Continuous Compliance

Chef Automate and InSpec Profiles

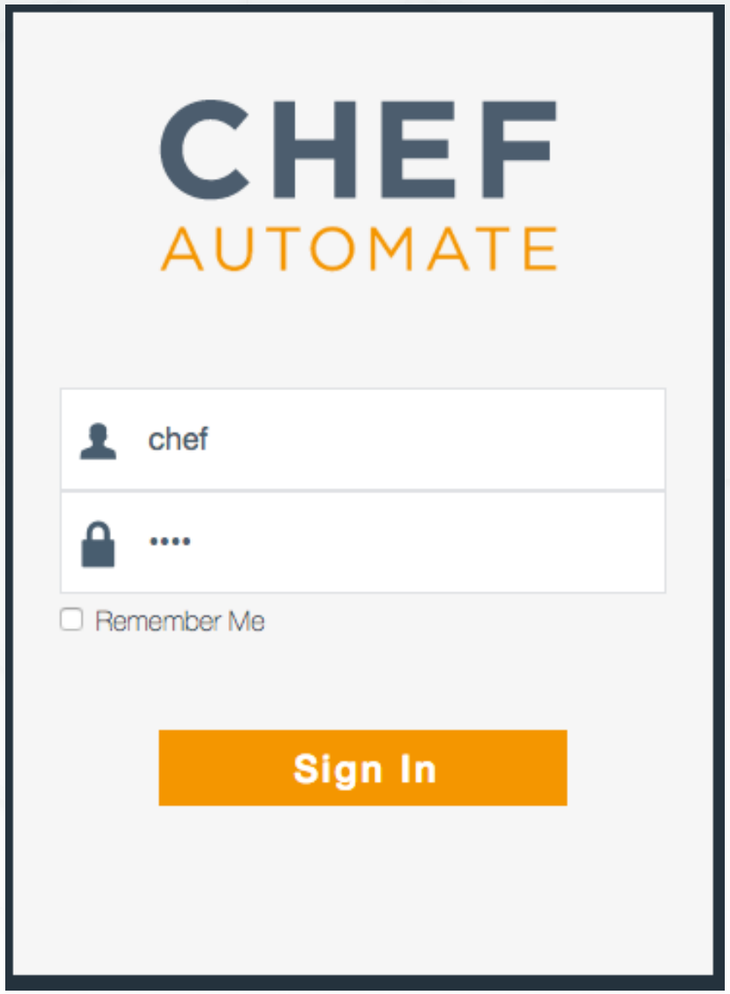
INSPEC

CHEF

Login to Chef Automate

- https://informatica-compliance-workshop.chefdemo.net
- Uses a self-signed certificate in this lab

