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

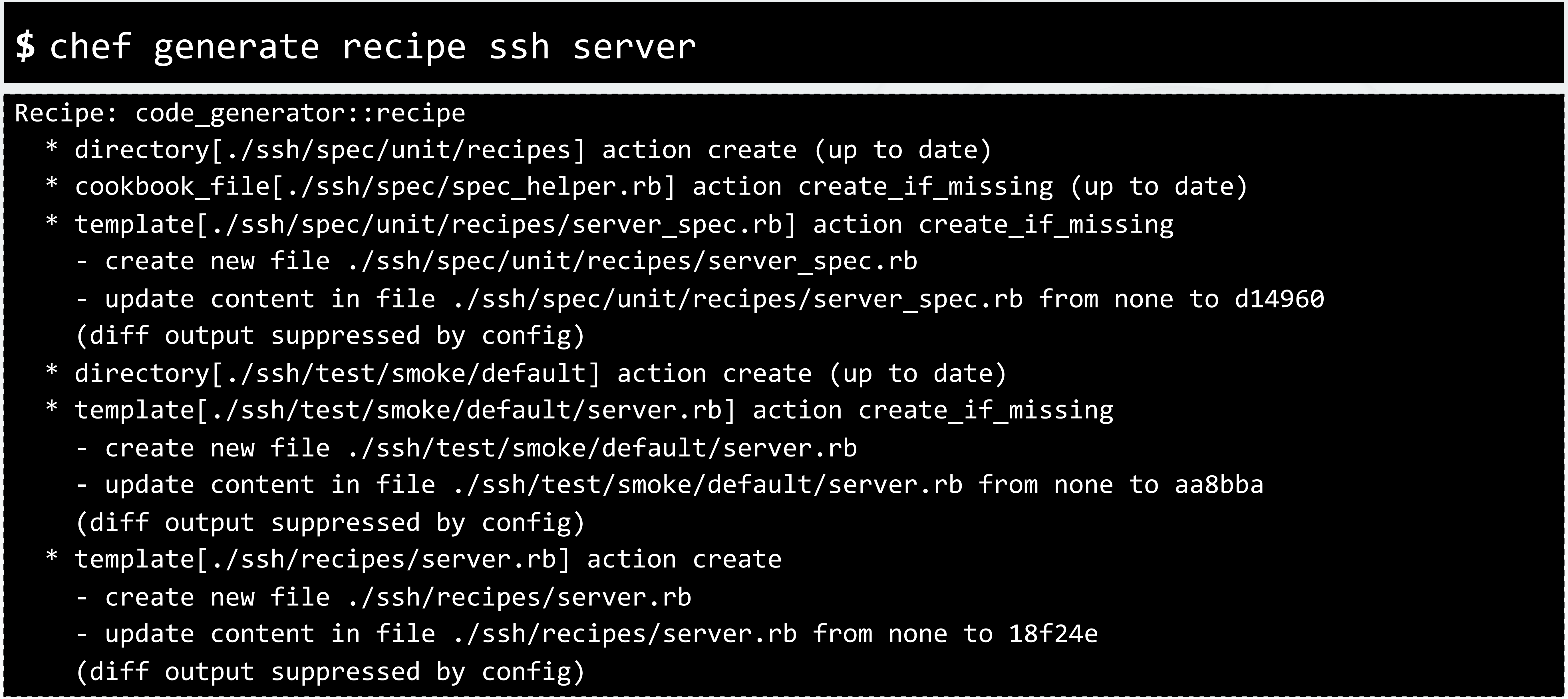
```
$ cd ~/cookbooks
```

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
```

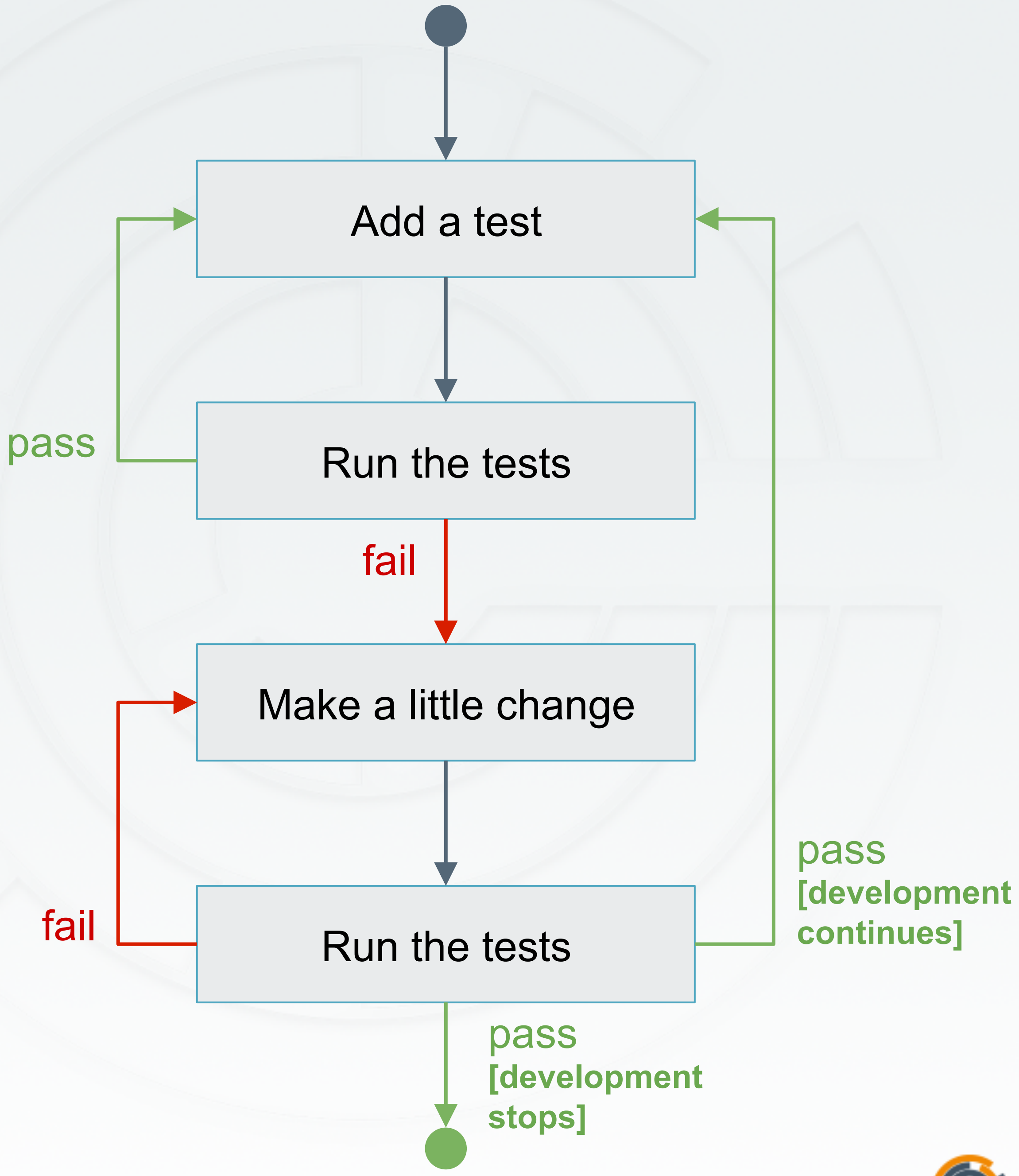
Remember…

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

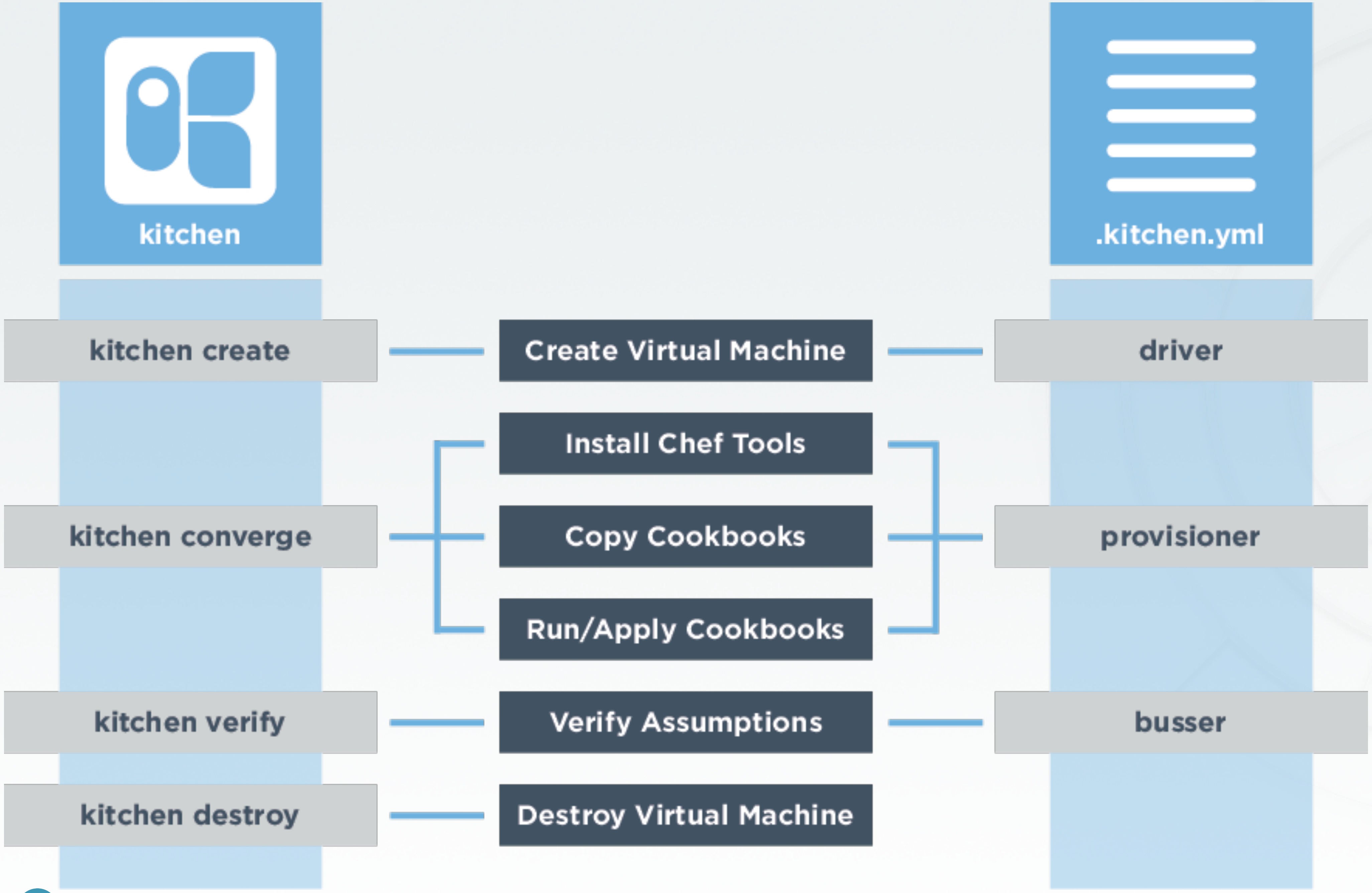
"Infrastructure as Code" should be tested like ANY other codebase.

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



