but for our purposes, realize you can minimize surprises by declaring strings with quotes ('' or "").
- Whitespace matters! YAML uses spaces (literal space characters—*not* tabs) to define structure (mappings, array lists, etc.), so set your editor to use spaces for tabs. You can technically use either a tab or a space to delimit parameters (like `apt: name=foo state=installed`—you can use either a tab or a space between parameters), but it's generally preferred to use spaces everywhere, to minimize errors and display irregularities across editors and platforms.
- YAML syntax is robust and well-documented. Read through the official [YAML Specification¹⁶⁴](#) and/or the [PyYAML Documentation¹⁶⁵](#) to dig deeper.

YAML for Ansible tasks

Consider the following task:

```
- name: Install foo.  
  apt: name=foo state=installed
```

All well and good, right? Well, as you get deeper into Ansible and start defining more complex configuration, you might start seeing tasks like the following:

¹⁶⁴<http://www.yaml.org/spec/1.2/spec.html>

¹⁶⁵<http://pyyaml.org/wiki/PyYAMLDocumentation>

```
- name: Copy Phergie shell script into place.  
  template: src=templates/phergie.sh.j2 dest=/opt/phergie.sh owner={{ phergie_user }} group={{ phergie_user }} mode=755
```

The one-line syntax (which uses Ansible-specific `key=value` shorthand for defining parameters) has some positive attributes:

- Simpler tasks (like installations and copies) are compact and readable (`apt: name=apache2 state=installed` is just about as simple as `apt-get install -y apache2`; in this way, an Ansible playbook feels very much like a shell script).
- Playbooks are more compact, and more configuration can be displayed on one screen.
- Ansible's official documentation follows this format, as do many existing roles and playbooks.

However, as highlighted in the above example, there are a few issues with this `key=value` syntax:

- Smaller monitors, terminal windows, and source control applications will either wrap or hide part of the task line.
- Diff viewers and source control systems generally don't highlight intra-line differences as well as full line changes.
- Variables and parameters are converted to strings, which may or may not be desired.

Ansible's shorthand syntax can be troublesome for complicated playbooks and roles, but luckily there are other ways you can write tasks which are better for narrower displays, version control software and diffing.

Three ways to format Ansible tasks

The following methods are most often used to define Ansible tasks in playbooks:

Shorthand/one-line (`key=value`)

Ansible's shorthand syntax uses `key=value` parameters after the name of a module as a key:

```
- name: Install Nginx.  
  yum: name=nginx state=installed
```

For any situation where an equivalent shell command would roughly match what I'm writing in the YAML, I prefer this method, since it's immediately obvious what's happening, and it's highly unlikely any of the parameters (like `state=installed`) will change frequently during development.

Ansible's official documentation generally uses this syntax, so it maps nicely to examples you'll find from Ansible, Inc. and many other sources.

Structured map/multi-line (`key:value`)

You can define a structured map of parameters (using `key: value`, with each parameter on its own line) for a task:

```
- name: Copy Phergie shell script into place.
  template:
    src: "templates/phergie.sh.j2"
    dest: "/home/{{ phergie_user }}/phergie.sh"
    owner: "{{ phergie_user }}"
    group: "{{ phergie_user }}"
    mode: 0755
```

A few notes on this syntax:

- The structure is all valid YAML, and functions similarly to Ansible's shorthand syntax.
- Strings, booleans, integers, octals, etc. are all preserved (instead of being converted to strings).
- Each parameter **must** be on its own line, so you can't chain together mode: 0755, owner: root, user: root to save space.
- YAML syntax highlighting (if you have an editor that supports it) works slightly better for this format than key=value, since each key will be highlighted, and values will be displayed as constants, strings, etc.

Folded scalars/multi-line (>)

You can also use the > character to break up Ansible's shorthand key=value syntax over multiple lines.

```
- name: Copy Phergie shell script into place.
  template: >
    src=templates/phergie.sh.j2
    dest=/home/{{ phergie_user }}/phergie.sh
    owner={{ phergie_user }} group={{ phergie_user }} mode=755
```

In YAML, the > character denotes a ***folded scalar***, where every line that follows (as long as it's indented further than the line with the >) will be joined with the line above by a space. So the above YAML and the earlier template example will function exactly the same.

