



**INSPEC**  
BY **CHEF**™

# Compliance Automation with InSpec

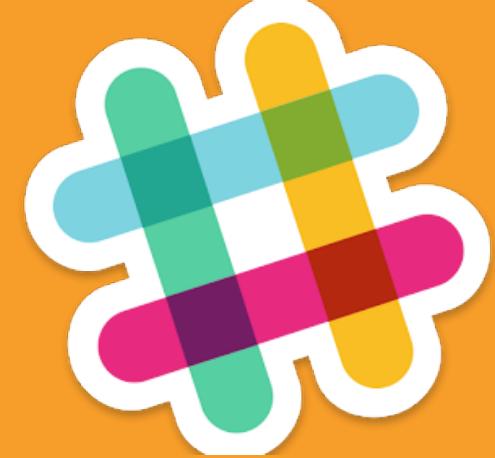
Nathen Harvey - @nathenharvey



# Learning Lab

# Join Slack Team & Channel

- <http://community-slack.chef.io>
- #CHANNEL-NAME



#CHANNEL-NAME

# Find your IP Address

# Login to remote workstation



```
$ ssh chef@IP_ADDRESS
```

```
The authenticity of host '52.54.113.210 (52.54.113.210)' can't be established.
```

```
ECDSA key fingerprint is
```

```
SHA256:zAtoe029XbhRNvg542cuh4qsKCEaX8hNlEOCbgd3I.
```

```
Are you sure you want to continue connecting (yes/no)?
```

# Login to remote workstation



```
$ ssh chef@IP_ADDRESS
```

```
The authenticity of host '52.54.113.210 (52.54.113.210)' can't be established.
```

```
ECDSA key fingerprint is
```

```
SHA256:zAtoe029XbhRNvg542cuh4qsKCEaX8hNlEOCbgd3I.
```

```
Are you sure you want to continue connecting (yes/no)? yes
```

# Login to remote workstation



```
$ ssh chef@IP_ADDRESS
```

```
The authenticity of host '52.54.113.210 (52.54.113.210)' can't be established.
```

```
ECDSA key fingerprint is
```

```
SHA256:zAtoe029XbhRNvg542cuh4qsKCEaX8hNlEOCbgd3I.
```

```
Are you sure you want to continue connecting (yes/no)? Yes
```

```
Warning: Permanently added '52.54.113.210' (ECDSA) to the list of known hosts.
```

```
chef@52.54.113.210's password:
```

# Login to remote workstation



```
$ ssh chef@IP_ADDRESS
```

```
The authenticity of host '52.54.113.210 (52.54.113.210)' can't be established.
```

```
ECDSA key fingerprint is
```

```
SHA256:zAtoe029XbhRNvg542cuh4qsKCEaX8hNlEOCbgd3I.
```

```
Are you sure you want to continue connecting (yes/no)? Yes
```

```
Warning: Permanently added '52.54.113.210' (ECDSA) to the list of known hosts.
```

```
chef@52.54.113.210's password: chef
```

# Touch a file with your name



```
$ touch firstname.lastname
```

# List your home directory



```
$ sleep 60 && ls -t
```

```
firstname.lastname  cookbooks      Berksfile    profiles  
nodes           Berksfile.lock  config.json
```

# Verify the installation



```
$ which inspec
```

```
/opt/chefdk/bin/inspec
```

# Verify the installation



```
$ inspec version
```

```
1.11.0
```

Your version of InSpec is out of date! The latest version is 1.15.0.

# Verify the installation



```
$ which chef
```

```
/opt/chefdk/bin/chef
```

# Verify the installation



```
$ chef --version
```

```
Chef Development Kit Version: 1.2.22
chef-client version: 12.18.31
delivery version: master (0b746cafed65a9ea1a79de3cc546e7922de9187c)
berks version: 2017-03-02T09:46:48.762338 20503]
2017-03-02T09:46:48.762505 20503] 2017-03-02T09:46:48.762618 20503]
2017-03-02T09:46:48.762722 20503] 2017-03-02T09:46:48.791141 20503]
2017-03-02T09:46:48.791248 20503] 5.6.0
kitchen version: 1.15.0
```

# Chef DK - The Chef Development Kit

- Definitive tooling for local development of Chef code & Infrastructure as Code development

## FAST INEXPENSIVE TESTING

### Foodcritic

#### Test Your “Chef Style”

- Validate your Chef code against Chef best practices
- Extend with rules to enforce organizational Chef development best practices
- Enforce compliance & security practices

### CookStyle

#### Validate your Ruby

- Validate your Chef code against Ruby best practices
- Identify potential Ruby errors  
Unclosed strings, etc.
- Identify style/convention that helps write better code  
Single quotes vs. double quotes

### ChefSpec

#### Simulate Chef

- Validate your Chef code will run
- Testing for more Chef advanced use cases
- Useful for regression testing

## DEEP INTEGRATION TESTING

### Test Kitchen

#### Let's do this (almost) for real

- Executes your Chef code on an instance or container
- Integrates with Cloud and Virtualization providers
- Validate your Chef code locally before sharing
- Speed development of Chef Cookbooks

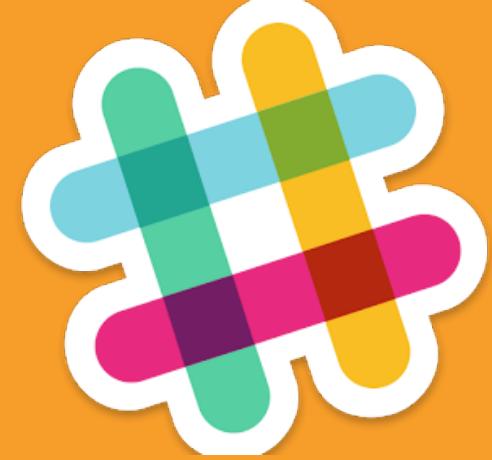
### InSpec

#### Verify automation results & ensure compliance

- Assert the intention of your Chef code
- Verify on live systems that your Chef code produced the correct result
- Confirm your Chef code didn't not produce compliance drift