kitchen

.kitchen.yml

kitchen create — Create Virtual Machine — driver

kitchen converge — Install Chef Tools, Copy Cookbooks, Run/Apply Cookbooks — provisioner

kitchen verify — Verify Assumptions — busser

kitchen destroy — Destroy Virtual Machine

amazon web services

Microsoft Azure

vmware®

openstack™

Test Kitchen Configuration (1 of 3)

`~/cookbooks/ssh/.kitchen.yml`

```diff
---
driver:
-  name: vagrant
+  name: docker

...
```

Test Kitchen Configuration (2 of 3)

~/cookbooks/ssh/.kitchen.yml

```diff
 ...

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

 ...
```

Test Kitchen Configuration (3 of 3)

~/cookbooks/ssh/.kitchen.yml

```diff
 suites:
-  - name: default
+  - name: server
     run_list:
-      - recipe[ssh::default]
+      - recipe[ssh::server]
     verifier:
       inspec_tests:
-        - test/smoke/default
+        - test/smoke/default/server.rb
     attributes:
```

Move to the cookbook's directory

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

List the kitchens

```
$ kitchen list
```

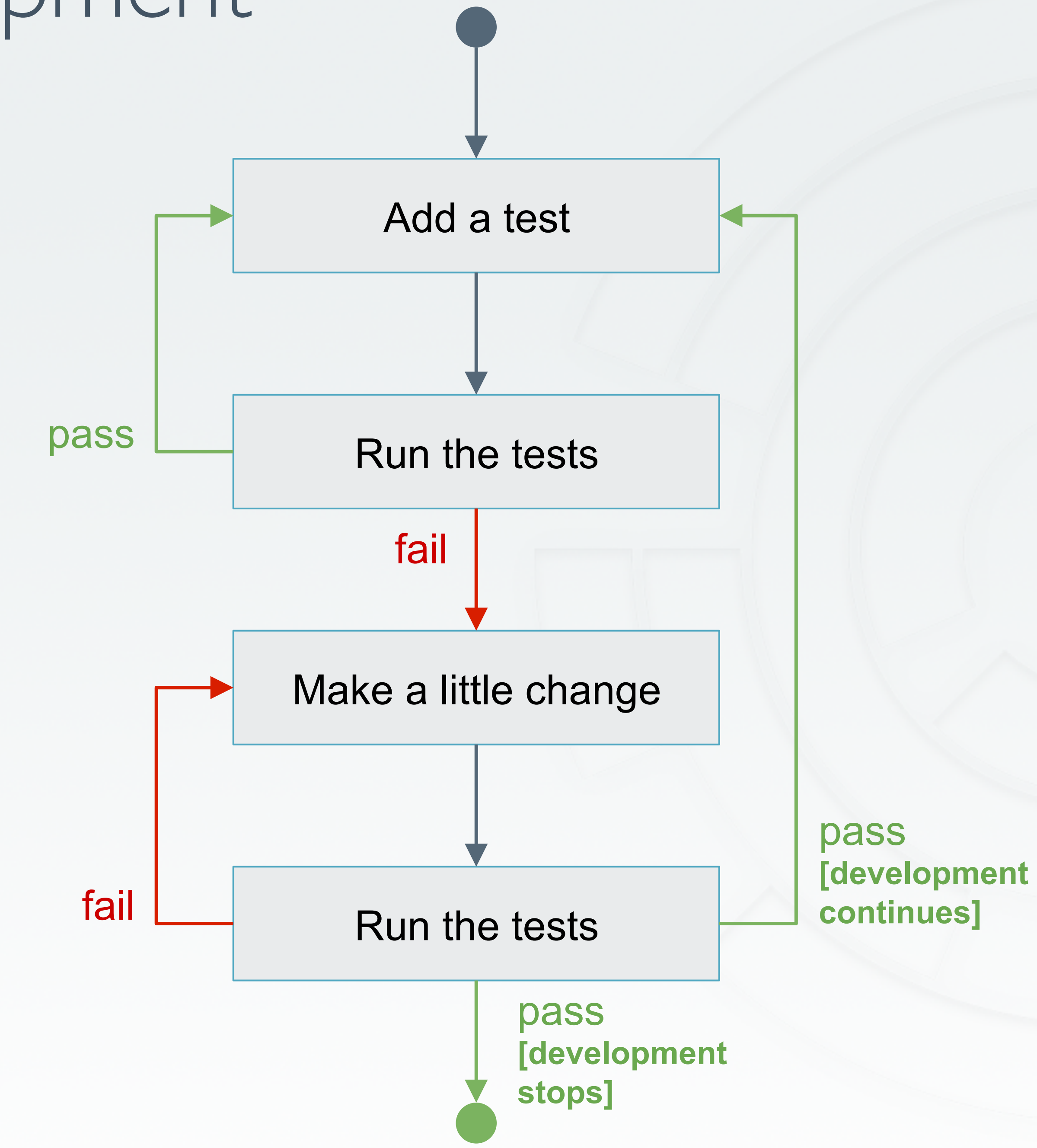
```
Instance            Driver  Provisioner  Verifier  Transport  Last Action    Last Error
server-centos-73    Docker  ChefZero     Inspec    Ssh        <Not Created>  <None>
```

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



Add Smoke Tests

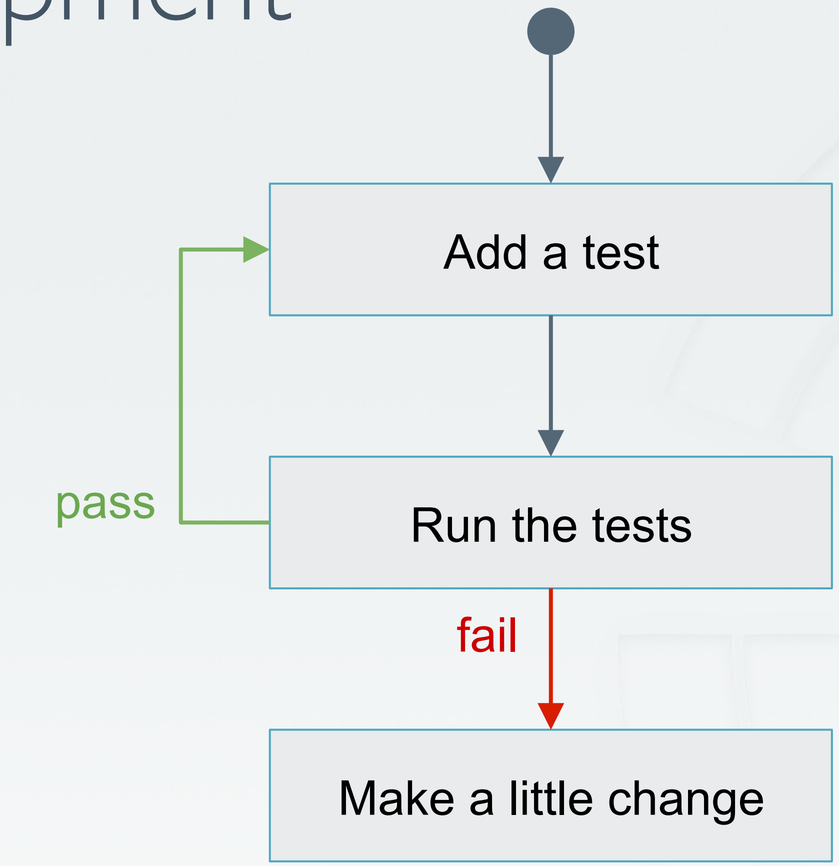