This syntax allows arbitrary splitting of lines on parameters, but it does not preserve value types (0775 would be converted to a string, for example).

While this syntax is often seen in the wild, I don't recommend it except for certain situations, like tasks using the command and shell modules with extra options:

```
- name: Install Drupal.
  command: >
    drush si -y
    --site-name="{{ drupal_site_name }}"
    --account-name=admin
    --account-pass={{ drupal_admin_pass }}
    --db-url=mysql://root@localhost/{{ domain }}
    chdir={{ drupal_core_path }}
    creates={{ drupal_core_path }}/sites/default/settings.php
```

If you can find a way to run a command without having to use `creates` and `chdir`, or very long commands (which are arguably unreadable either in single *or* multiline format!), it's better to do that instead of this monstrosity.

Sometimes, though, the above is as good as you can do to keep unwieldy tasks sane.

Using | to format multiline variables

In addition to using `>` to join multiple lines using spaces, YAML allows the use of `|` (pipe) to define literal scalars, so you can define strings with newlines preserved.

For example:

```
1 extra_lines: |
2   first line
3   second line
4   third line
```

Would be translated to a block of text with newlines intact:

```
1 first line
2 second line
3 third line
```

Using a folded scalar (`>`) would concatenate the lines, which might not be desirable. For example:

```
1 extra_lines: >
2   first line
3   second line
4   third line
```

Would be translated to a single string with no newlines:

```
1 first line second line third line
```

Using ansible-playbook

Generally, running playbooks from your own computer or a central playbook runner is preferable to running Ansible playbooks locally (using `--connection=local`), since you can avoid installing Ansible and all its dependencies on the system you're provisioning. Because of Ansible's optimized use of SSH for connecting to remote machines, there is usually minimal difference in performance running Ansible locally or from a remote workstation (barring network flakiness or a high-latency connection).

Use Ansible Tower

If you are able to use Ansible Tower to run your playbooks, this is even better, as you'll have a central server running Ansible playbooks, logging output, compiling statistics, and even allowing a team to work together to build servers and deploy applications in one place.

Specify --forks for playbooks running on > 5 servers

If you are running a playbook on a large number of servers, consider increasing the number of `forks` Ansible uses to run tasks simultaneously. The default, 5, means Ansible will only run a given task on 5 servers at a time. Consider increasing this to 10, 15, or however many connections your local workstation and ISP can handle—this can dramatically reduce the amount of time it takes a playbook to run.

You can also use Ansible's configuration file to set the default `--forks` value for all playbook runs, instead of specifying it on the command line.

Use Ansible's Configuration file

Ansible's main configuration file, in `/etc/ansible/ansible.cfg`, can contain a wealth of optimizations and customizations that help you run playbooks and ad-hoc tasks more easily, faster, or with better output than stock Ansible provides.

Read through the official documentation's [Ansible Configuration File¹⁶⁶](#) page for details on options you can customize in `ansible.cfg`.

¹⁶⁶http://docs.ansible.com/intro_configuration.html

Summary

One of Ansible's strengths is its flexibility; there are often multiple 'right' ways of accomplishing your goals. I have chosen to use the methods I outlined above as they have proven to help me write and maintain a variety of playbooks and roles with minimal headaches.

It's perfectly acceptable to try a different approach; as with most programming and technical things, being *consistent* is more important than following a particular set of rules, especially if that set of rules isn't universally agreed upon. Consistency is especially important when you're not working solo—if every team member used Ansible in a different way, it would become difficult to share work very quickly!

Changelog

This log will track changes between releases of the book. Until version 1.0, each release number will correlate to the amount complete, so ‘Version 0.75’ equals 75% complete. After the final, complete book, major version numbers will track editions.

Hopefully these notes will help readers figure out what’s changed since the last time they’ve downloaded the book.

Current version

- Added example of zero-downtime deployments with HAProxy to chapter 9.
- Completed remaining sections in chapter 9.