# Join Slack Team & Channel

- <http://community-slack.chef.io>
- #CHANNEL-NAME



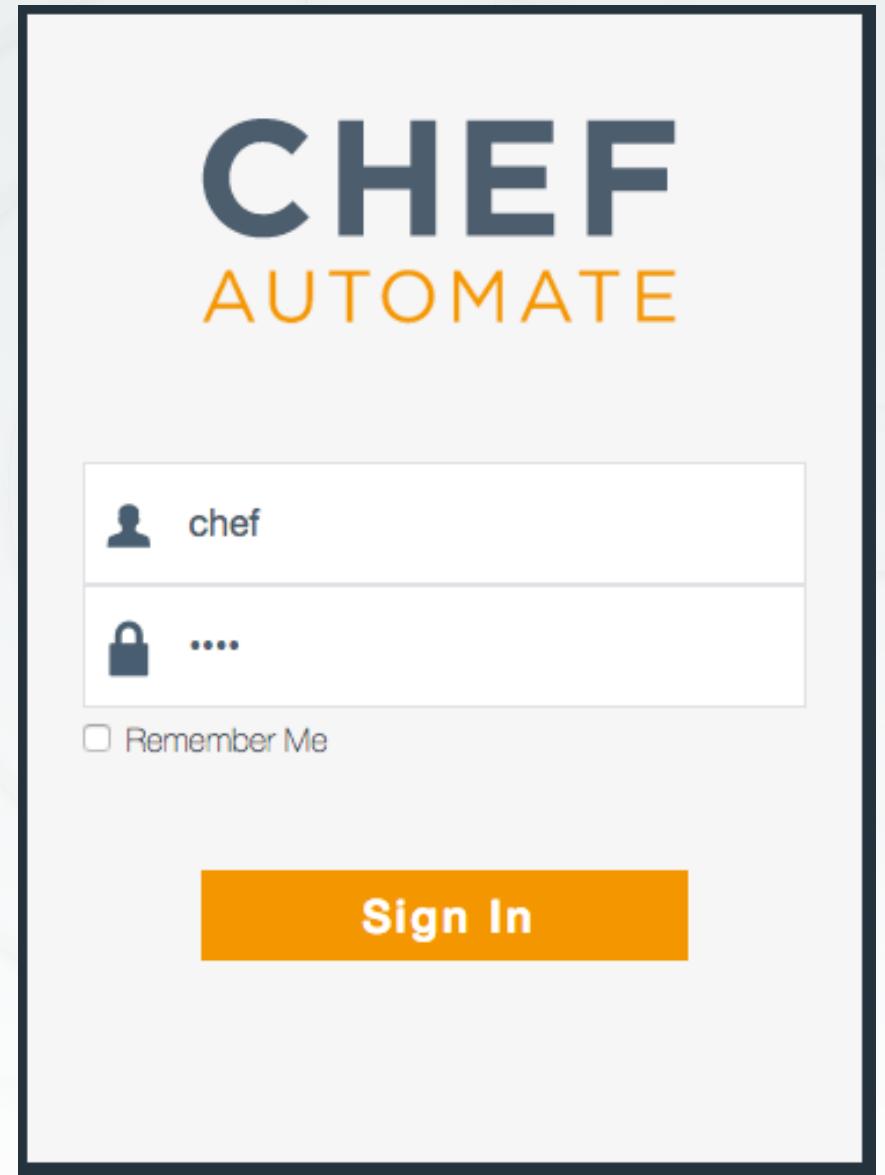
#CHANNEL-NAME

# Continuous Compliance

Chef Automate and InSpec Profiles

# Login to Chef Automate

- <https://informatica-compliance-workshop.chefdemo.net>
- Uses a self-signed certificate in this lab
- Username: **chef**
- Password: **chef**



# Browse to your node

The screenshot shows the Chef Automate dashboard interface. At the top, there is a navigation bar with the Chef Automate logo, a user icon labeled "chef", and menu items: "Nodes", "Workflow", and "Admin". An orange arrow points from the left towards the "Nodes" button, which is also highlighted with an orange border. Below the navigation bar, there are two main sections: "Converge Status" on the left and "Runner Activity" on the right.

**Converge Status** (Left Section):

- Converge Status:** A large green circle icon with a white server icon inside.
- FAILED NODES:** 0 (red exclamation mark icon)
- SUCCESSFUL NODES:** 3 (green checkmark icon)
- COOKBOOK CHANGES \***: 0 (orange 'c' icon)
- WORKFLOW CHANGES \***: 0 (purple 'w' icon)

**Runner Activity** (Right Section):

- ACTIVE RUNNERS:** 0 (green play button icon)
- IDLE RUNNERS:** 0 (blue clock icon)

# Browse to your node

Total Nodes ● 3	Failed Nodes ⚠ 0	Successful Nodes ✓ 3	Missing Nodes ? 0	
<b>Converge</b> Node Name ▲ Check-in ▲ Uptime ▲ Platform ▲ Environment ▲				
✓ orange-2-of-hearts	2 minutes ago	a minute	centos	_default >
✓ orange-3-of-hearts	3 minutes ago	2 minutes	centos	_default >
✓ orange-4-of-hearts	2 minutes ago	2 minutes	centos	_default >

# View details of your node

[All Nodes](#)

## Node Detail

Use the run history list to examine recent Chef client runs for this node.

Node Name	orange-3-of-hearts
Org Name	chef_solo
Environment	_default

Converge Status      Compliance Status

✓ This run succeeded on 03/13/2017 at 4:47 PM. All resources ran successfully!

Run Progress  
100%

Node Name	orange-3-of-hearts	Uptime	2 minutes
Run Duration	4:47 PM - 4:47 PM	Environment	_default
Run Initiator	Not Available	Platform(s)	centos
Run Type	Not Available	IP Address	172.31.1.145
Run ID	9f70014f-b27c-4774-9eca-66552214ba45	FQDN	ip-172-31-1-145.us-west-2.compute.internal

[Resources](#)    [Run List](#)    [Attributes](#)

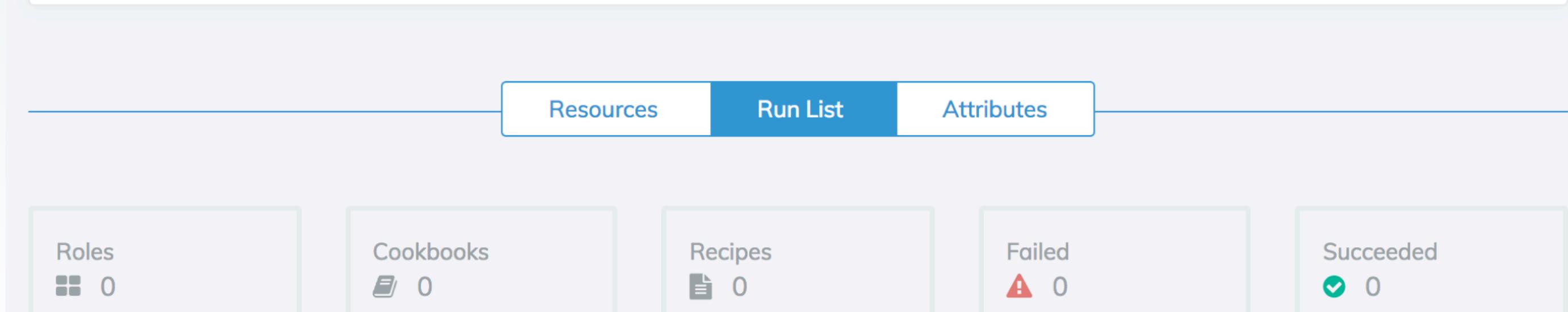
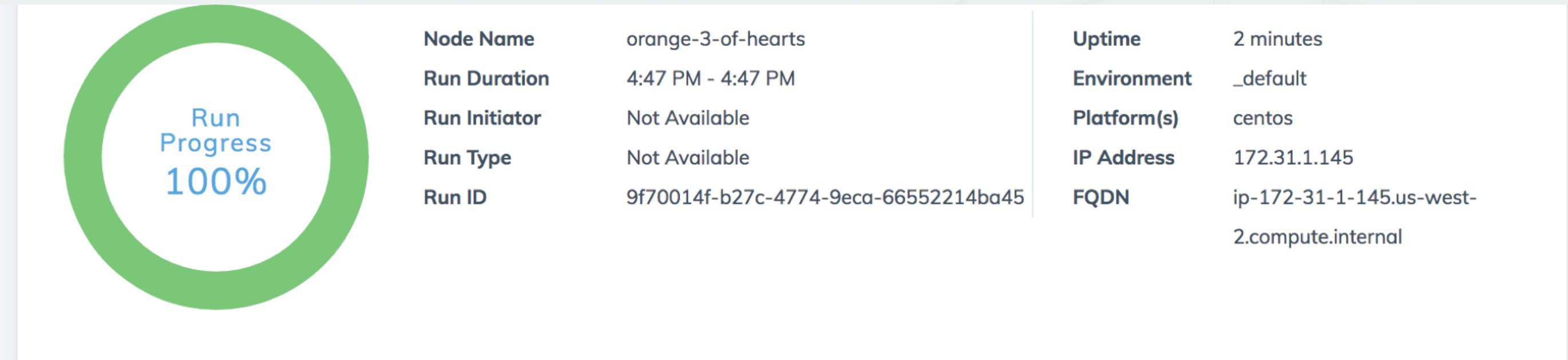
**Run History**

Last 24 hours

1	0	1
---	---	---

03/13/17 16:47:08  
a few seconds 16:47:08

# View details of your node



# View details of your node

The screenshot shows the Chef Attributes view for a node. At the top, there are three tabs: Resources, Run List, and Attributes, with Attributes selected. Below the tabs is a search bar containing "Search attributes..." and a magnifying glass icon. Underneath the search bar are five filter buttons: All (orange, showing 4,107), Default (0), Normal (0), Overall (0), and Automatic (4,107). Below the filters is a section with two buttons: "Expand All" and "Collapse All". The main area displays a list of attributes, each preceded by a plus sign and followed by a truncated value. The attributes listed are: "block\_device" : { ... }, "chef\_packages" : { ... }, "cloud" : { ... }, "cloud\_v2" : { ... }, "command" : { ... }, "counters" : { ... }, "cpu" : { ... }, "current\_user" : "chef", "dmi" : { ... }, and "domain" : "us-west-2.compute.internal".