```
$ cp ~/profiles/ssh/controls/ssh.rb ~/cookbooks/ssh/test/smoke/default/server.rb
```

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


Add a test

Run the tests

pass

fail

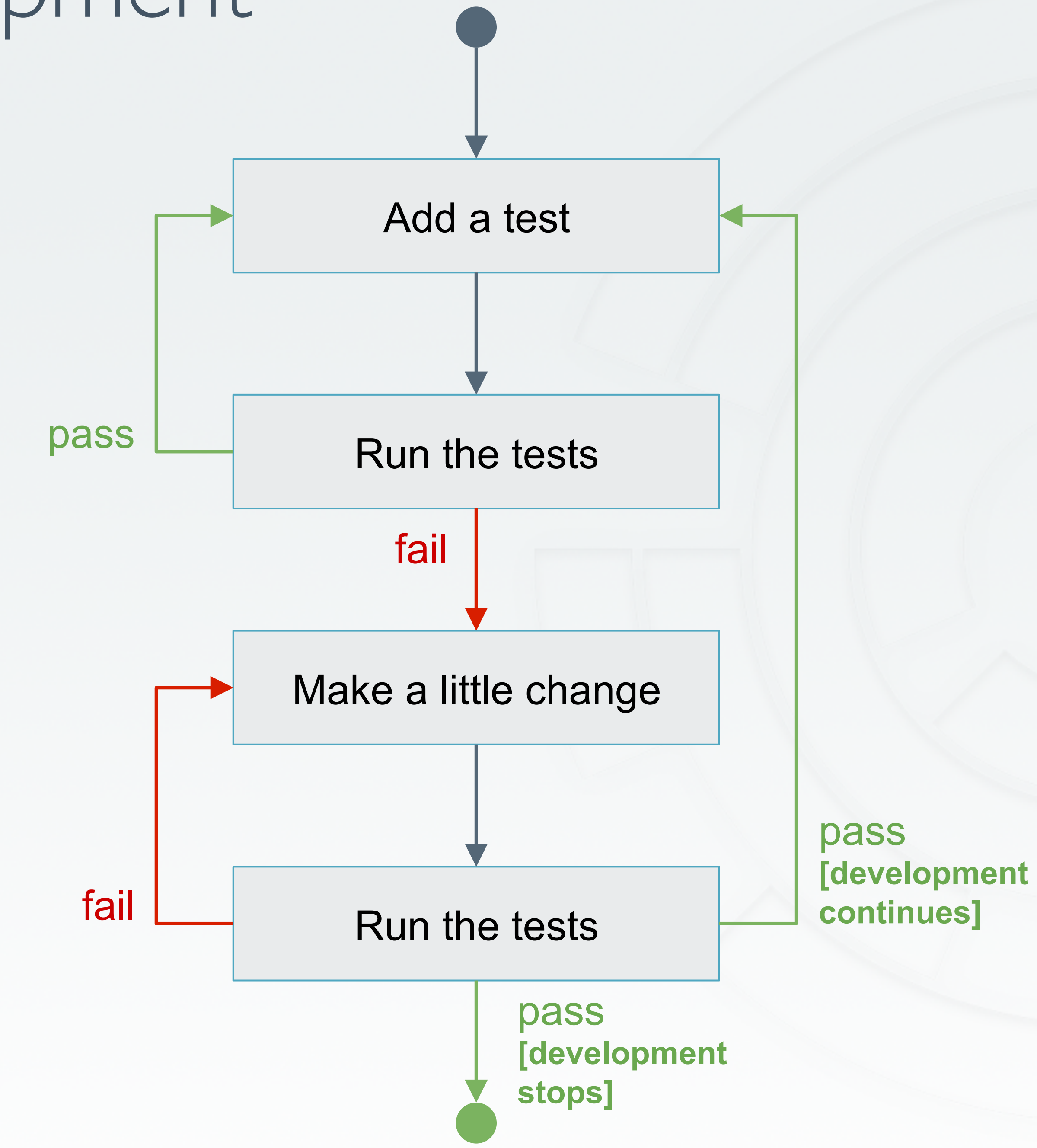
Make a little change

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



Converge

```
$ kitchen converge
```

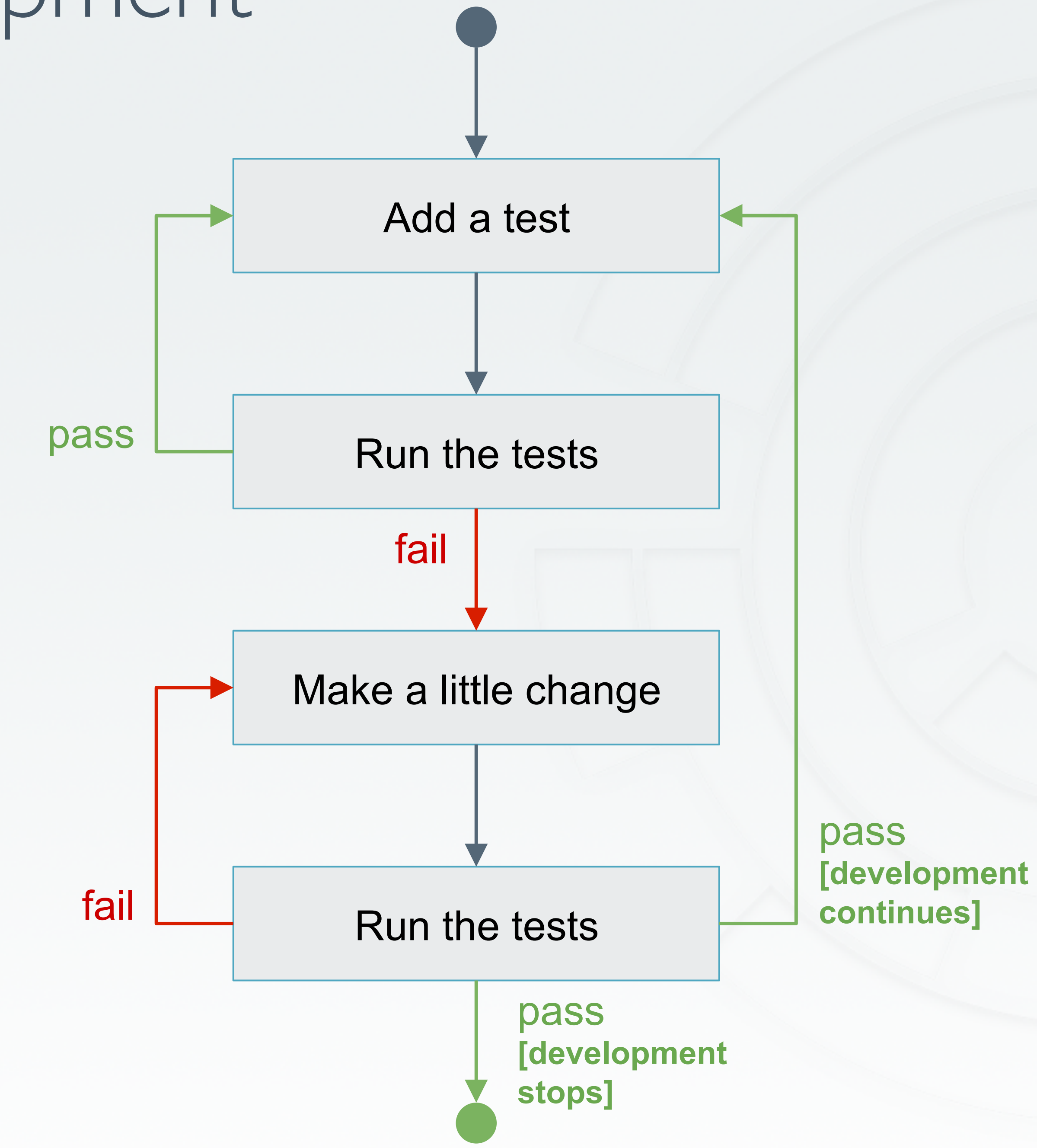
```
-----> Starting Kitchen (v1.15.0)
...
-----> Converging <server-centos-73>...