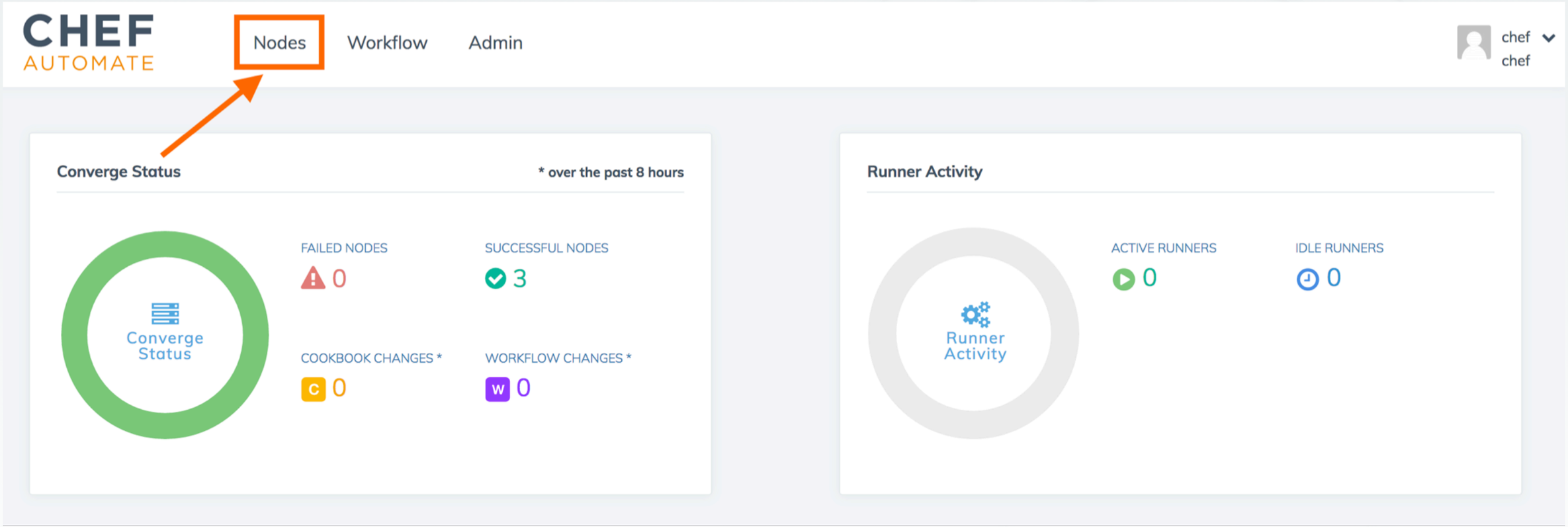
- Username: `chef`
- Password: `chef`



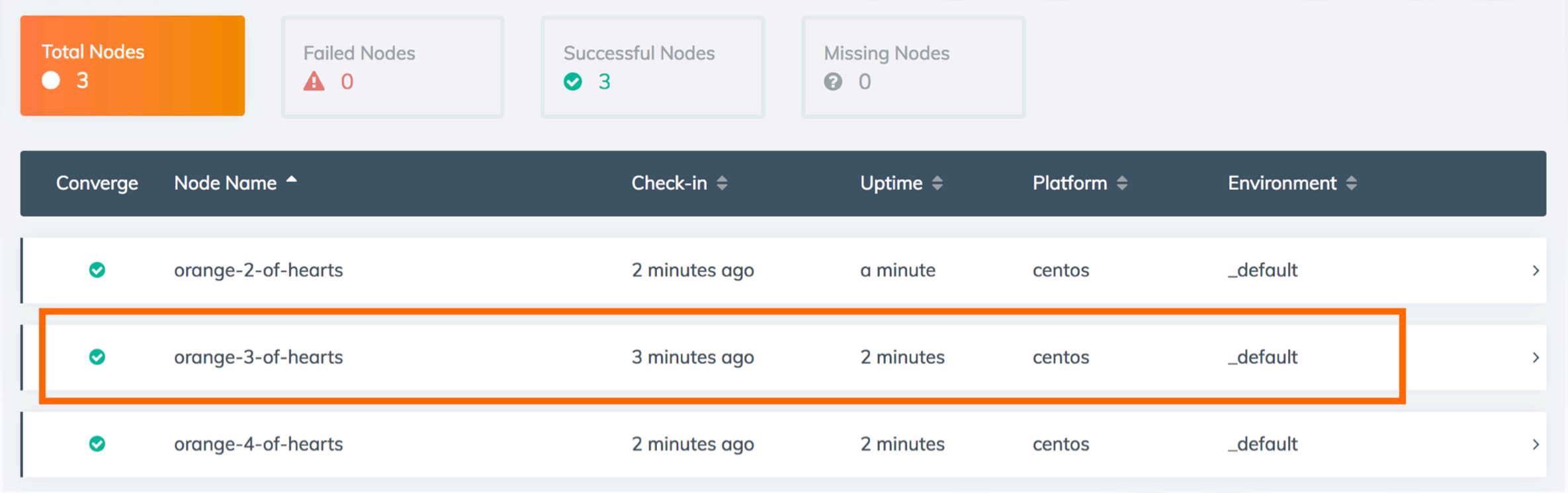
INSPEC

CHEF

Browse to your node



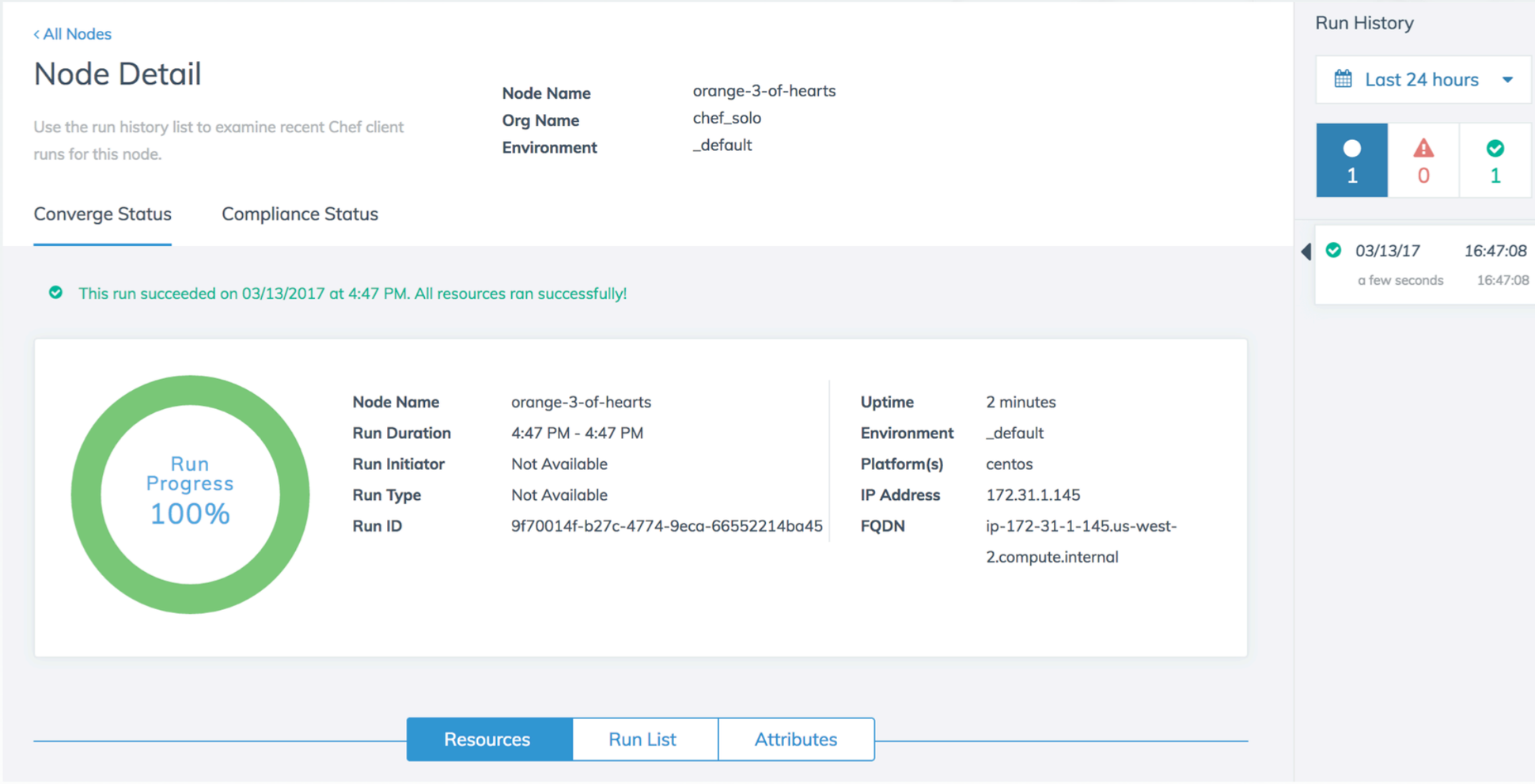
Browse to your node



INSPEC

CHEF

View details of your node



INSPEC

CHEF

View details of your node

Node Name	orange-3-of-hearts
Run Duration	4:47 PM - 4:47 PM
Run Initiator	Not Available
Run Type	Not Available
Run ID	9f70014f-b27c-4774-9eca-66552214ba45

Uptime	2 minutes
Environment	_default
Platform(s)	centos
IP Address	172.31.1.145
FQDN	ip-172-31-1-145.us-west-2.compute.internal