All	Default	Normal	Overall	Automatic
4,107	0	0	0	4,107

[+ Expand All](#) | [- Collapse All](#)

```
+ "block_device" : { ... },
+ "chef_packages" : { ... },
+ "cloud" : { ... },
+ "cloud_v2" : { ... },
+ "command" : { ... },
+ "counters" : { ... },
+ "cpu" : { ... },
"current_user" : "chef",
+ "dmi" : { ... },
"domain" : "us-west-2.compute.internal",
```

# View details of your node

Converge Status    Compliance Status

Compliance Scores

Node Name	Scan Duration
Scan Time	4:51 PM - 4:51 PM
Scan Initiator	a few seconds
Scan ID	Scheduled

Inspec Version	Profiles Scanned
Platform(s)	0

Total Controls 0

Critical Controls 0

Major Controls 0

Minor Controls 0

Compliant Controls 0

Skipped Controls 0

Status	Score	Control	Profile	Failed	Skipped	Passed	Details
--------	-------	---------	---------	--------	---------	--------	---------

# The node uses chef solo

[\*\*< All Nodes\*\*](#)

## Node Detail

Use the run history list to examine recent Chef client runs for this node.

Node Name	orange-3-of-hearts
Org Name	chef_solo
Environment	_default

# Chef Automate – Node View

- View aggregate status of your infrastructure

Overall & trend views of converge status

Overall & trend views of compliance status

Filter & search options

- View details of any node

Status of converged resources

Run List applied to the node

Attributes of the node

# Chef Solo

Executes chef-client without relying on a Chef server to provide configuration policies (cookbooks, environments, etc.)

[https://docs.chef.io/chef\\_solo.html](https://docs.chef.io/chef_solo.html)

# Chef Solo

- Local directory for configuration policy
  - Or a URL from which a `.tar.gz` file can be downloaded
- Node objects stored as a local JSON file
- Attribute data stored in a JSON file
  - Local or remote
- Does not pull from a Chef Server
- Can be configured to send data to a Chef Server

# Chef Client – Local Mode

Local mode is a way to run the chef-client against the chef-repo on a local machine as if it were running against the Chef server.

[https://docs.chef.io/ctl\\_chef\\_client.html#run-in-local-mode](https://docs.chef.io/ctl_chef_client.html#run-in-local-mode)

# Go home



```
$ cd ~
```

# Run chef-client in local mode



```
$ sudo run_chef
```

```
[2017-03-10T14:05:49+00:00] INFO: Forking chef instance to converge...
Starting Chef Client, version 12.18.31
...
Converging 0 resources
[2017-03-10T14:05:51+00:00] INFO: Chef Run complete in 0.19413018 seconds

Running handlers:
[2017-03-10T14:05:51+00:00] INFO: Running report handlers
Running handlers complete
[2017-03-10T14:05:51+00:00] INFO: Report handlers complete
Chef Client finished, 0/0 resources updated in 01 seconds
```

# Check the converge status in Automate

Node Name: orange-3-of-hearts  
Org Name: chef\_solo  
Environment: \_default

ces ran successfully!

orange-3-of-hearts 4:54 PM - 4:54 PM Not Available Not Available 6b040a4a-537b-4541-a5ea-19efcc3c7204	Uptime Environment Platform(s) IP Address FQDN	9 minutes _default centos 172.31.1.145 ip-172-31-1-145.us-west- 2.compute.internal
---	--	---

### Run History

Last 24 hours

Count	Warnings	Successes
3	0	3

Date	Time	Duration	Time
03/13/17	16:54:22	a few seconds	16:54:28
03/13/17	16:54:13	a few seconds	16:54:13
03/13/17	16:47:08	a few seconds	16:47:08

# Run with additional parameters



```
$ sudo run_chef "recipe[audit::default]"
```

```
[2017-03-10T14:10:34+00:00] INFO: Forking chef instance to converge...
Starting Chef Client, version 12.18.31
[2017-03-10T14:10:34+00:00] INFO: *** Chef 12.18.31 ***
...
[2017-03-10T14:10:40+00:00] INFO: Chef Run complete in 4.10402964 seconds
```

Running handlers:

```
[2017-03-10T14:10:40+00:00] INFO: Running report handlers
[2017-03-10T14:10:40+00:00] WARN: Format is json
[2017-03-10T14:10:40+00:00] INFO: Initialize InSpec
[2017-03-10T14:10:40+00:00] INFO: Running tests from: [{:name=>"ssh", :path=>"/home/chef/profiles/ssh"}]
[2017-03-10T14:10:40+00:00] INFO: Reporting to chef-visibility
...
```

Running handlers complete

```
[2017-03-10T14:10:40+00:00] INFO: Report handlers complete
Chef Client finished, 1/2 resources updated in 06 seconds
```

# Check the converge status in Automate



Run Progress  
100%

<b>Node Name</b>	orange-3-of-hearts	<b>Uptime</b>	9 minutes
<b>Run Duration</b>	4:54 PM - 4:54 PM	<b>Environment</b>	_default
<b>Run Initiator</b>	Not Available	<b>Platform(s)</b>	centos
<b>Run Type</b>	Not Available	<b>IP Address</b>	172.31.1.145
<b>Run ID</b>	6b040a4a-537b-4541-a5ea-19efcc3c7204	<b>FQDN</b>	ip-172-31-1-145.us-west-2.compute.internal

---

- Resources
- Run List
- Attributes

Total Resources ● 2	Failed ⚠ 0	Successful ✓ 1	Unchanged ✓ 1	Unprocessed ? 0
------------------------	---------------	-------------------	------------------	--------------------

# Check the converge status in Automate

Total Resources ● 2	Failed ⚠ 0	Successful ✓ 1	Unchanged ✓ 1	Unprocessed ❓ 0
Status Step Type Name Action Cookbook View				
✓ 1/2 chef_gem inspec		install	audit	--
✓ 2/2 chef_gem inspec		install	audit	--

# Check the compliance status in Automate

Converge Status    **Compliance Status**

**A** This node is uncompliant. Too many Critical and Major scored tests failed during the scan. | [View scan results](#)

<b>Node Name</b>	orange-3-of-hearts	<b>Inspec Version</b>	1.15.0
<b>Scan Duration</b>	4:54 PM - 4:54 PM	<b>Profiles Scanned</b>	1
<b>Scan Time</b>	a few seconds	<b>Platform(s)</b>	not defined
<b>Scan Initiator</b>	Scheduled		
<b>Scan ID</b>	6b040a4a-537b-4541-a5ea-19efcc3c7204		

<b>Total Controls</b> ● 1	<b>Critical Controls</b> ✖ 1	<b>Major Controls</b> 🚫 0	<b>Minor Controls</b> ❗ 0	<b>Compliant Controls</b> ✓ 0	<b>Skipped Controls</b> ❓ 0
------------------------------	---------------------------------	------------------------------	------------------------------	----------------------------------	--------------------------------

# Check the compliance status in Automate

Total Controls ● 1	Critical Controls ✖ 1	Major Controls 🚫 0	Minor Controls ❗ 0	Compliant Controls ✓ 0	Skipped Controls ❓ 0
Status Score Control Profile Failed Skipped Passed Details					
✖ 0.7 SSH Version 2 SSH Configuration 1 0 0 details					

# View details of the failing control

Status	Score	Control	Profile	Failed	Skipped	Passed	Details
<span style="color: red;">✖</span>	0.7	SSH Version 2	SSH Configuration	1	0	0	<span>details</span>