...
# The default requires explicit activation of protocol 1
-#Protocol 2
+Protocol 2

# 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



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>...
...
       Finished creating <server-centos-73> (0m0.60s).
-----> Converging <server-centos-73>...
...
```

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?

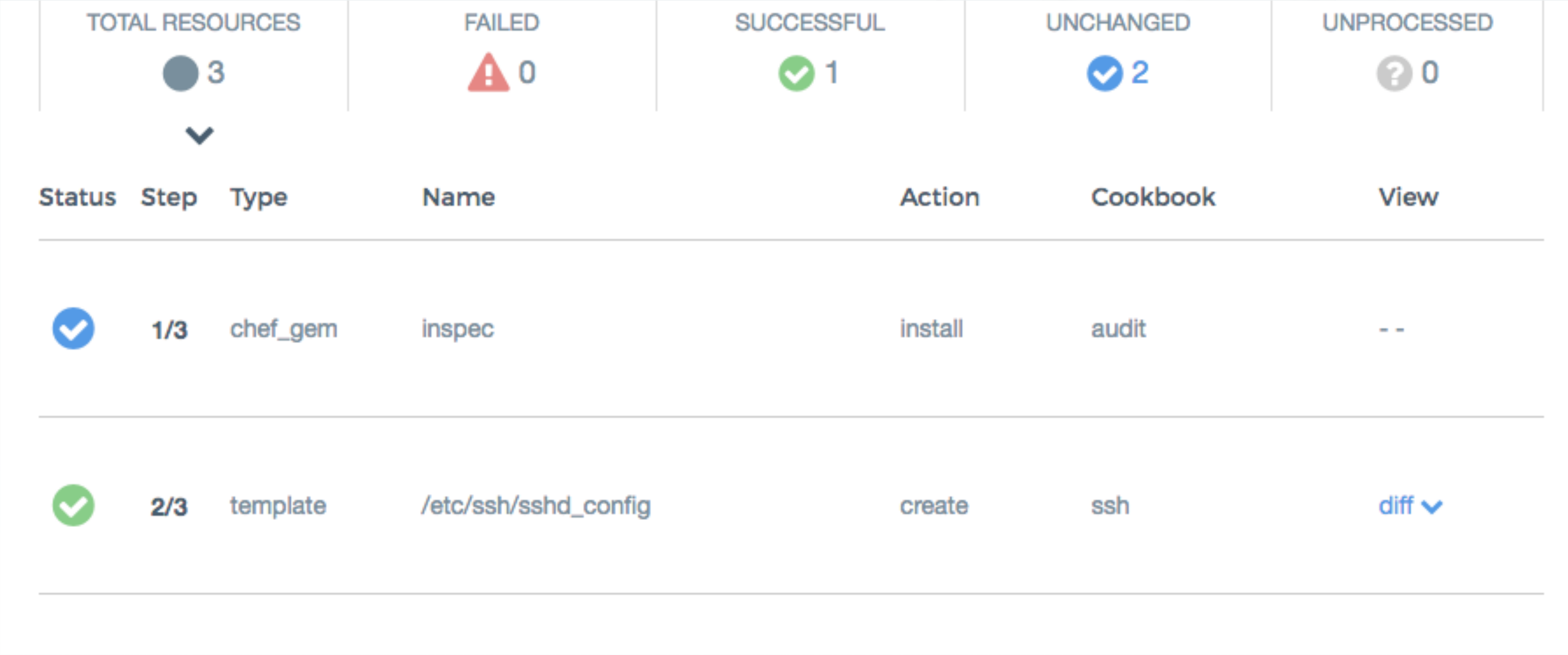
- Test-driven development cycle is complete