Version 0.99 (2015-07-19)

- Incorporated editor’s changes into chapters 5 and 6.
- Added --check and --check-syntax information to chapter 11.
- Added information about rolespec in chapter 11.
- Fixed missing files in book’s GitHub repository Node.js role example (thanks to @geoand!).
- Fixed simple Node.js app server example playbook in chapter 4 (thanks to @erimar77!).
- Fixed 1ineinfile task regex syntax in chapter 4 (thanks to @erimar77!).
- Clarified EPEL requirements/installation for Enterprise Linux systems in chapter 1 (thanks to @michel_slm!).
- Fixed a broken configuration item in chapter 4 playbook example.

Version 0.97 (2015-06-10)

- Incorporated editor’s changes into chapter 4.
- Added dynamic inventory examples in chapter 7.
- Corrected a few other grammatical flaws in all chapters prior to chapter 4.
- Added notes about getting a Python environment configured for barebones containers/-CoreOS in chapter 8 (thanks to @andypost!).
- Mentioned a way to bootstrap Ansible on Windows with Babun in appendix a (thanks to @jonathanhle!).
- Added section on custom dynamic inventory in chapter 7, as well as code examples in the book’s GitHub repository.

Version 0.95 (2015-05-26)

- Added Jenkins CI installation and usage guide in chapter 11.
- Added section on `debug`, `fail` and `assert` in chapter 11.
- Updated a few best practices and otherwise completed appendix b.
- Removed appendix c (on Jinja2 and Ansible); will consider adding back in post-launch.

Version 0.94 (2015-05-16)

- Added information about Capistrano and blue-green deployments in chapter 9.
- Reorganized chapter 9 with an eye towards a 1.0 release.
- Merged chapter 12 into chapter 11 with an eye towards a 1.0 release.
- Fixed `vagrant init` command in chapter 2 (thanks to Ned Schumann!).
- Completed ‘Delegation, Local Actions, and Pauses’ section in chapter 5.
- Completed DigitalOcean dynamic inventory example in chapter 7.
- Fixed CentOS 6 vs 7 nomenclature in chapters 2 and 3 (thanks to @39digits and @aazon!).
- Completed Ansible Tower installation guide in chapter 11.
- Completed Ansible Tower usage guide and alternatives in chapter 11.

Version 0.92 (2015-04-09)

- Update Ansible project ‘stars’ count on GitHub in the introduction.
- Added zero-downtime multi-server deployment example to chapter 9.
- Removed frequent use of the filler word ‘simply’ (thanks to a reader’s suggestion!).
- Fixed language around ‘plays’ vs. ‘tasks’ in chapters 4, 5, and 6 (thanks to André!).
- Fixed ad-hoc Django installation in chapter 3 (thanks to @wimvandijck!).

Version 0.90 (2015-03-16)

- Tweaked `requirements.txt` explanation in chapter 8.
- Tweaked formatting of GlusterFS cookbook in chapter 6.
- Fixed GlusterFS example ports and mount task in chapter 8.
- Fixed some examples in chapter 4 to ensure apt repositories update cache.
- Fixed some typos in chapter 8 (thanks to Juan Martinez!).
- Updated Ansible installation instructions for Debian/Ubuntu in chapter 1.
- Corrected use of `yum` module in `fail2ban` example in chapter 10 (thanks to @lekum!).
- Fixed references to `ansible.cfg` config file in appendix b (thanks to @lekum!).

- Fixed DigitalOcean provisioning playbook in chapter 8 (thanks to @jonathanhle!).
- Adjusted DigitalOcean dynamic inventory example in chapter 7.
- Rewrote completely nonsensical sentence in chapter 7 (thanks to @dan_bohea!).
- Fixed some errors throughout the first few chapters (thanks to nesfel!).
- Fixed a couple errors in chapters 2 and 4 (thanks to Barry McClendon!).

Version 0.89 (2015-02-26)

- Completed first deployment example for Rails app in chapter 9.
- Added notes on role requirements.txt and requirements.yml options in chapter 6.
- Tweaked language and cleaned up examples for roles in chapter 6.
- Added GlusterFS cookbook to chapter 6.

Version 0.88 (2015-02-13)

- Fixed two errors in chapter 7 (thanks to Jonathan Le / @jonathanhle!)
- Wrote introduction to chapter 9.
- Wrote first deployment example for Rails app in chapter 9.