**Description:**  
Only SSH version 2 should be enabled

- Scan Results
- Additional Information

Status	Message	Start Time	Run Time
<span style="color: red;">⚠</span>	SSH Configuration Protocol should cmp == 2	03/13/2017   4:54 PM	a few seconds

# View details of the failing control

- Scan Results
- Additional Information



## Control:

```
control 'sshd-1.0' do
  impact 0.7
  title 'SSH Version 2'
  desc 'Only SSH version 2 should be enabled'
  describe sshd_config do
    its('Protocol') { should cmp 2 }
  end
end
```

## Tags:

# Review the set-up

tying it all together

# Go home



```
$ cd ~
```

# List contents



```
$ ls
```

```
Berksfile      config.json  firstname.lastname  profiles  
Berksfile.lock  cookbooks    nodes
```

# List cookbooks



```
$ ls cookbooks
```

```
audit  compat_resource
```

# Audit Cookbook

- Install InSpec
- Run InSpec profiles
- Report results to Chef Compliance or Chef Automate

# Compat Resource Cookbook

- Adds functionality introduced in the latest chef-client releases to any chef-client from 12.1 onwards.
- Includes
  - Custom Resource functionality
  - notification improvements
  - new resources added to core chef
- Allows for these new resources in cookbooks without requiring the very latest Chef client release.

# config.json



```
$ cat config.json
```

```
{  
  "audit": {  
    "collector": "chef-visibility",  
    "inspec_version": "1.15.0",  
    "profiles": [  
      {  
        "name": "ssh",  
        "path": "/home/chef/profiles/ssh"  
      }  
    ]  
  }  
}
```

# Local Profiles



```
$ tree profiles
```

```
profiles/
└── ssh
    ├── controls
    │   └── ssh.rb
    ├── inspec.lock
    └── inspec.yml
```

2 directories, 3 files

# Run Locally with InSpec



```
$ inspec exec profiles/ssh
```

```
Profile: SSH Configuration (ssh)
Version: 0.1.0
Target: local://

  x sshd-1.0: SSH Version 2 (
    expected: 2
      got:

        (compared using `cmp` matcher)
    )
  x SSH Configuration Protocol should cmp == 2

    expected: 2
      got:

        (compared using `cmp` matcher)

Profile Summary: 0 successful, 1 failures, 0 skipped
Test Summary: 0 successful, 1 failures, 0 skipped
```

# Next Steps

- Remediate the failing control
- Run the audit cookbook to verify the remediation
- View the compliant node in Automate

# Remediate the Failing Control

# Fix your ssh configuration on your own

- Write a cookbook to manage SSH
- Manually update the SSH configuration

# Verify Compliance Status in Automate

Converge Status      **Compliance Status**

✓ This node is compliant. View scan results

A large green circle with a white center. Inside the white center, the words "Compliance Scores" are written in a blue, sans-serif font.

Node Name orange-3-of-hearts  
Scan Duration 5:03 PM - 5:03 PM  
Scan Time a few seconds  
Scan Initiator Scheduled  
Scan ID 6076b098-e02c-4b6e-8731-  
8c63217e8733

Inspec Version 1.15.0  
Profiles Scanned 1  
Platform(s) not defined

# Verify Compliance Status in Automate

Total Controls ● 1	Critical Controls ✖ 0	Major Controls 🚫 0	Minor Controls ❗ 0	Compliant Controls ✓ 1	Skipped Controls ❓ 0		
Status	Score	Control	Profile	Failed	Skipped	Passed	Details
✓	0.7	SSH Version 2	SSH Configuration	0	0	1	<a href="#">details</a>

# Remediate Failing SSH Control

# Simple SSH Cookbook

- A server recipe to manage the sshd\_config file
- Local test environment configured

# Move to the cookbooks directory



```
$ cd ~/cookbooks
```

# Generate an ssh cookbook



```
$ chef generate cookbook ssh
```

```
Generating cookbook ssh
- Ensuring correct cookbook file content
- Committing cookbook files to git
- Ensuring delivery configuration
- Ensuring correct delivery build cookbook content
- Adding delivery configuration to feature branch
- Adding build cookbook to feature branch
- Merging delivery content feature branch to master
```

Your cookbook is ready. Type `cd ssh` to enter it.

There are several commands you can run to get started locally developing and testing your cookbook.  
Type `delivery local --help` to see a full list.

Why not start by writing a test? Tests for the default recipe are stored at:

test/smoke/default/default\_test.rb

If you'd prefer to dive right in, the default recipe can be found at:

recipes/default.rb

# Add a server recipe to the ssh cookbook



```
$ chef generate recipe ssh server
```

```
Recipe: code_generator::recipe
  * directory[./ssh/spec/unit/recipes] action create (up to date)
  * cookbook_file[./ssh/spec/spec_helper.rb] action create_if_missing (up to date)
  * template[./ssh/spec/unit/recipes/server_spec.rb] action create_if_missing
    - create new file ./ssh/spec/unit/recipes/server_spec.rb
    - update content in file ./ssh/spec/unit/recipes/server_spec.rb from none to d14960
      (diff output suppressed by config)
  * directory[./ssh/test/smoke/default] action create (up to date)
  * template[./ssh/test/smoke/default/server.rb] action create_if_missing
    - create new file ./ssh/test/smoke/default/server.rb
    - update content in file ./ssh/test/smoke/default/server.rb from none to aa8bba
      (diff output suppressed by config)
  * template[./ssh/recipes/server.rb] action create
    - create new file ./ssh/recipes/server.rb
    - update content in file ./ssh/recipes/server.rb from none to 18f24e
      (diff output suppressed by config)
```

# Add a template to the cookbook



```
$ chef generate template ssh sshd_config -s /etc/ssh/sshd_config
```

```
Recipe: code_generator::template
```

```
* directory[./ssh/templates/default] action create
  - create new directory ./ssh/templates/default
* file[./ssh/templates/sshd_config.erb] action create
  - create new file ./ssh/templates/sshd_config.erb
  - update content in file ./ssh/templates/sshd_config.erb from none to
```

```
a16b11
```

```
(diff output suppressed by config)
```

# Server Recipe

~/.cookbooks/ssh/recipes/server.rb

```
template '/etc/ssh/sshd_config' do
  source 'sshd_config.erb'
  owner 'root'
  group 'root'
  mode '0600'
end
```