- Deploy the change

Remediate with Chef

```
$ sudo chef-client --local-mode -j config.json -r "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
```

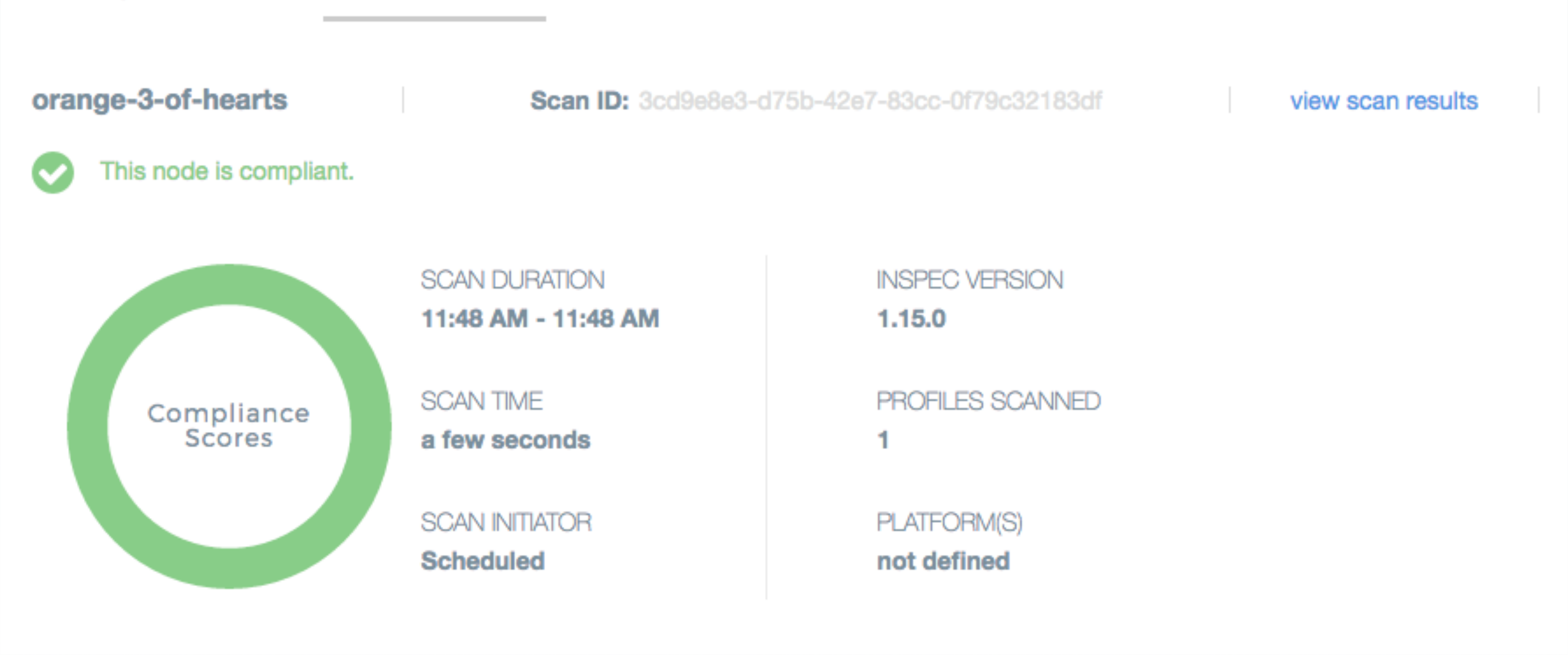
Verify Converge Status in Automate



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	diff

Verify Compliance Status in Automate



orange-3-of-hearts | **Scan ID:** 3cd9e8e3-d75b-42e7-83cc-0f79c32183df | view scan results

✓ This node is compliant.