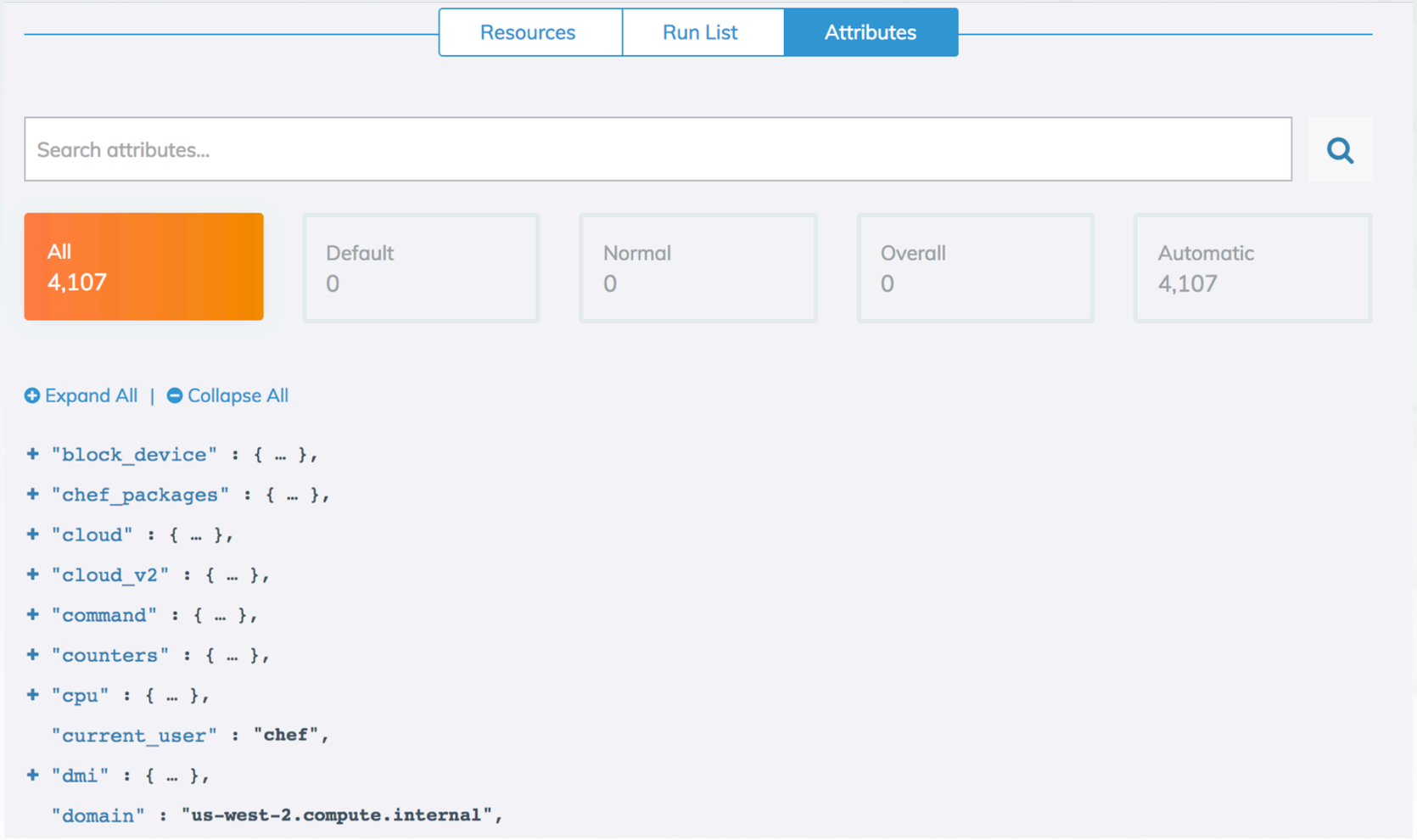
Resources | Run List | Attributes

Roles	Cookbooks	Recipes	Failed	Succeeded
0	0	0	0	0

INSPEC

CHEF

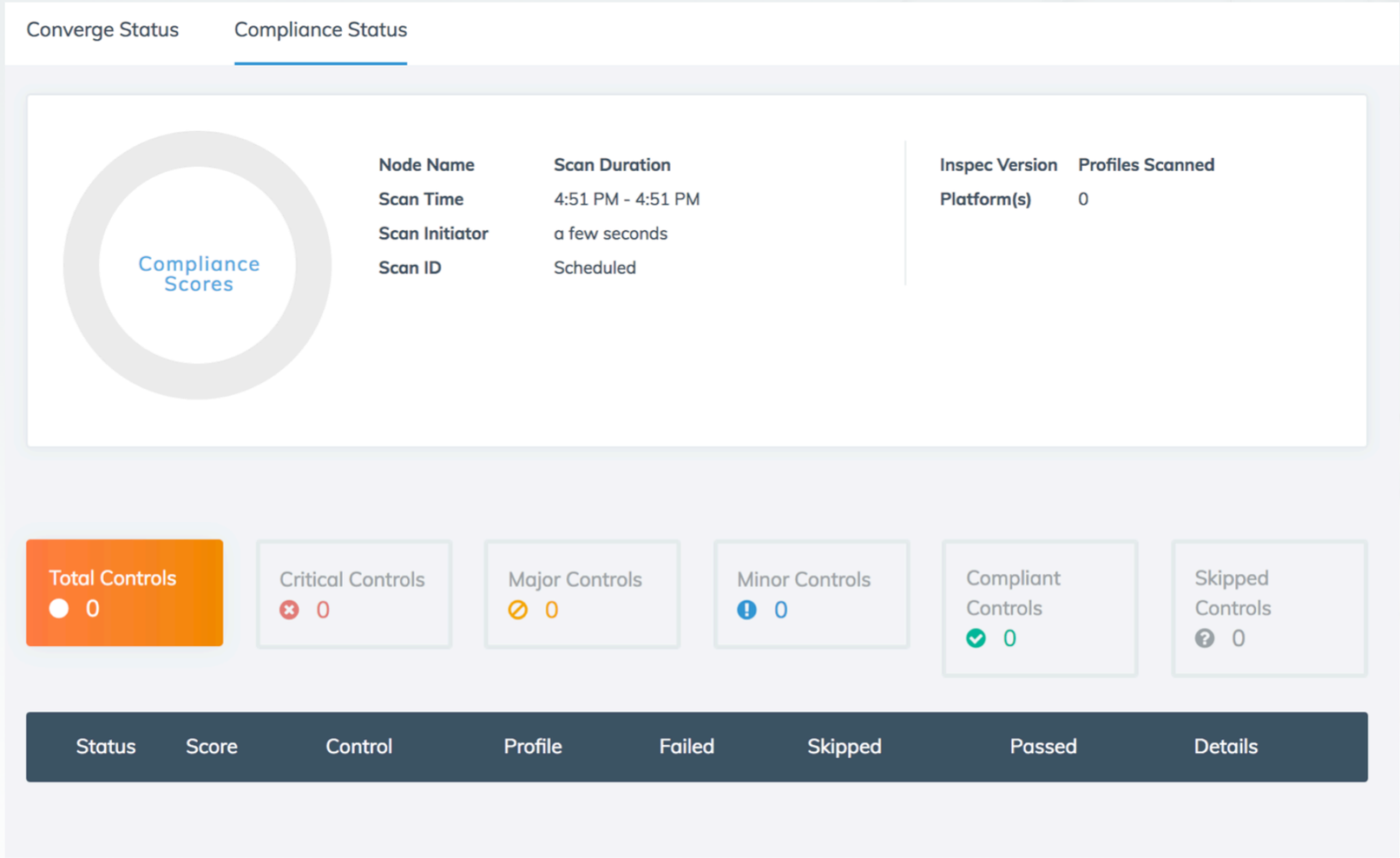
View details of your node



INSPEC

CHEF

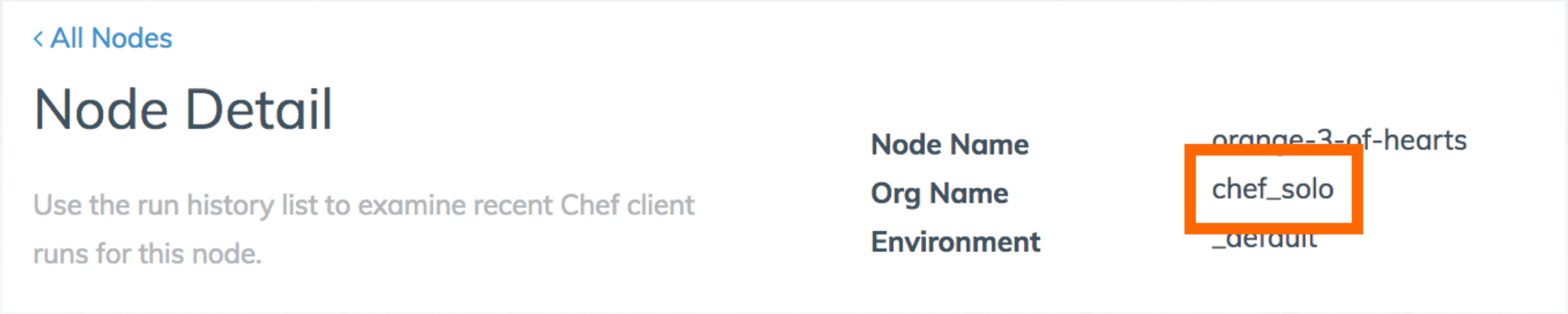
View details of your node



INSPEC

CHEF

The node uses chef solo



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

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