# Remember...

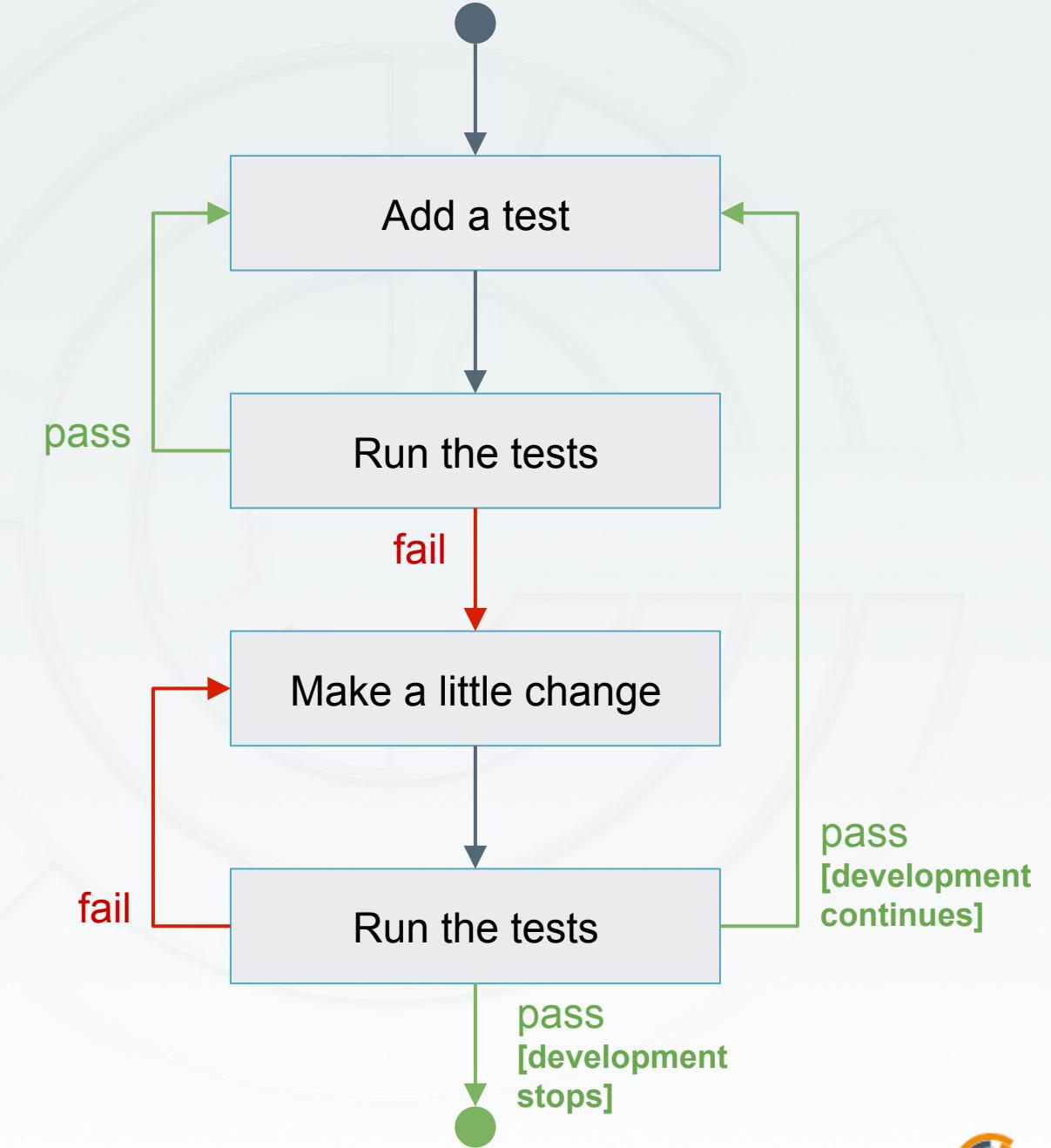
- Infrastructure policies need testing
  - ↳ Linting
  - ↳ Static Analysis
  - ↳ Unit Testing
  - ↳ Integration Testing
  - ↳ Compliance Testing



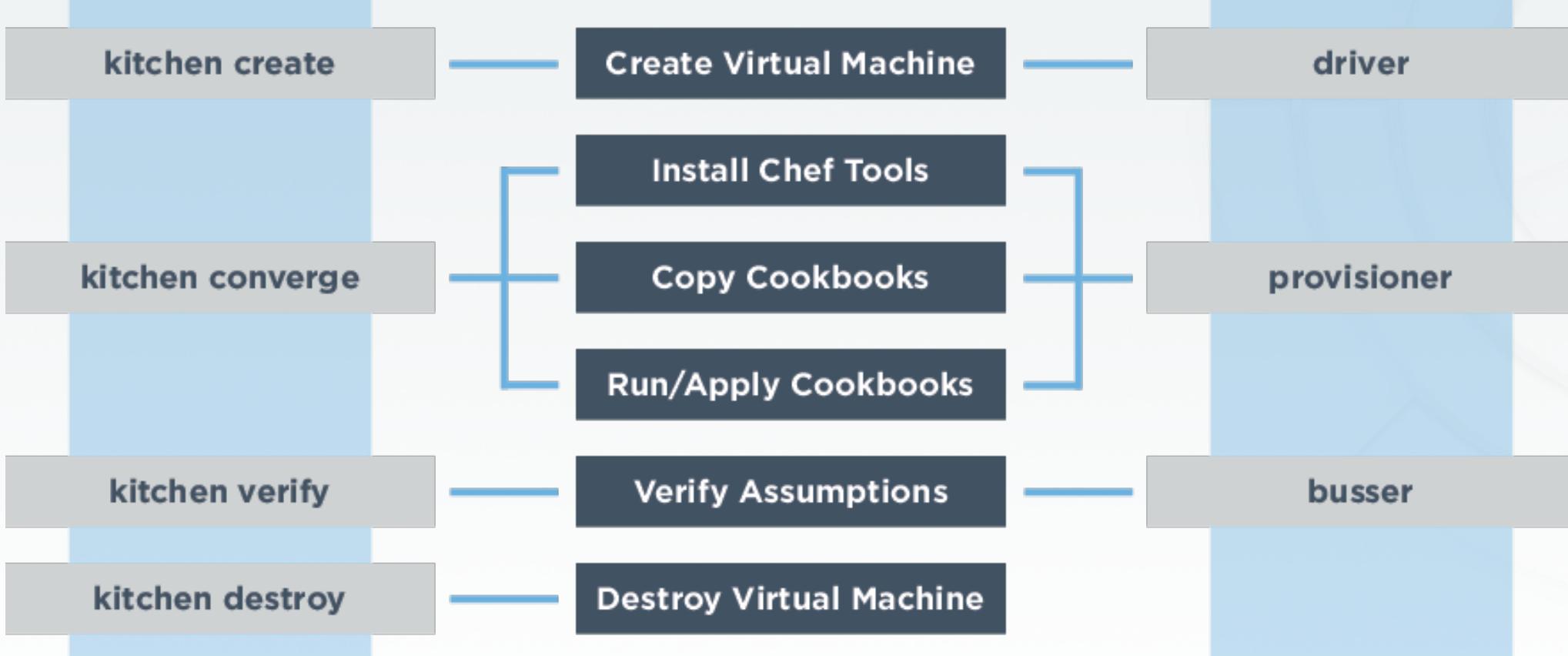
**"Infrastructure as Code"** should be tested like ANY other codebase.

# Test-driven Development

- Write a test, watch it fail
- Write some code
- Write and run more tests
- Code review
- Delivery pipeline to production
- Lowered chance of production failure

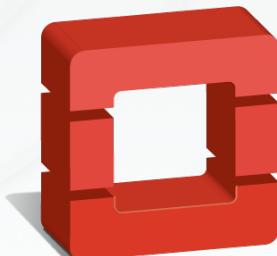


# Testing the change



Microsoft Azure

vmware®



openstack™



# Test Kitchen Configuration (1 of 3)

└── `~/cookbooks/ssh/.kitchen.yml`

```
---
```

```
driver:
```

```
- name: vagrant
```

```
+ name: docker
```

```
...
```

# Test Kitchen Configuration (2 of 3)

└── `~/cookbooks/ssh/.kitchen.yml`

```
...
```

```
platforms:
```

- `- name: ubuntu-16.04`
- `- name: centos-7.2`
- + `- name: centos-7.3`

```
...
```

# Test Kitchen Configuration (3 of 3)

~/.kitchen.yml

```
suites:  
- name: default
```

```
+ name: server  
  run_list:
```

```
- recipe[ssh::default]  
+ recipe[ssh::server]
```

```
verifier:
```

```
  inspec_tests:
```

```
- test/smoke/default  
+ /home/chef/profiles/ssh
```

```
attributes:
```

# Move to the cookbook's directory



```
$ cd ~/cookbooks/ssh
```

# List the kitchens



```
$ kitchen list
```

Instance	Driver	Provisioner	Verifier	Transport	Last Action	Last Error
server-centos-73	Docker	ChefZero	Inspec	Ssh	<Not Created>	<None>