Version 0.87 (2015-02-01)

- Cleaned up Docker examples in chapter 8.
- Fixed a typo in chapter 3 (thanks to Jonathan Le / @jonathanhle!)
- Added section on configuring firewalls with ufw and firewalld in chapter 10.
- Updated Apache Solr version in chapter 4 example.
- Fixed APC uploadprogress task in Drupal example in chapter 4.
- Added section on installing and configuring Fail2Ban in chapter 10.
- Added suggestion for setting ANSIBLE_HOSTS environment variable in chapter 3 (thanks to Jason Baker / @diermakeralch!).
- Added section on SELinux and AppArmor in chapter 10.
- Completed chapter 10.

Version 0.84 (2015-01-27)

- Added Docker introduction and cookbooks in chapter 8.

Version 0.81 (2015-01-11)

- Fixed Vagrantfile examples to work with Vagrant 1.7.x.
- Added local Mac configuration example in chapter 8.
- Used `name` instead of `pkg` for packaging modules as per updated Ansible style guide.
- Incorporated editorial changes for introduction, chapter 1, chapter 2, and chapter 3.
- Fixed references to Vagrant Cloud/HashiCorp's Atlas.
- Finished almost all the rest of chapter 5.

Version 0.75 (2014-12-23)

- Fixed code formatting in examples in chapter 8.
- Added YAML | multiline variable delimiter example to appendix b.
- Edited and updated examples and guide for HA Infrastructure in chapter 8.
- Completed the ELK and Logstash Forwarder examples in chapter 8.
- Started on the Mac provisioning example in chapter 8.

Version 0.73 (2014-12-09)

- Added `wait_for` to DigitalOcean example in chapter 7.
- Completed Highly-Available Infrastructure cookbook in chapter 8.
- Began work on ELK log monitoring cookbook in chapter 8.
- Fixed a few typos in chapters 5 and 6 (thanks to George Boobyer / @ibluebag!).
- Incorporated edits in preface from technical editor.

Version 0.71 (2014-11-27)

- Added Highly-Available Infrastructure cookbook to chapter 8.
- Updated screenshots throughout the book.
- Began incorporating changes from copy editor (more to come!).

Version 0.70 (2014-11-16)

- Converted Testing/CI section into its own chapter.
- Added cowsay to chapter 12.
- Removed glossary (and pointed readers directly to Ansible's very helpful glossary).
- Added missing link in chapter 7.

- Converted chapter 8 from “Ansible Modules” to “Ansible Cookbooks” due to reader interest.
- Cleaned up Vagrantfile in chapter 3, as well as throughout `ansible-for-devops` git repo.
- Added “Web Architecture Example” example to `ansible-for-devops` git repo.
- Built structure of chapter 8 (“Ansible Cookbooks”).
- Added cowsay to chapter 8.
- Added information about `add_host` and `group_by` to chapter 7.
- Reworked sections in chapter 12 and fixed a few problems.

Version 0.64 (2014-10-24)

- Added Server Check.in architecture diagram (chapter 7).
- Wrote about `host_vars`, `group_vars`, and dynamic inventory (chapter 7).
- Added Digital Ocean provisioning and dynamic inventory walkthrough (chapter 7).

Version 0.62 (2014-10-07)

- Wrote a good deal of chapter 7 (Inventories).
- Cleaned up code examples to follow updated best practices in appendix b.
- Updated installation instructions to use Ansible’s official PPA for Ubuntu (thanks to Rohit Bhute!).

Version 0.60 (2014-09-30)

- Wrote most of appendix b (Best Practices).
- Updated definition of idempotence in chapter 1.
- Fixed a few LeanPub-related code formatting issues.
- Many grammar fixes throughout the book (thanks to Jon Forrest!).
- Some spelling and ad-hoc command fixes (thanks to Hugo Posca!).
- Had a baby (thus the dearth of updates from 8/1-10/1 :-).
- Wrote introduction and basic structure of chapter 11 (Ansible Tower).

Version 0.58 (2014-08-01)

- Even more sections on variables in chapter 5 (almost finished!).
- Fixed a few old Ansible and Drupal version references.
- Added a playbook include tag example in chapter 6.
- Completed first draft of chapter 6.
- Fixed broken handler in chapter 4’s Tomcat handler (thanks to Joel Shprentz!).
- Fixed a missing closing quotation in chapter 3 example (thanks to Jonathan Nakatsui!).

