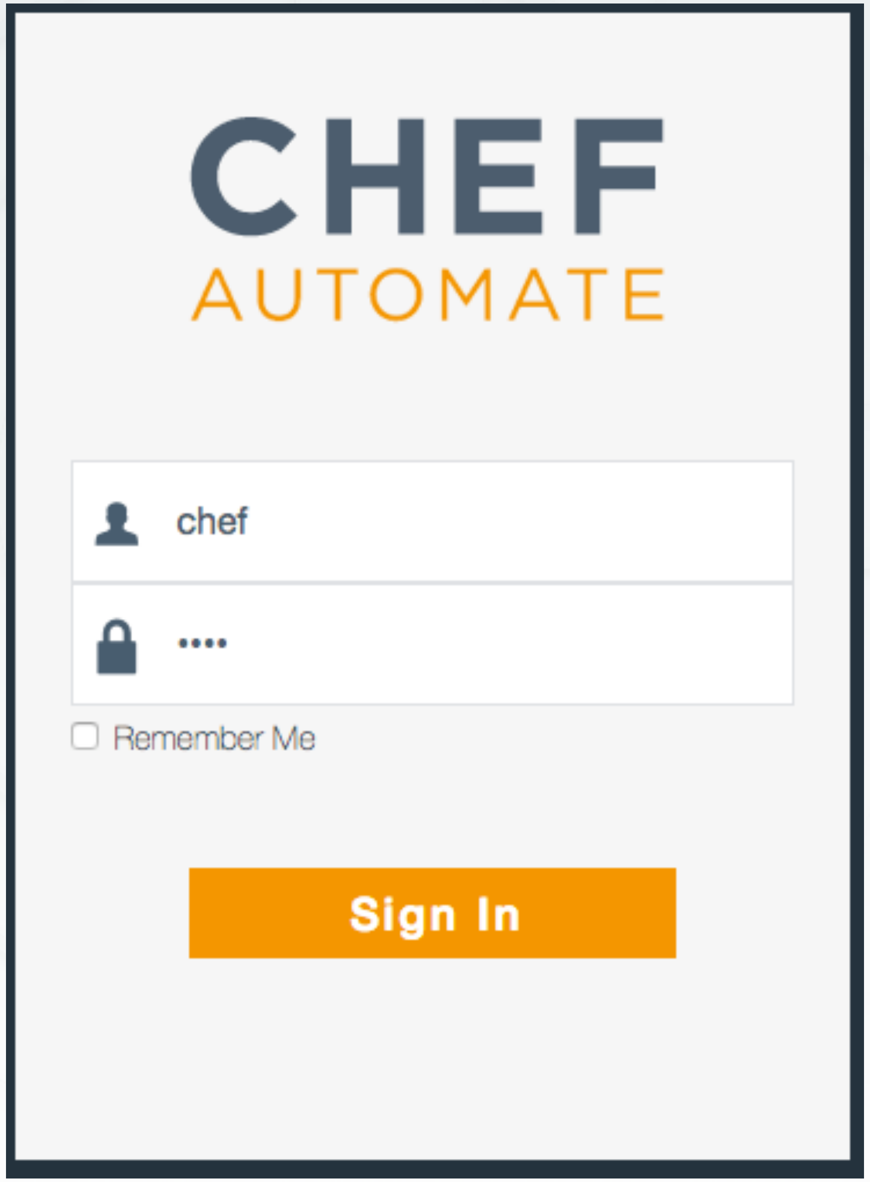
Continuous Compliance

Chef Automate and InSpec Profiles

Login to Chef Automate

- URL_OF_AUTOMATE_SERVER
- Uses a self-signed certificate in this lab

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



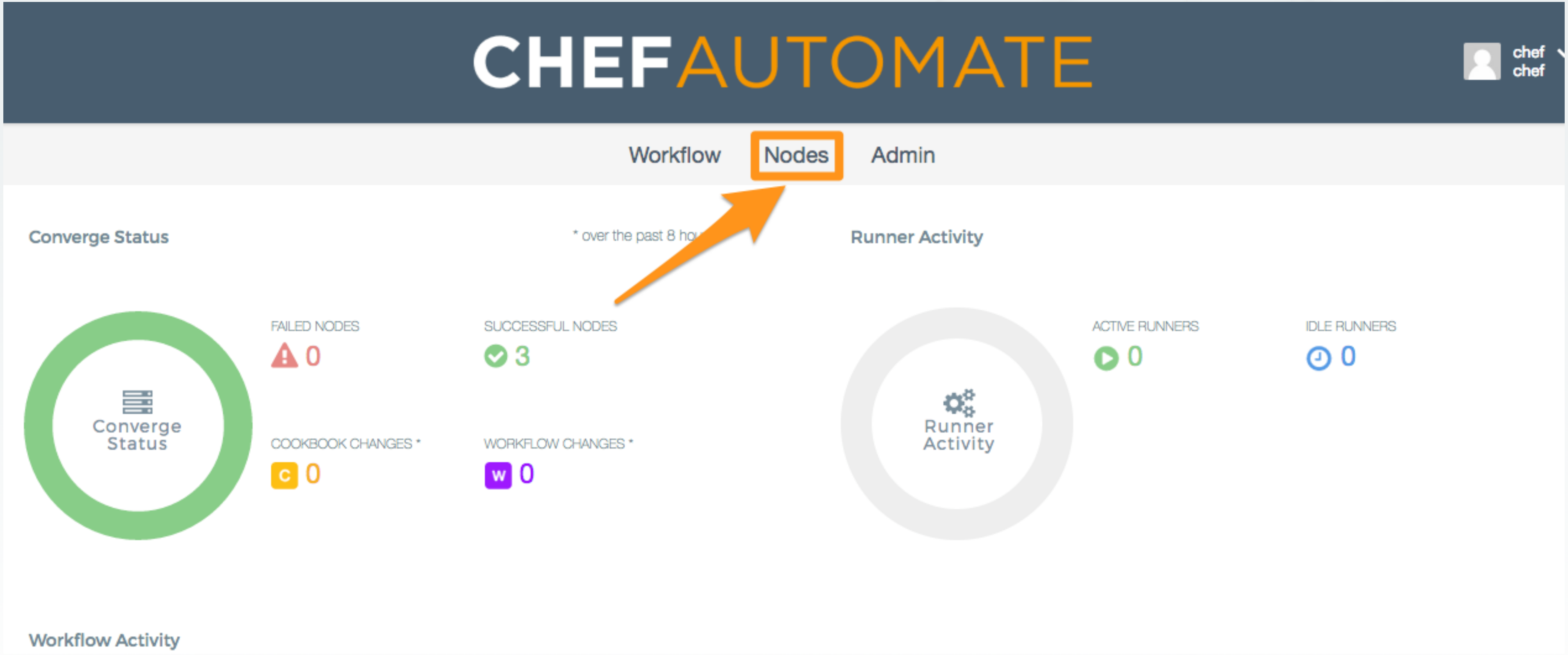
CHEF AUTOMATE

chef

••••

□ Remember Me

Browse to your node



Converge Status

* over the past 8 ho

Runner Activity

FAILED NODES