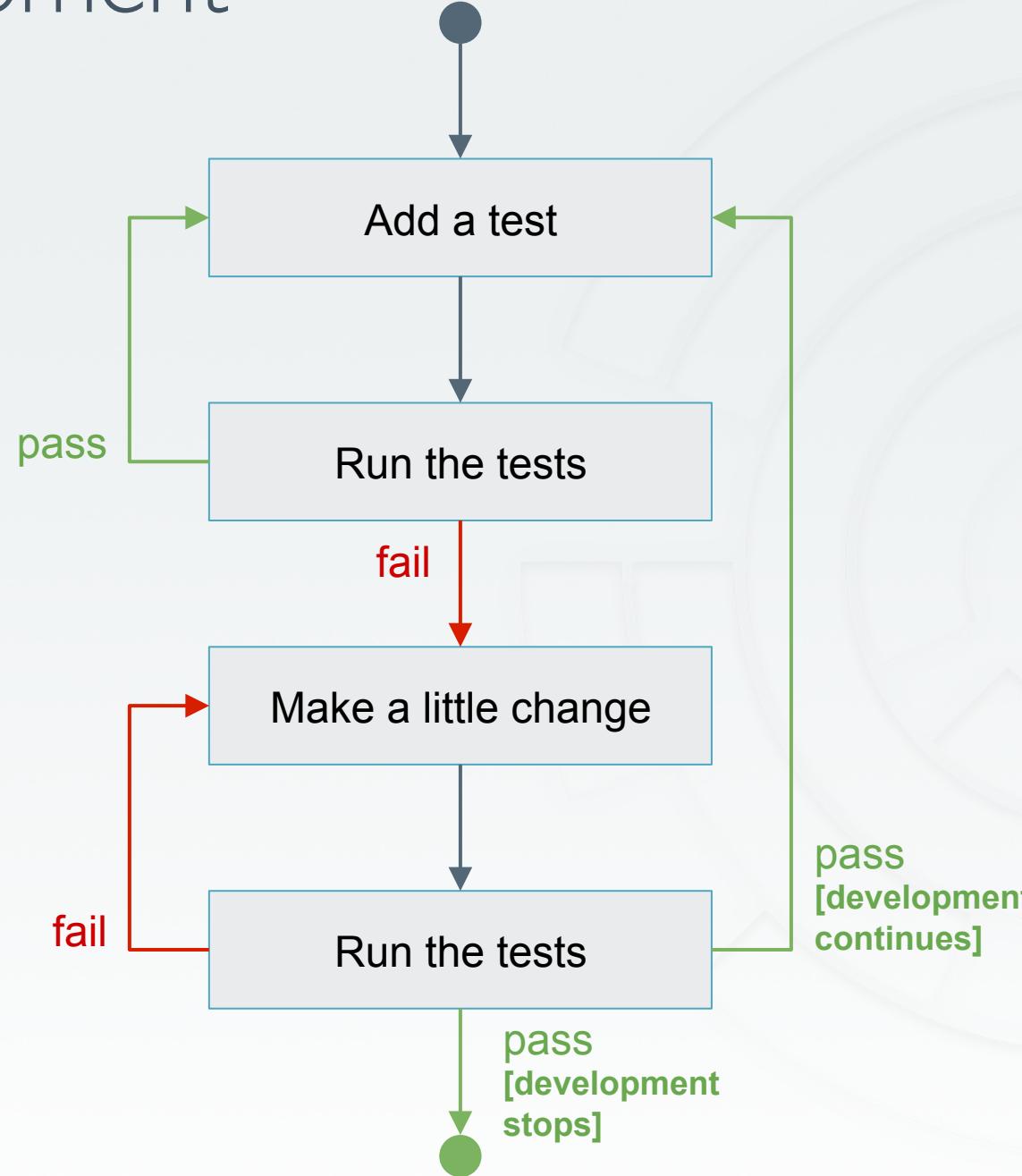
# Converge



```
$ kitchen converge
```

```
----> Starting Kitchen (v1.15.0)
...
----> Creating <server-centos-73>...
      Sending build context to Docker daemon 227.8 kB
      Sending build context to Docker daemon
      Step 0 : FROM centos:centos7
      ...
Running handlers:
[2017-03-12T02:26:16+00:00] INFO: Running report handlers
Running handlers complete
[2017-03-12T02:26:16+00:00] INFO: Report handlers complete
Chef Client finished, 1/1 resources updated in 01 seconds
Finished converging <server-centos-73> (0m23.54s).
----> Kitchen is finished. (1m0.39s)
```

# Test-driven Development



pass  
[development  
continues]

pass  
[development  
stops]

# Verify the Kitchen



```
$ kitchen verify
```

```
----> Verifying <server-centos-73>...
Loaded

Target: ssh://kitchen@localhost:32771

× sshd-1.0: SSH Version 2 (
  expected: 2
  got:

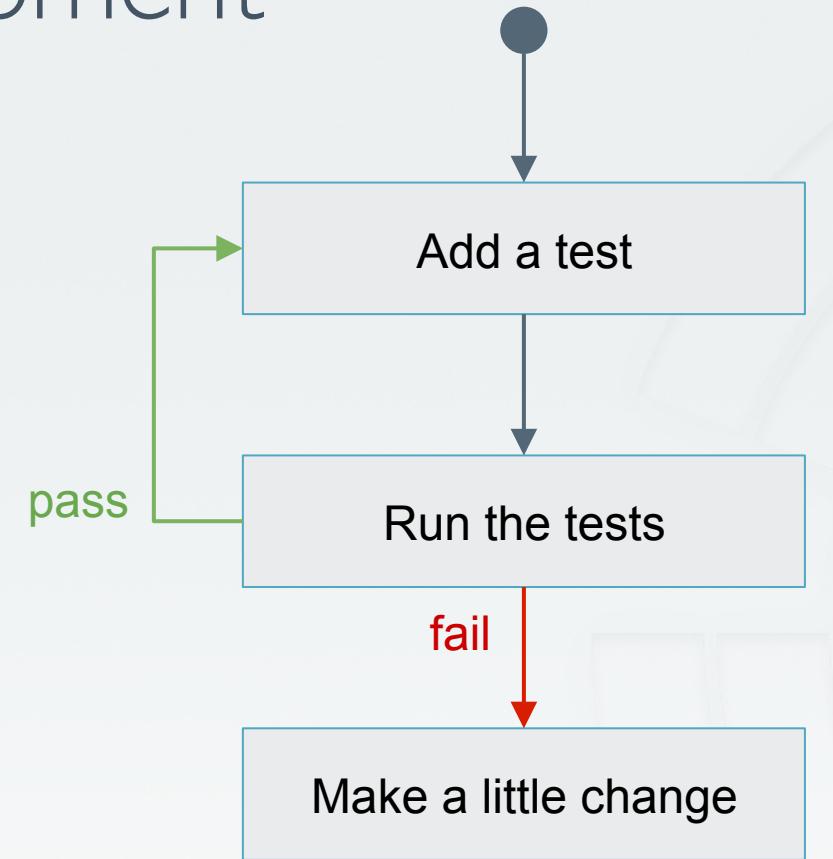
    (compared using `cmp` matcher)
  )
× SSH Configuration Protocol should cmp == 2

  expected: 2
  got:

    (compared using `cmp` matcher)

Profile Summary: 0 successful, 1 failures, 0 skipped
Test Summary: 0 successful, 1 failures, 0 skipped
```