Go home

```
$ cd ~
```

INSPEC

CHEF

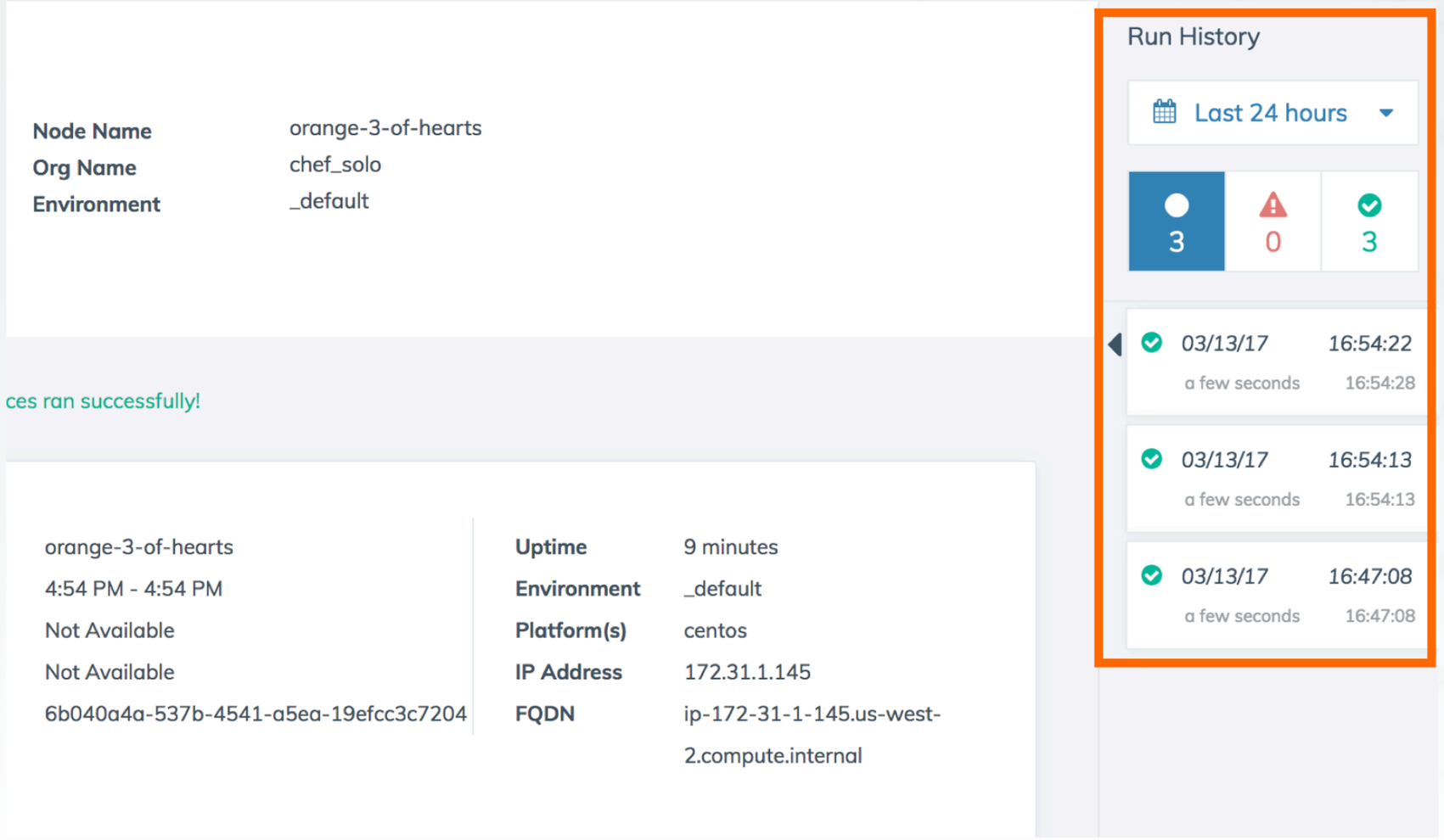
Run chef-client in local mode

```
$ 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



INSPEC

CHEF

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

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

Resources | Run List | Attributes

Total Resources	Failed	Successful	Unchanged	Unprocessed
2	0	1	1	0

INSPEC

CHEF