0

SUCCESSFUL NODES
3

COOKBOOK CHANGES *
C 0

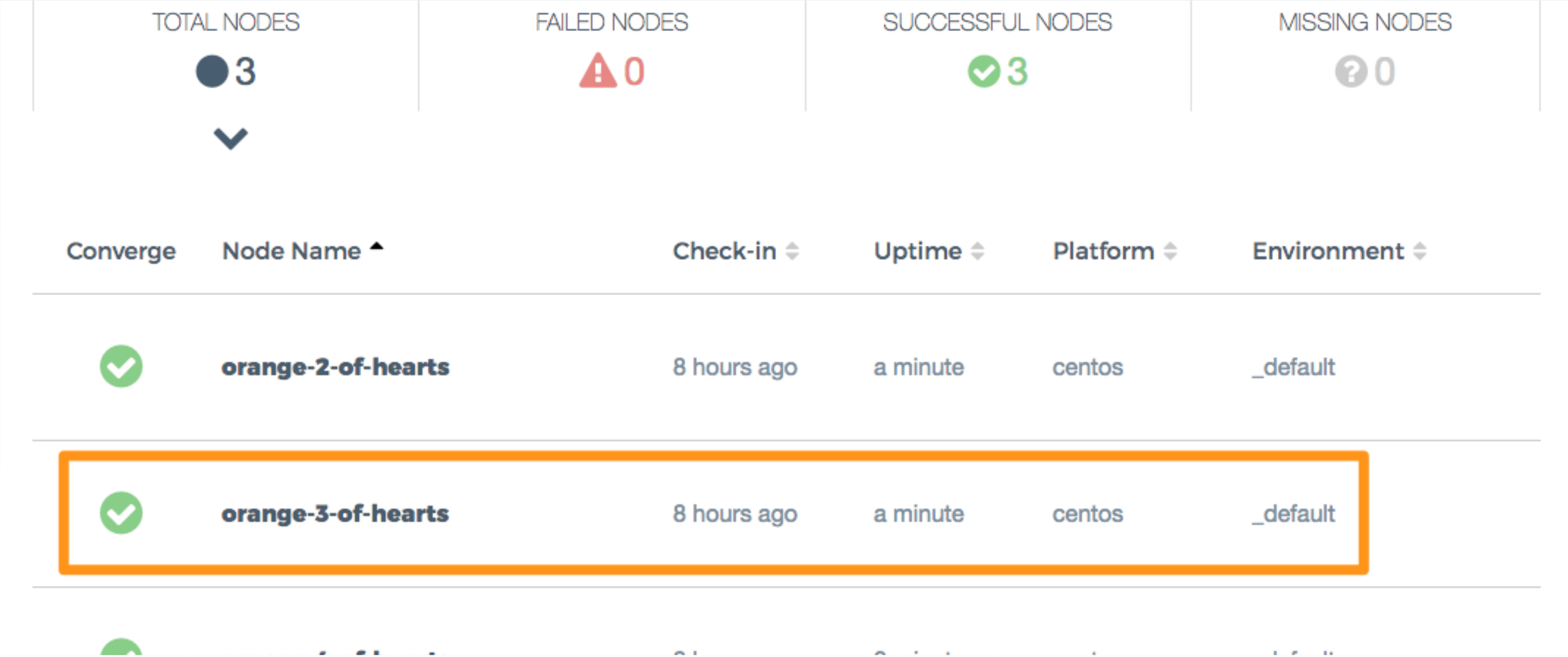
WORKFLOW CHANGES *
W 0

ACTIVE RUNNERS
0

IDLE RUNNERS
0

Workflow Activity

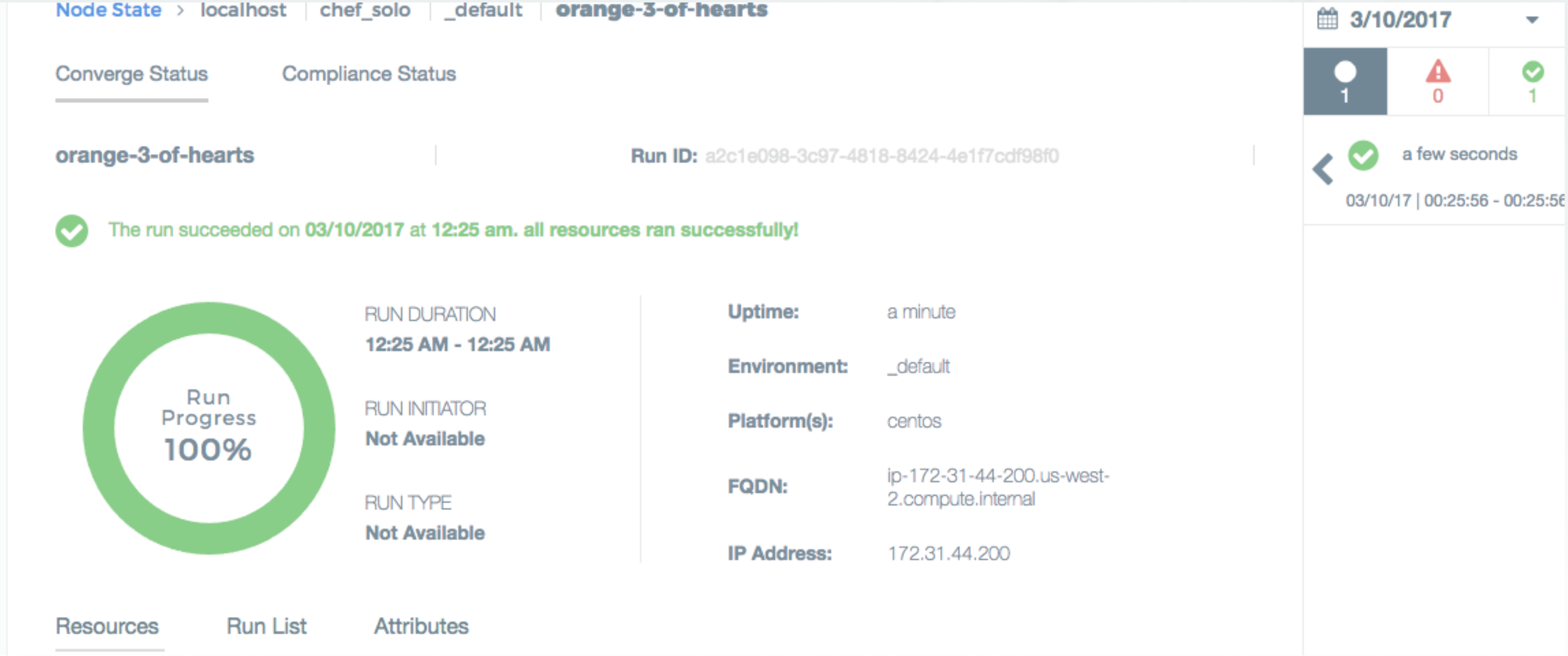
Browse to your node



TOTAL NODES	FAILED NODES	SUCCESSFUL NODES	MISSING NODES
● 3	⚠ 0	✓ 3	? 0

Converge	Node Name ▲	Check-in ⇕	Uptime ⇕	Platform ⇕	Environment ⇕
✓	**orange-2-of-hearts**	8 hours ago	a minute	centos	_default
✓	**orange-3-of-hearts**	8 hours ago	a minute	centos	_default

View details of your node



Node State › localhost | chef_solo | _default | orange-3-of-hearts

📅 3/10/2017

● 1 | ⚠ 0 | ✓ 1

Converge Status | Compliance Status

orange-3-of-hearts | Run ID: a2c1e098-3c97-4818-8424-4e1f7cdf98f0

‹ ✓ a few seconds
03/10/17 | 00:25:56 - 00:25:56

✓ The run succeeded on 03/10/2017 at 12:25 am. all resources ran successfully!