# Test-driven Development



# Edit the SSH Configuration Template

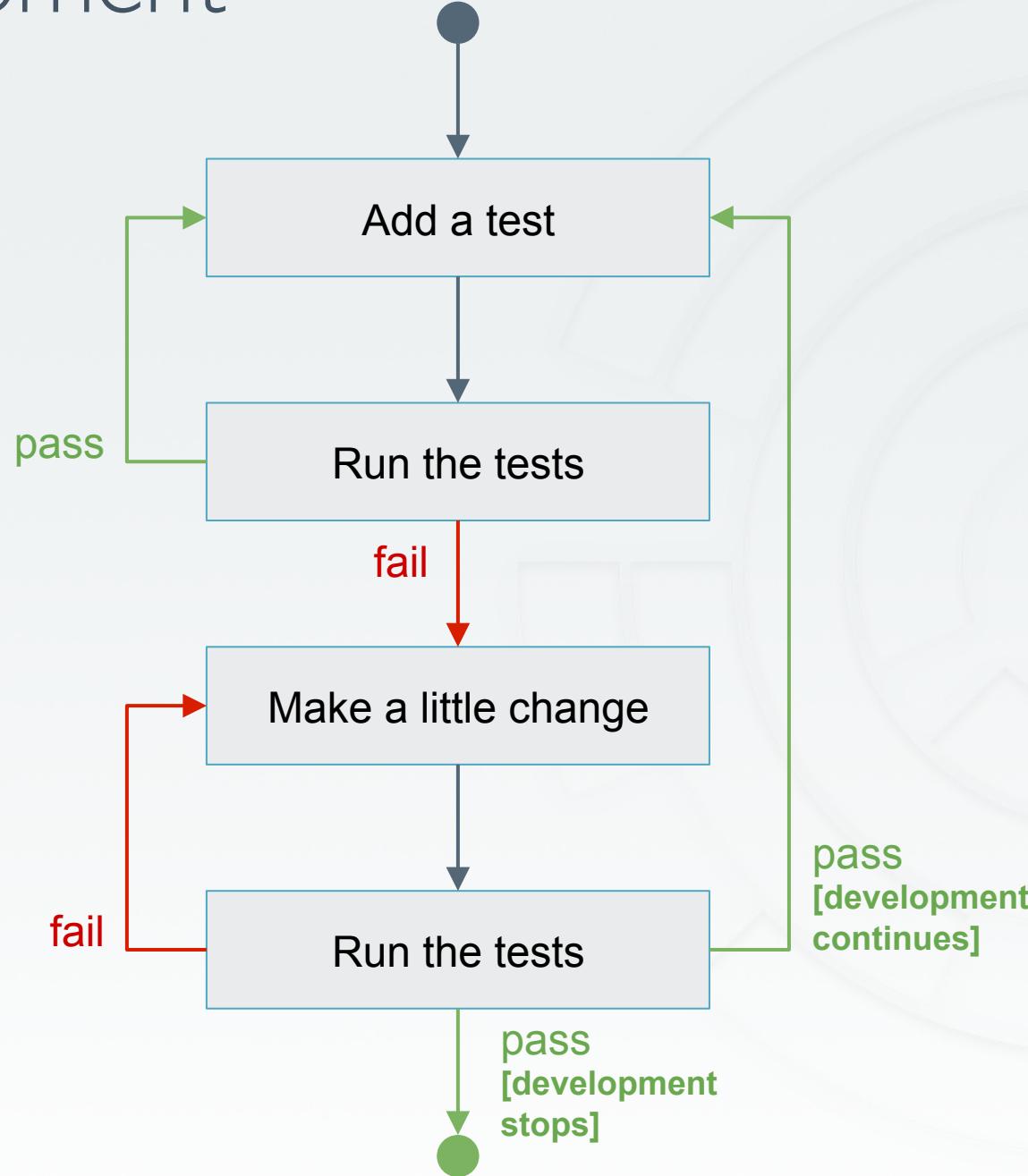
~/cookbooks/ssh/templates/sshd\_config.erb

```
#ListenAddress 0.0.0.0
#ListenAddress ::

# The default requires explicit activation of protocol 1
- #Protocol 2
+ Protocol 2

# HostKey for protocol version 1
```

# Test-driven Development



pass  
[development  
continues]

pass  
[development  
stops]

# Converge



```
$ kitchen converge
```

```
----> Starting Kitchen (v1.15.0)
...
----> Converging <server-centos-73>...
...
# The default requires explicit activation of protocol 1
-#Protocol 2
+Protocol 2

# HostKey for protocol version 1
...
Running handlers:
[2017-03-12T02:32:32+00:00] INFO: Running report handlers
Running handlers complete
[2017-03-12T02:32:32+00:00] INFO: Report handlers complete
Chef Client finished, 1/1 resources updated in 01 seconds
Finished converging <server-centos-73> (0m16.32s).
----> Kitchen is finished. (0m17.34s)
```

# Verify the Kitchen



```
$ kitchen verify
```

```
----> Starting Kitchen (v1.15.0)
...
----> Verifying <server-centos-73>...
     Loaded
```

Target: ssh://kitchen@localhost:32771

- ✓ sshd-1.0: SSH Version 2
- ✓ SSH Configuration Protocol should cmp == 2

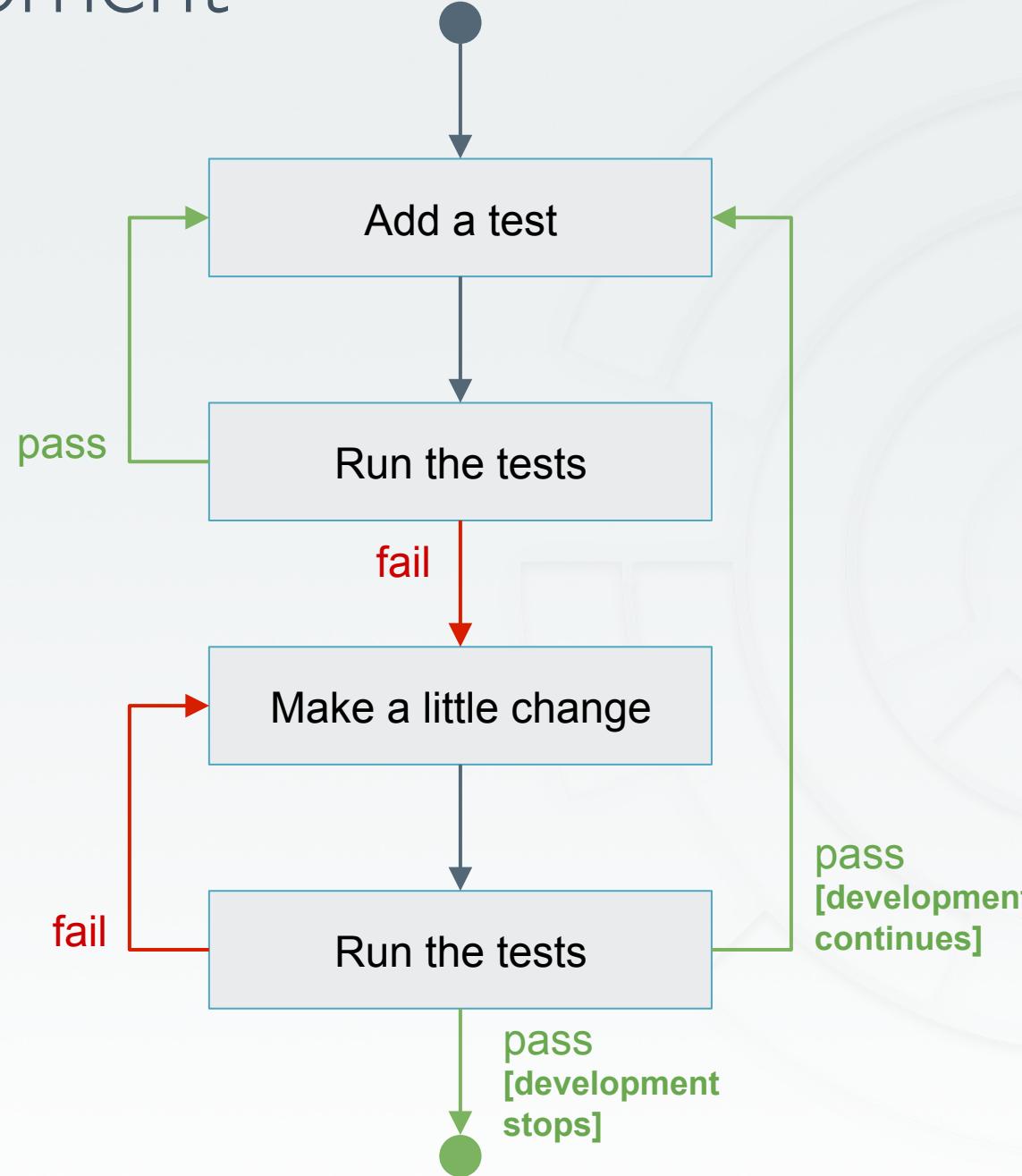
Profile Summary: 1 successful, 0 failures, 0 skipped