Check the converge status in Automate

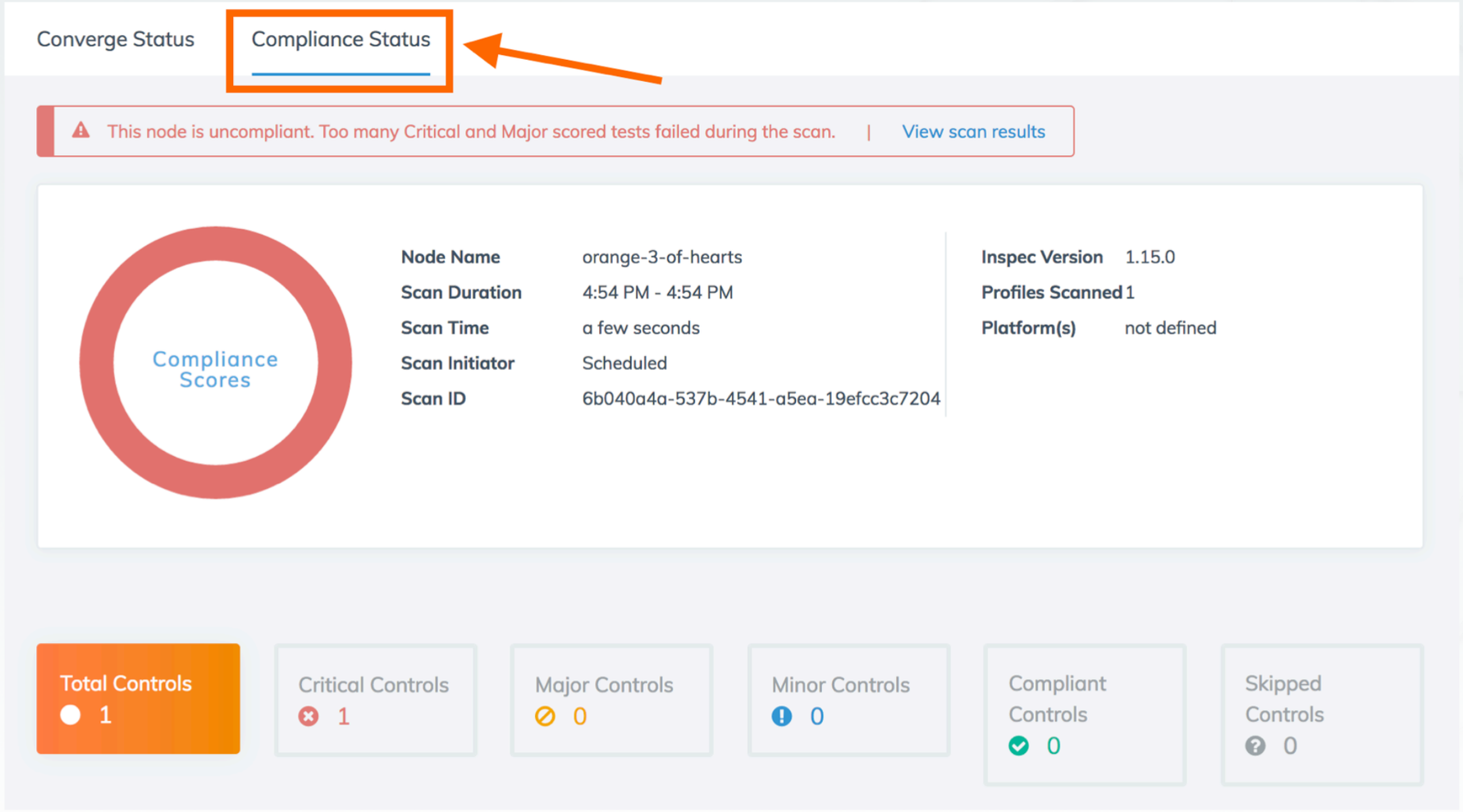
Total Resources	Failed	Successful	Unchanged	Unprocessed
2	0	1	1	0

Status	Step	Type	Name	Action	Cookbook	View
✓	1/2	chef_gem	inspec	install	audit	- -
✓	2/2	chef_gem	inspec	install	audit	- -

INSPEC

CHEF

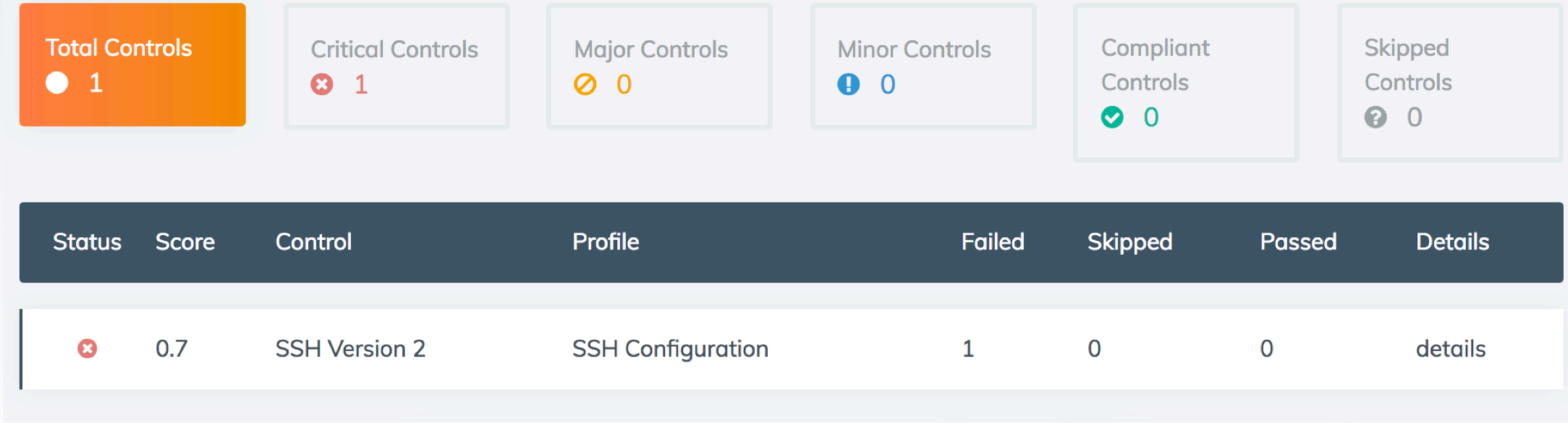
Check the compliance status in Automate



INSPEC

CHEF

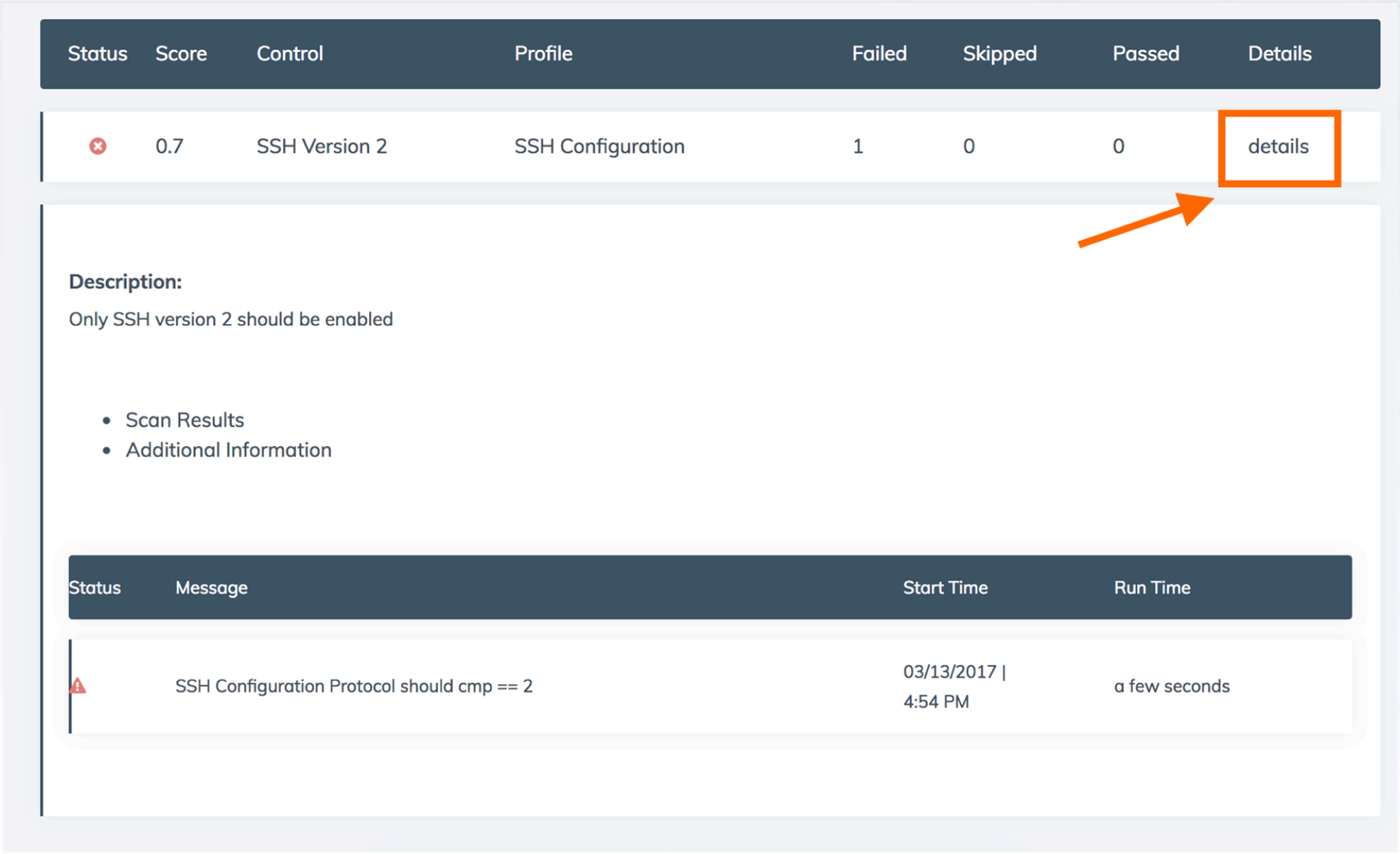
Check the compliance status in Automate



INSPEC

CHEF

View details of the failing control



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

Description:

Only SSH version 2 should be enabled

- Scan Results
- Additional Information

Status	Message	Start Time	Run Time
⚠	SSH Configuration Protocol should cmp == 2	03/13/2017 | 4:54 PM	a few seconds

INSPEC

CHEF

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
```