Run Progress 100%

RUN DURATION
12:25 AM - 12:25 AM

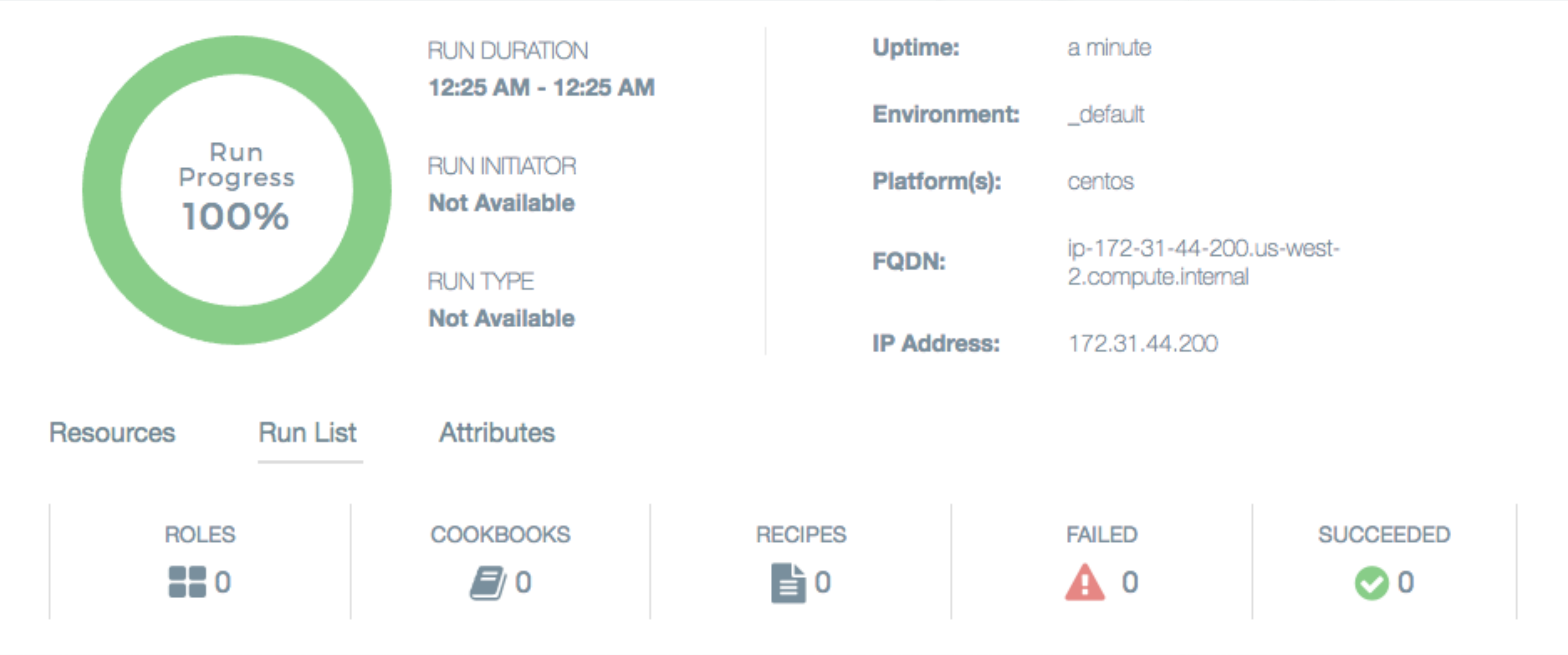
RUN INITIATOR
Not Available

RUN TYPE
Not Available

Uptime:	a minute
Environment:	_default
Platform(s):	centos
FQDN:	ip-172-31-44-200.us-west-2.compute.internal
IP Address:	172.31.44.200

Resources | Run List | Attributes

View details of your node



RUN DURATION
12:25 AM - 12:25 AM

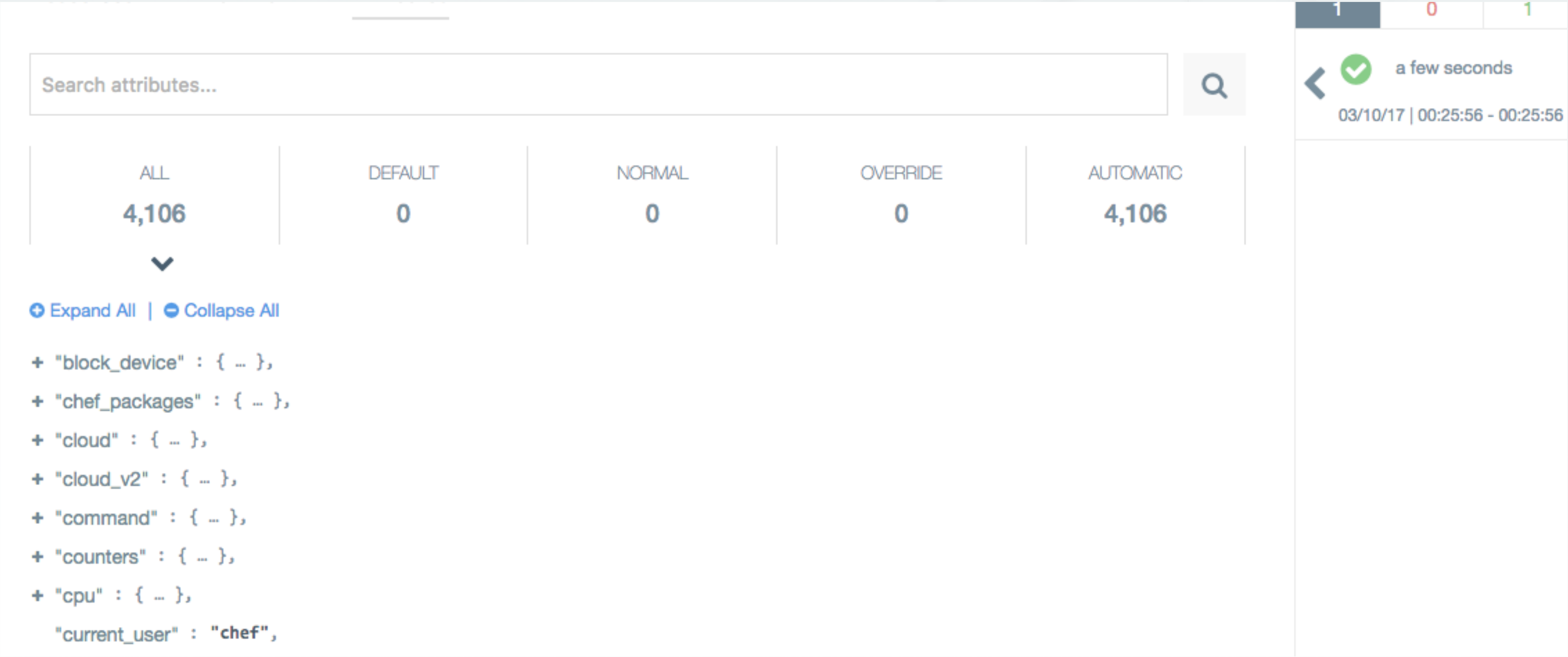
RUN INITIATOR
Not Available

RUN TYPE
Not Available

Uptime:	a minute
Environment:	_default
Platform(s):	centos
FQDN:	ip-172-31-44-200.us-west-2.compute.internal
IP Address:	172.31.44.200