Test Summary: 1 successful, 0 failures, 0 skipped

Finished verifying <server-centos-73> (0m0.22s).

```
----> Kitchen is finished. (0m1.27s)
```

# Test-driven Development



pass  
[development  
continues]

pass  
[development  
stops]

# Test the Kitchen (1 of 2)



```
$ kitchen test
```

```
-----> Starting Kitchen (v1.15.0)
...
-----> Cleaning up any prior instances of <server-centos-73>
-----> Destroying <server-centos-73>...
...
-----> Testing <server-centos-73>
-----> Creating <server-centos-73>...
...
-----> Creating <server-centos-73>...
...
-----> Converging <server-centos-73>...
...
          Finished creating <server-centos-73> (0m0.60s).
```

# Test the Kitchen (2 of 2)



```
$ kitchen test
```

```
----> Installing Chef Omnibus (install only if missing)
...
----> Setting up <server-centos-73>...
      Finished setting up <server-centos-73> (0m0.00s).
----> Verifying <server-centos-73>...
...
Profile Summary: 1 successful, 0 failures, 0 skipped
Test Summary: 1 successful, 0 failures, 0 skipped
      Finished verifying <server-centos-73> (0m0.51s).
----> Destroying <server-centos-73>...
...
----> Kitchen is finished. (0m25.18s)
```

# What's next?

- Test-driven development cycle is complete
- Deploy the change

# Remediate with Chef



```
$ sudo run_chef "recipe[ssh::server],recipe[audit::default]"
```

```
[2017-03-10T16:48:02+00:00] INFO: Forking chef instance to converge...
```

```
Starting Chef Client, version 12.18.31
```

```
...
```

```
Synchronizing Cookbooks:
```

- ssh (0.1.0)
- audit (2.4.0)
- compat\_resource (12.16.3)

```
...
```

```
-#Protocol 2  
+Protocol 2
```

```
...
```

```
[2017-03-10T16:48:05+00:00] INFO: Chef Run complete in 1.248588588 seconds
```

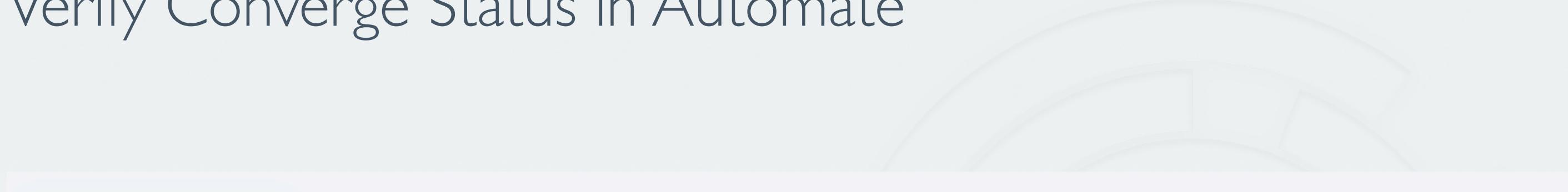
```
Running handlers:
```

```
...
```

```
[2017-03-10T16:48:05+00:00] INFO: Report handlers complete
```

```
Chef Client finished, 1/3 resources updated in 03 seconds
```

# Verify Converge Status in Automate



Total Resources	Failed	Successful	Unchanged	Unprocessed		
● 3	⚠ 0	✓ 1	✓ 2	?	0	
Status	Step	Type	Name	Action	Cookbook	View
✓	1/3	chef_gem	inspec	install	audit	--
✓	2/3	template	/etc/ssh/sshd_config	create	ssh	--

# Verify Compliance Status in Automate

Converge Status      **Compliance Status**

✓ This node is compliant. View scan results

A large green circle with a white center. Inside the white center, the words "Compliance Scores" are written in a blue, sans-serif font.

Node Name orange-3-of-hearts  
Scan Duration 5:03 PM - 5:03 PM  
Scan Time a few seconds  
Scan Initiator Scheduled  
Scan ID 6076b098-e02c-4b6e-8731-  
8c63217e8733

Inspec Version 1.15.0  
Profiles Scanned 1  
Platform(s) not defined

# Verify Compliance Status in Automate

Total Controls ● 1	Critical Controls ✖ 0	Major Controls 🚫 0	Minor Controls ❗ 0	Compliant Controls ✓ 1	Skipped Controls ❓ 0		
Status	Score	Control	Profile	Failed	Skipped	Passed	Details
✓	0.7	SSH Version 2	SSH Configuration	0	0	1	<a href="#">details</a>

# More hands-on Exercises

Still have time to play around?

# Server SSH Key

- Write a control that:
  - Tests for the existence of `/etc/ssh/ssh_host_rsa_key`
  - Tests that `/etc/ssh/ssh_host_rsa_key` contains “`BEGIN RSA PRIVATE KEY`”
- Check out the docs on <http://inspec.io> for what InSpec resource you can use

# Ensure SSH root login is disabled

- The PermitRootLogin parameter specifies if the root user can log in using ssh(1). The default is no.
- Disallowing root logins over SSH requires system admins to authenticate using their own individual account, then escalating to root via sudo or su. This in turn limits opportunity for non-repudiation and provides a clear audit trail in the event of a security incident
- Add a control to `~/profiles/ssh/controls/ssh.rb`

# Supermarket Profiles

- List profiles available on the Supermarket
- View information about the dev-sec/ssh-baseline profile
- Execute the dev-sec/ssh-baseline profile from the Supermarket
- Write a cookbook to remediate failing controls from dev-sec/ssh-baseline

Or look at the ssh-hardening cookbook

# Build additional CIS controls

- <https://github.com/chef-training/workshops/tree/master/InSpec>

# Static Analysis

- Ensure cookbooks pass chefstyle
- Ensure cookbooks pass foodcritic

# Unit Testing

- Add unit testing to the cookbooks

# Further Resources

Where to go for additional help

# Community Resources

- InSpec Website, includes tutorials and docs - <http://inspec.io/>
- #inspec channel of the Chef Community Slack - <http://community-slack.chef.io/>
- InSpec category of the Chef Mailing List - <https://discourse.chef.io/c/inspec>
- Compliance Profiles on the Supermarket - [https://supermarket.chef.io/tools?type=compliance\\_profile](https://supermarket.chef.io/tools?type=compliance_profile)
- Open Source Project - <https://github.com/chef/inspec>



MAY 22-24 | AUSTIN

# CHEFCONF 2017

## DAY 1 // MAY 22

- ★ Workshops & Chef Training
- ★ DevOps Leadership Summit
- ★ Community Summit
- ★ Partner Summit
- ★ Welcome Reception
- ★ Customer Dinner
- ★ Analyst Day

## DAY 2 // MAY 23

- ★ Keynotes
- ★ Technical Sessions
- ★ Happy Hour
- ★ Game Night
- ★ Executive Dinner

## DAY 3 // MAY 24

- ★ Keynotes
- ★ Technical Sessions
- ★ Awesome Chef Awards
- ★ Community Celebration

## DAY 4 // MAY 25

- ★ Hackday

• Exhibit Hall Open & Sales suites available • [chefconf.chef.io](http://chefconf.chef.io) •

A photograph of a conference stage. A man with a beard and glasses, wearing a light-colored shirt and jeans, stands on the left side of the stage, gesturing with his right hand while holding a microphone in his left. He is positioned in front of a large, curved, purple-lit backdrop. To his right, a long line of people, mostly men, stands on a brick-paved floor, facing the stage. The lighting is dramatic, with strong stage lights and a colorful, blurred background.

MAY 22-24 | AUSTIN

# CHEFCONF 2017

[chefconf.chef.io](http://chefconf.chef.io)

# REGISTER NOW

\$995 EARLY  
BIRD PRICE  
ENDS MARCH 31<sup>st</sup>