SCAN DURATION
11:48 AM - 11:48 AM

SCAN TIME
a few seconds

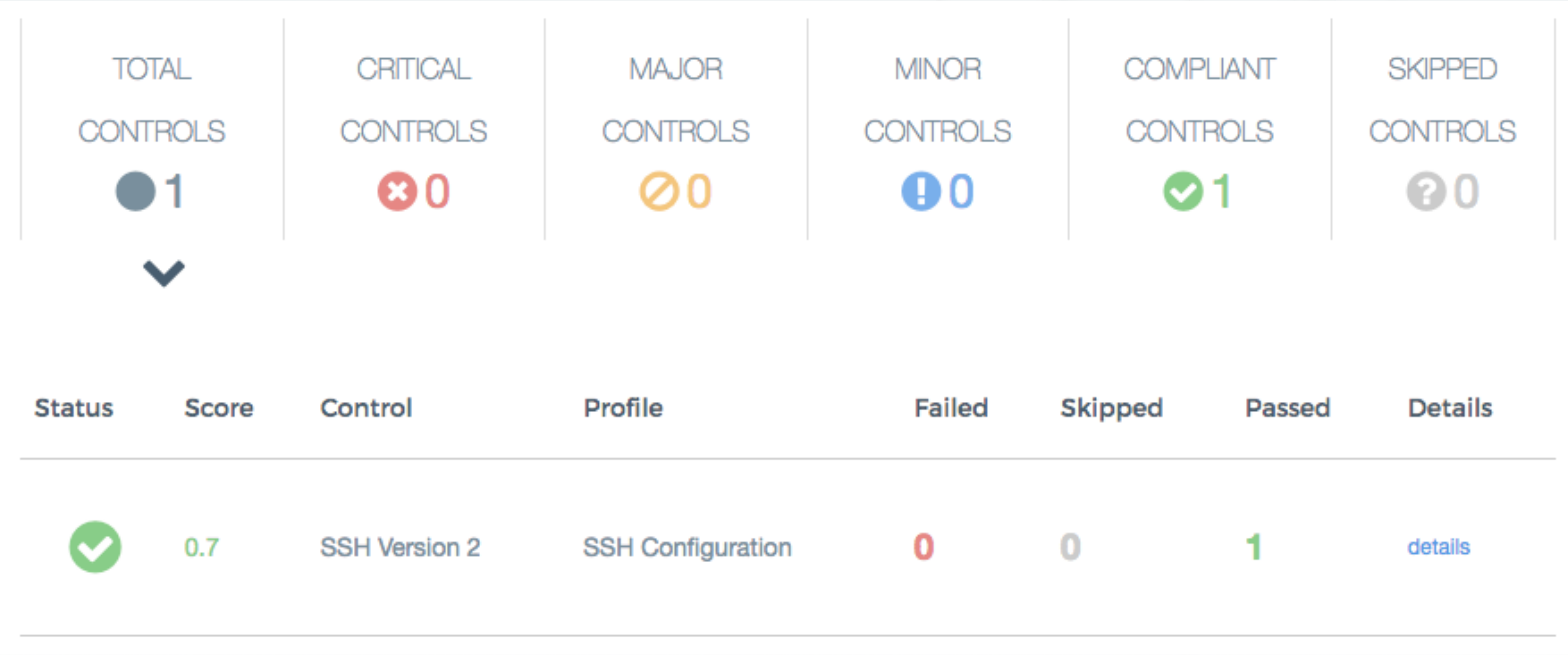
SCAN INITIATOR
Scheduled

INSPEC VERSION
1.15.0

PROFILES SCANNED
1

PLATFORM(S)
not defined

Verify Compliance Status in Automate



TOTAL CONTROLS	CRITICAL CONTROLS	MAJOR CONTROLS	MINOR CONTROLS	COMPLIANT CONTROLS	SKIPPED CONTROLS
● 1	✖ 0	⊘ 0	! 0	✓ 1	? 0

Status	Score	Control	Profile	Failed	Skipped	Passed	Details
✓	0.7	SSH Version 2	SSH Configuration	0	0	1	details