ROLES	COOKBOOKS	RECIPES	FAILED	SUCCEEDED
0	0	0	0	✓ 0

View details of your node



✓ a few seconds

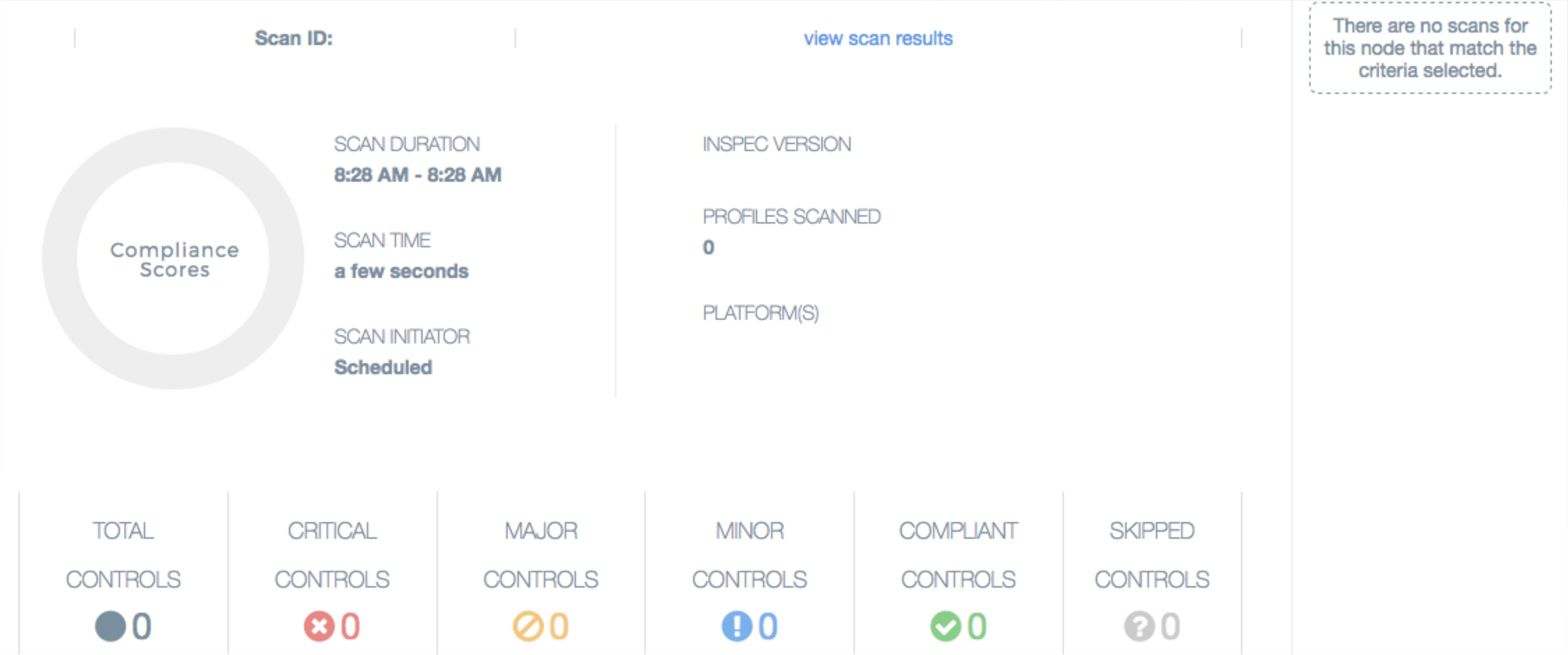
03/10/17 | 00:25:56 - 00:25:56

Search attributes...

ALL	DEFAULT	NORMAL	OVERRIDE	AUTOMATIC
4,106	0	0	0	4,106

```
+ "block_device" : { … },
+ "chef_packages" : { … },
+ "cloud" : { … },
+ "cloud_v2" : { … },
+ "command" : { … },
+ "counters" : { … },
+ "cpu" : { … },
  "current_user" : "chef",
```

View details of your node



Scan ID:

view scan results

There are no scans for this node that match the criteria selected.