Version 0.56 (2014-07-20)

- Filled in many more sections on variables in chapter 5.
- Some editing in chapter 6.
- Side work on some supplemental material for a potential chapter on Docker.

Version 0.54 (2014-07-02)

- Finished roles section in chapter 6.
- Fixed a few code examples for better style in chapter 4.
- Fixed references to official code repository in chapters 4 and 6.

Version 0.53 (2014-06-28)

- Added note about [Windows Support¹⁶⁷](#) in appendix a.
- Wrote large portion of roles section in chapter 6.

Version 0.52 (2014-06-14)

- Adjusted some code listings to make more readable line breaks.
- Added section on Ansible testing with Travis CI in chapter 12.
- Expanded mention of Ansible's excellent documentation in introduction.
- Greatly expanded security coverage in chapter 10.
- Added link to security role on Ansible Galaxy in chapter 10.

Version 0.50 (2014-05-05)

- Wrote includes section in chapter 6.
- Added links to code repository examples in chapters 4 and 6.
- Fixed broken internal links.
- Fixed typos in chapter 10.
- Added note about --force-handlers (new in Ansible 1.6) in chapter 4.
- Use Ansible's apache2_module module for LAMP example in chapter 4.
- Moved Jinja2 chapter to appendix c.
- Removed 'Variables' chapter (variables will be covered in-depth elsewhere).

¹⁶⁷http://docs.ansible.com/intro_windows.html

- Added Appendix B - Ansible Best Practices and Conventions.
- Started tagging code in [Ansible for DevOps GitHub repository](#)¹⁶⁸ to match manuscript version (starting with this version, 0.50).
- Fixed various layout issues.

Version 0.49 (2014-04-24)

- Completed history of SSH in chapter 10.
- Clarified definition of the word ‘DevOps’ in chapter 1.
- Added section “Testing Ansible Playbooks” in chapter 14.
- Added links to [Ansible for DevOps GitHub repository](#)¹⁶⁹ in the introduction and chapter 4.

Version 0.47 (2014-04-13)

- Added Apache Solr example in chapter 4.
- Updated VM diagrams in chapter 4.
- Added information about `ansible-playbook` command in chapter 4 (thanks to a reader’s suggestion!).
- Clarified code example in preface.

Version 0.44 (2014-04-04)

- Expanded chapter 10 (security).
- Fixed formatting issues in Warning/Info/Tip asides.
- Fixed formatting of some code examples to prevent line wrapping.
- Added section on Ansible Galaxy in chapter 6.
- Updated installation section in chapter 1 with simplified install processes.
- Added warnings concerning faster SSH in Ansible 1.5+ (thanks to [@LeeVanSteerthem](#)¹⁷⁰).

Version 0.42 (2014-03-25)

- Added history of SSH section.
- Expanded chapter 10 (security).
- Many small spelling and grammar mistakes corrected.
- Fixed formatting of info/warning/tip asides.

¹⁶⁸<https://github.com/geerlingguy/ansible-for-devops>

¹⁶⁹<https://github.com/geerlingguy/ansible-for-devops>

¹⁷⁰<https://twitter.com/LeeVanSteerthem>

Version 0.38 (2014-03-11)

- Added Appendix A - Using Ansible on Windows workstations (thanks to a reader's suggestion!).
- Updated chapter 1 to include a reference to appendix a.
- Clarified and expanded installation instructions for Mac and Linux in chapter 1.
- Added chapter 10 - Server Security and Ansible
- Updated chapter 1 to include a reference to chapter 10.
- Added notes to a few more areas of the book (random).

Version 0.35 (2014-02-25)

- Added this changelog.
- Split out roles and playbook organization into its own chapter.
- Expanded 'Environment Variables' section in chapter 5.
- Expanded 'Variables' section in chapter 5.
- MORE COWBELL! (Cowsay motivational quotes at the end of every completed chapter).
- Fixed NTP installation examples in chapter 2 (thanks to a reader's suggestion!).

Version 0.33 (2014-02-20)

- Initial published release, up to chapter 4, part of chapter 5.