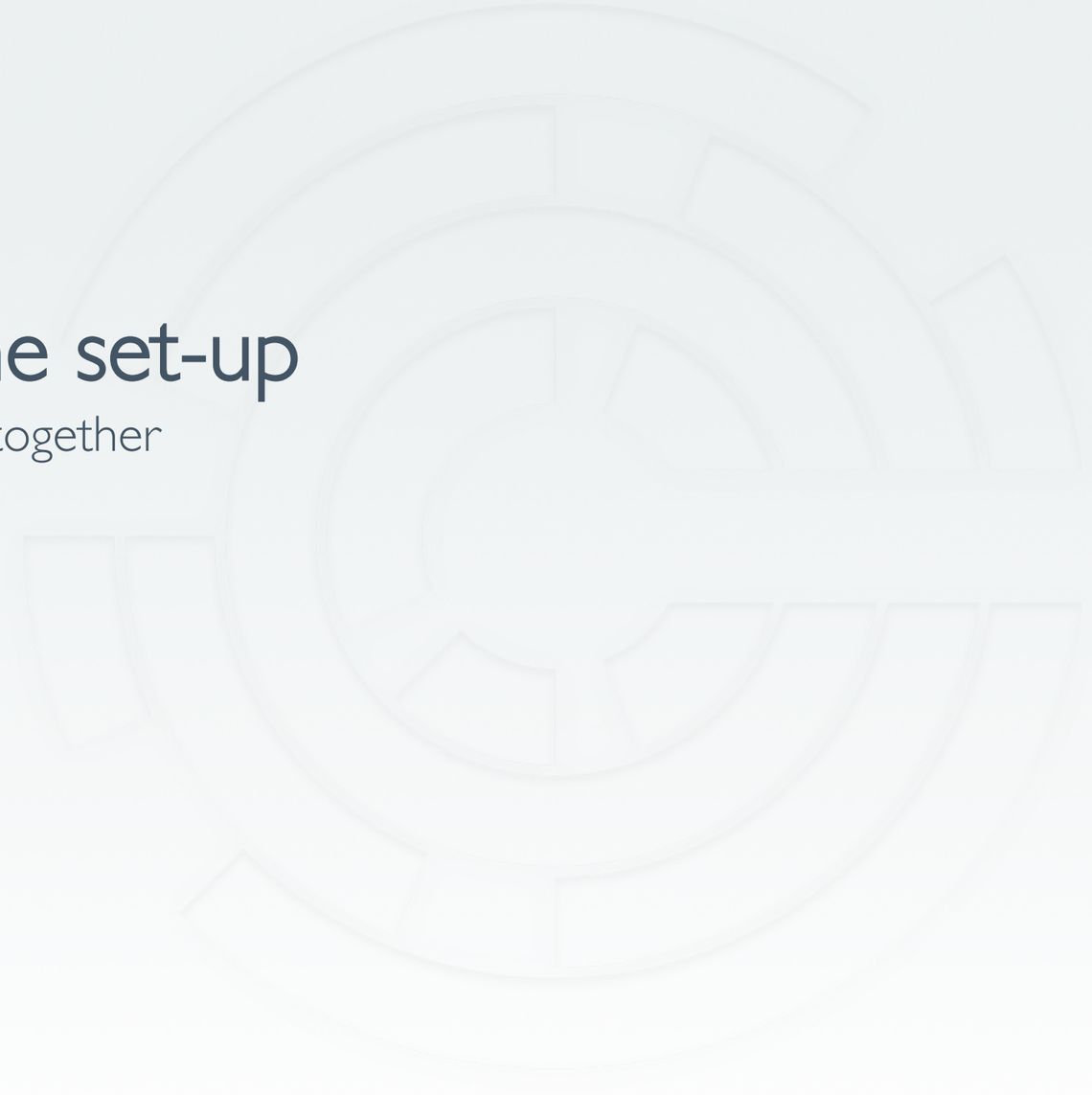
Tags:

INSPEC

CHEF

Review the set-up

tying it all together



INSPEC

CHEF

Go home

```
$ cd ~
```

INSPEC

CHEF

List contents

```
$ ls
```

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

INSPEC

CHEF

List cookbooks

```
$ ls cookbooks
```

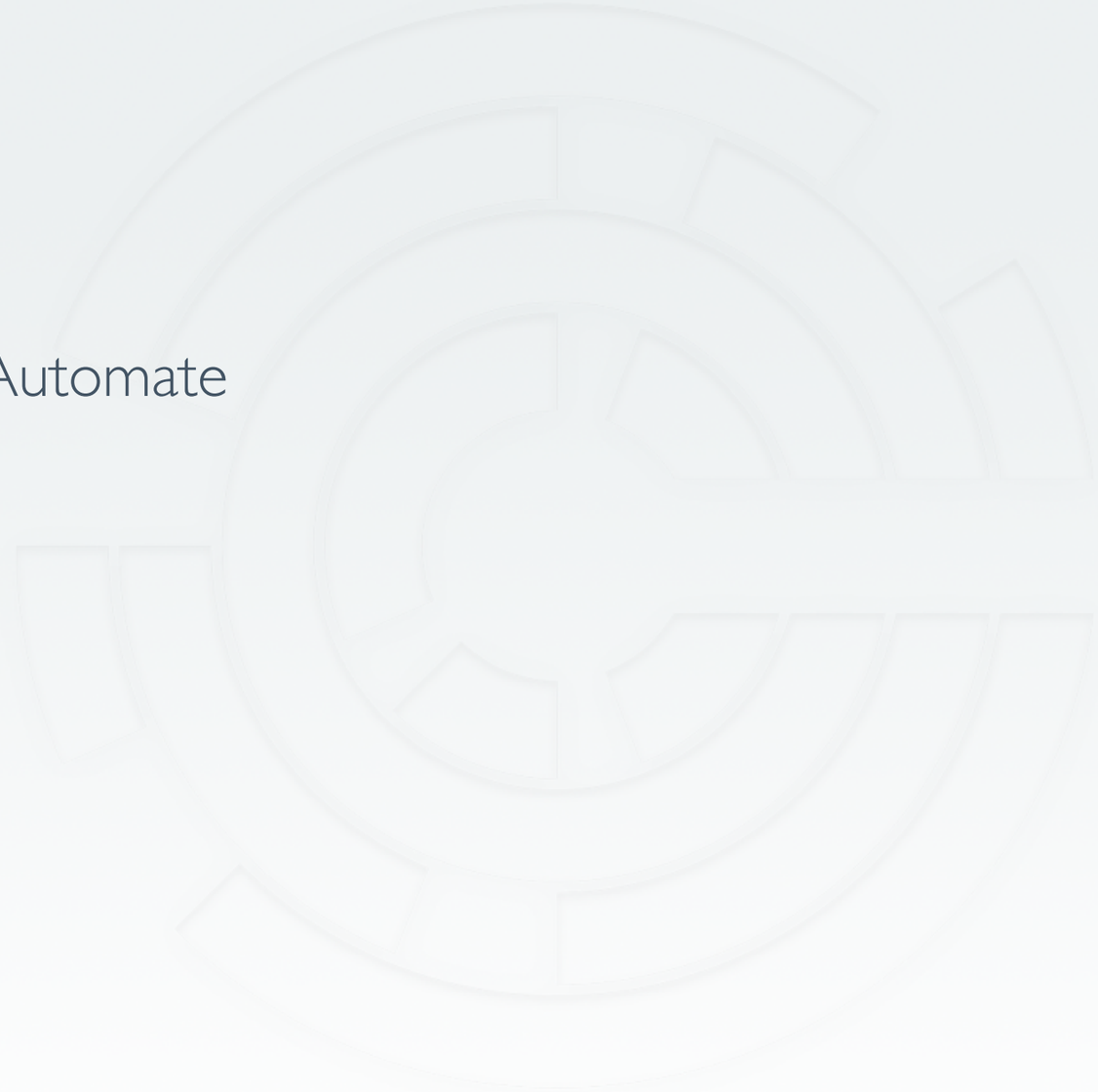
```
audit  compat_resource
```

INSPEC

CHEF

Audit Cookbook

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



INSPEC

CHEF

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://

  ×  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
```

INSPEC

CHEF

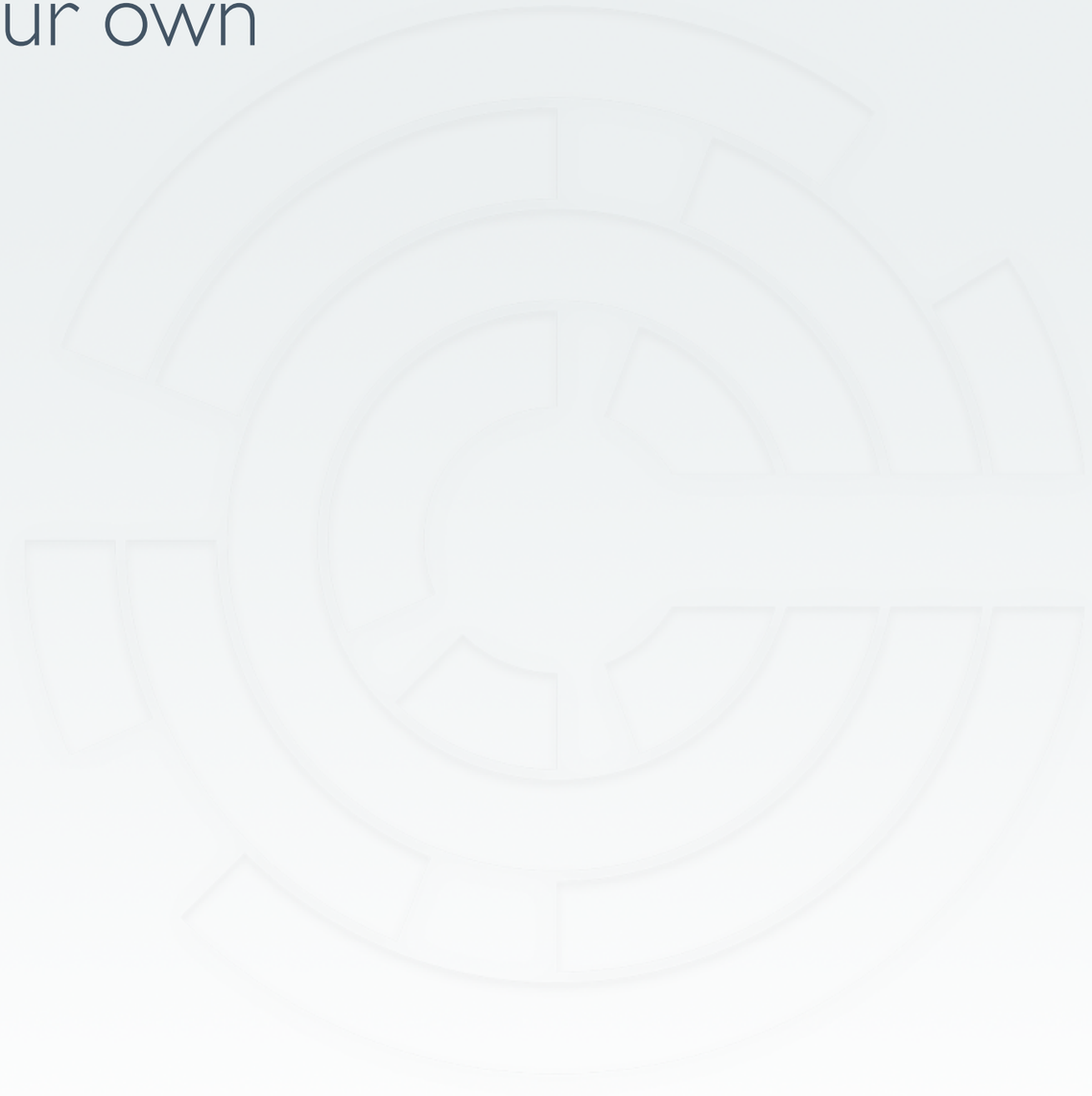
Next Steps

- 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

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

INSPEC

CHEF

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

INSPEC

CHEF