Compliance Scores

SCAN DURATION
8:28 AM - 8:28 AM

SCAN TIME
a few seconds

SCAN INITIATOR
Scheduled

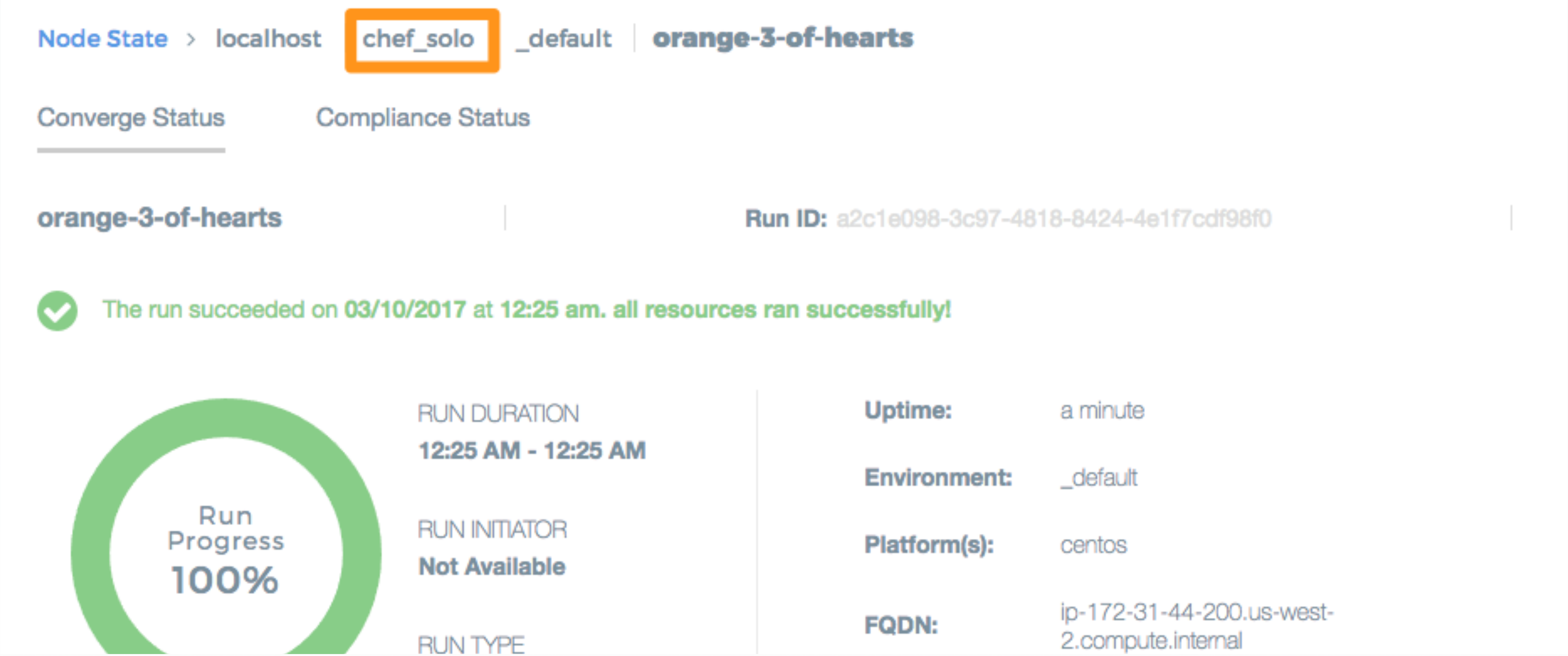
INSPEC VERSION

PROFILES SCANNED
0

PLATFORM(S)

TOTAL CONTROLS	CRITICAL CONTROLS	MAJOR CONTROLS	MINOR CONTROLS	COMPLIANT CONTROLS	SKIPPED CONTROLS
● 0	⊗ 0	⊘ 0	❗ 0	✓ 0	? 0

The node uses chef solo



Node State › localhost chef_solo _default | orange-3-of-hearts

Converge Status   Compliance Status

orange-3-of-hearts | Run ID: a2c1e098-3c97-4818-8424-4e1f7cdf98f0

✓ The run succeeded on 03/10/2017 at 12:25 am. all resources ran successfully!

RUN DURATION
12:25 AM - 12:25 AM

RUN INITIATOR
Not Available

RUN TYPE

Uptime:	a minute
Environment:	_default
Platform(s):	centos
FQDN:	ip-172-31-44-200.us-west-2.compute.internal

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 ~
```

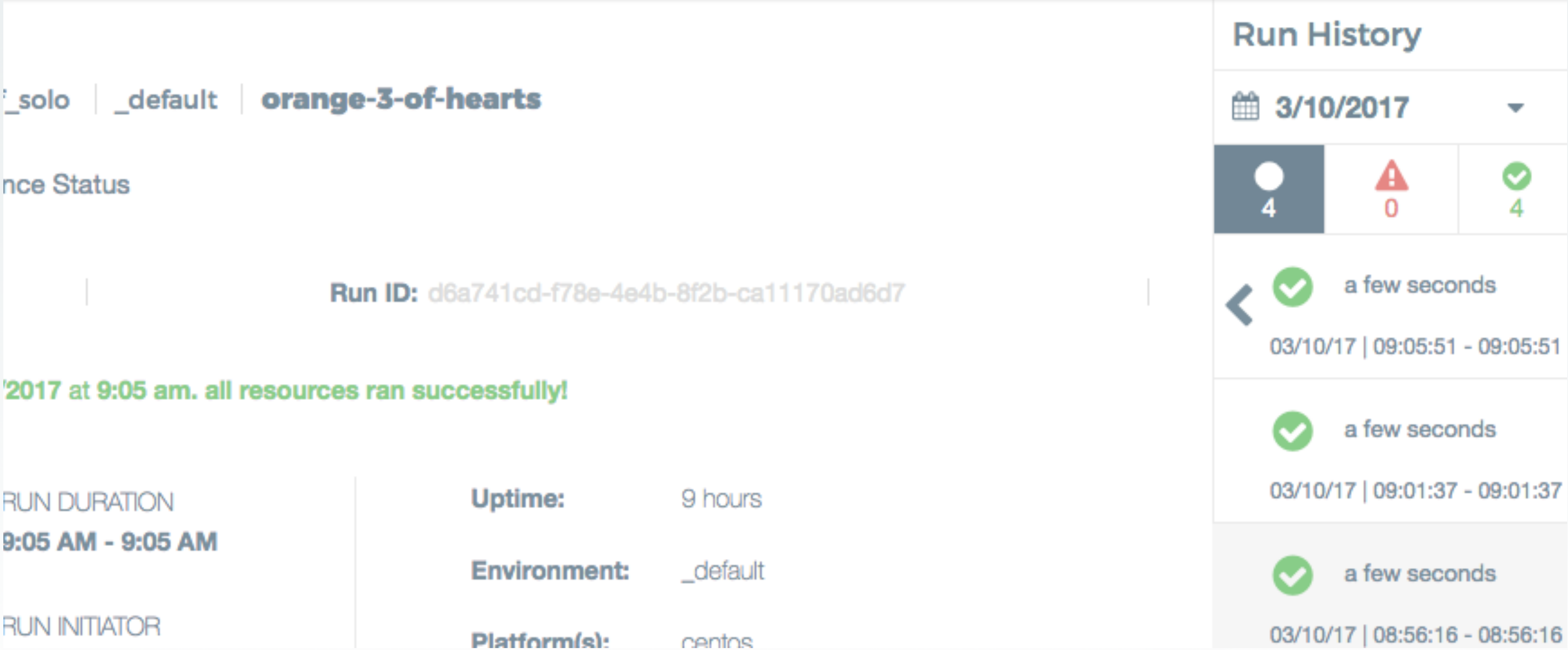
Run chef-client in local mode

```
$ sudo chef-client --local-mode
```

```
[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



_solo | _default | **orange-3-of-hearts**

nce Status

Run ID: d6a741cd-f78e-4e4b-8f2b-ca11170ad6d7

'2017 at 9:05 am. all resources ran successfully!

RUN DURATION
9:05 AM - 9:05 AM

RUN INITIATOR

Uptime: 9 hours

Environment: _default

Platform(s): centos

Run History

📅 3/10/2017 ▾

● 4 | ⚠ 0 | ✓ 4

✓ a few seconds
03/10/17 | 09:05:51 - 09:05:51

✓ a few seconds
03/10/17 | 09:01:37 - 09:01:37

✓ a few seconds
03/10/17 | 08:56:16 - 08:56:16

INSPEC

CHEF

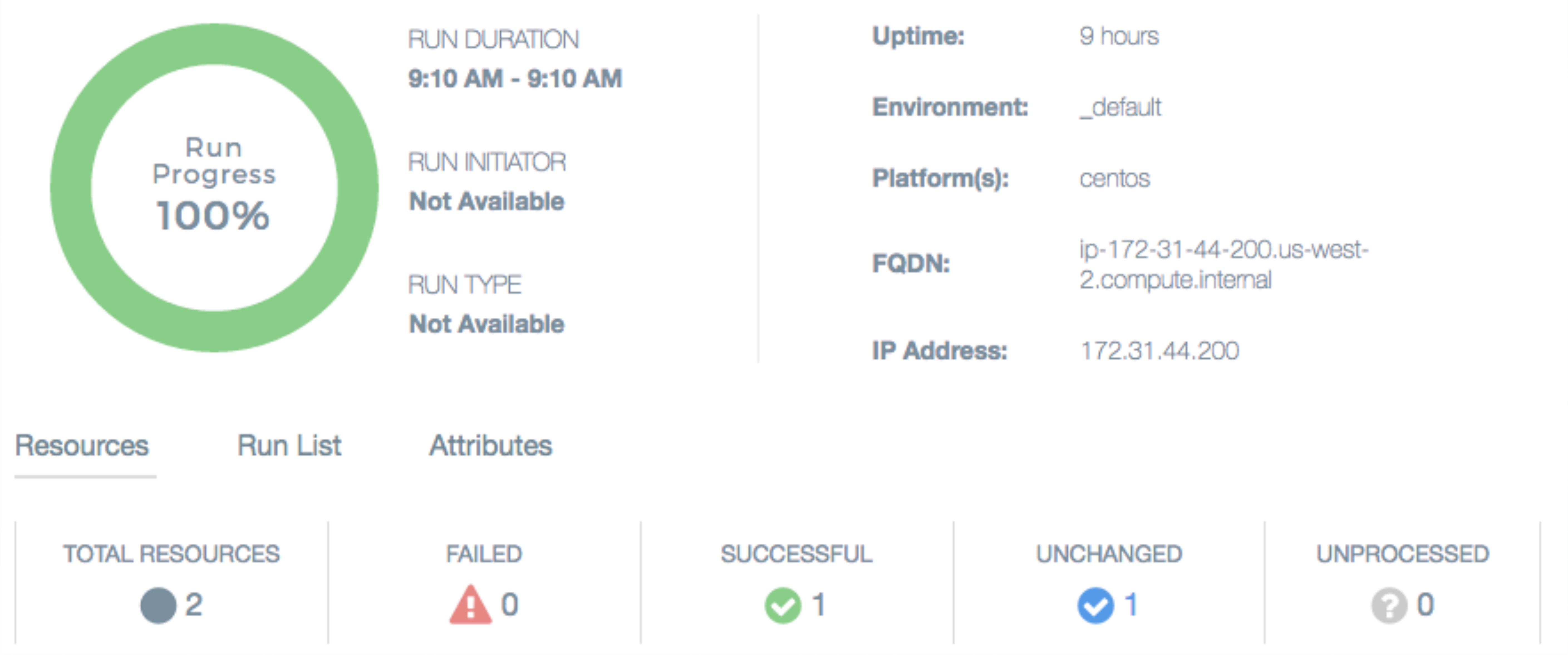
Run with additional parameters

```
$ sudo chef-client --local-mode -j config.json -r "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 DURATION
9:10 AM - 9:10 AM

RUN INITIATOR
Not Available

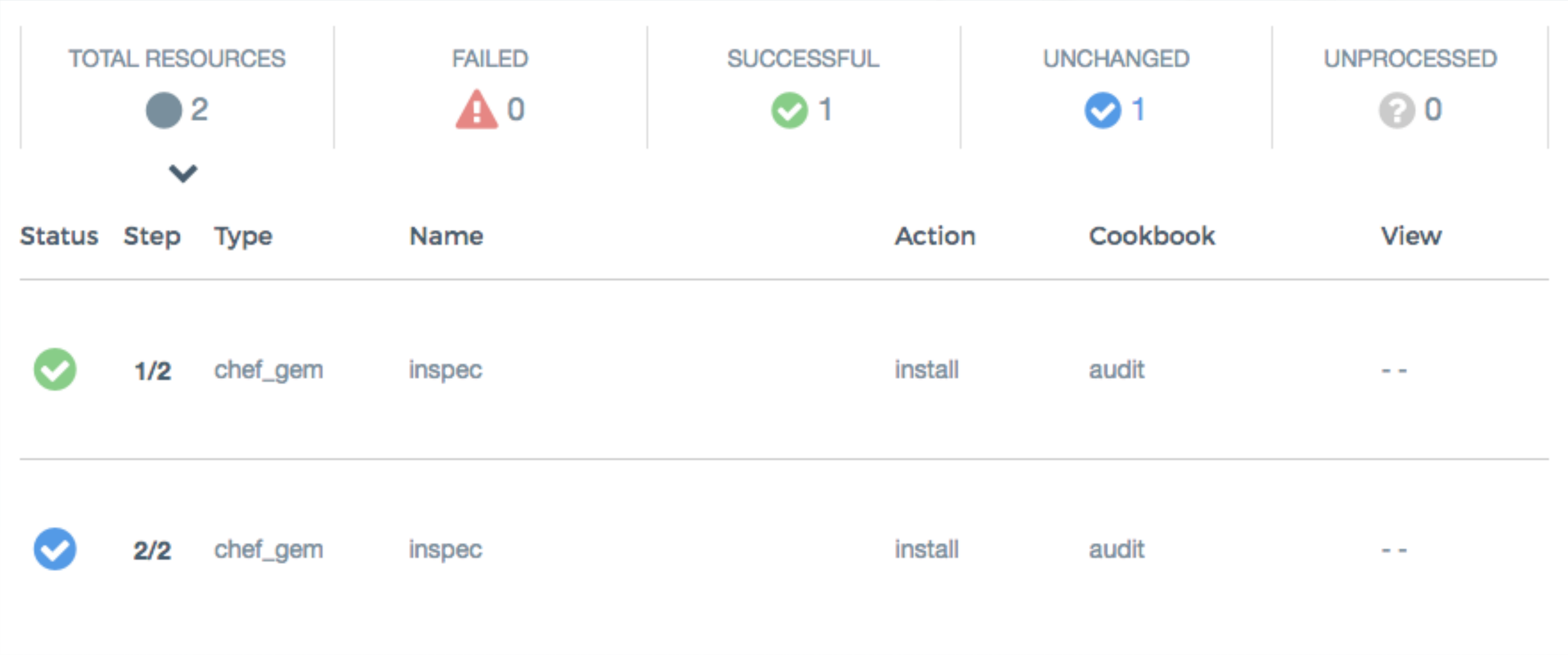
RUN TYPE
Not Available

Uptime:	9 hours
Environment:	_default
Platform(s):	centos
FQDN:	ip-172-31-44-200.us-west-2.compute.internal
IP Address:	172.31.44.200

Resources Run List Attributes

TOTAL RESOURCES	FAILED	SUCCESSFUL	UNCHANGED	UNPROCESSED
● 2	⚠ 0	✓ 1	✓ 1	? 0

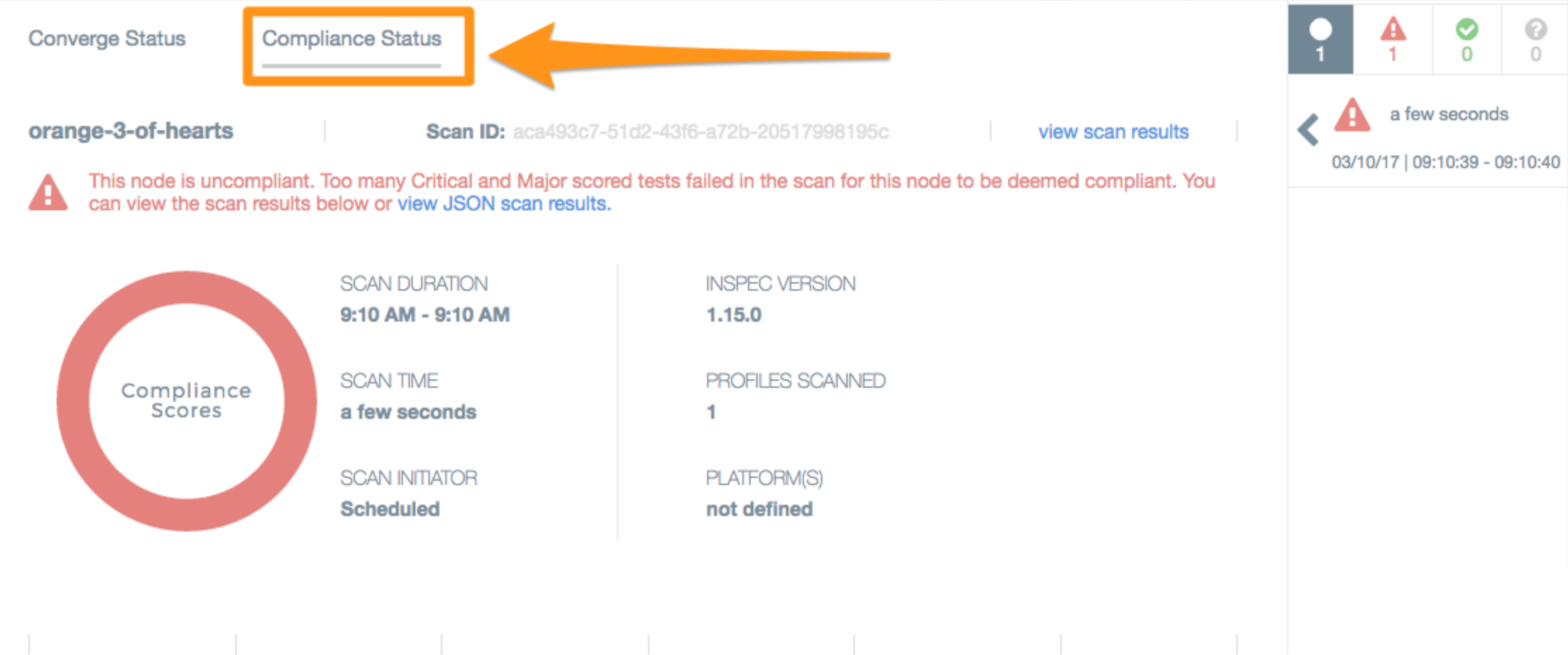
Check the converge status in Automate



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	- -

Check the compliance status in Automate



orange-3-of-hearts | **Scan ID:** aca493c7-51d2-43f6-a72b-20517998195c | view scan results

This node is uncompliant. Too many Critical and Major scored tests failed in the scan for this node to be deemed compliant. You can view the scan results below or view JSON scan results.

SCAN DURATION
9:10 AM - 9:10 AM

SCAN TIME
a few seconds

SCAN INITIATOR
Scheduled

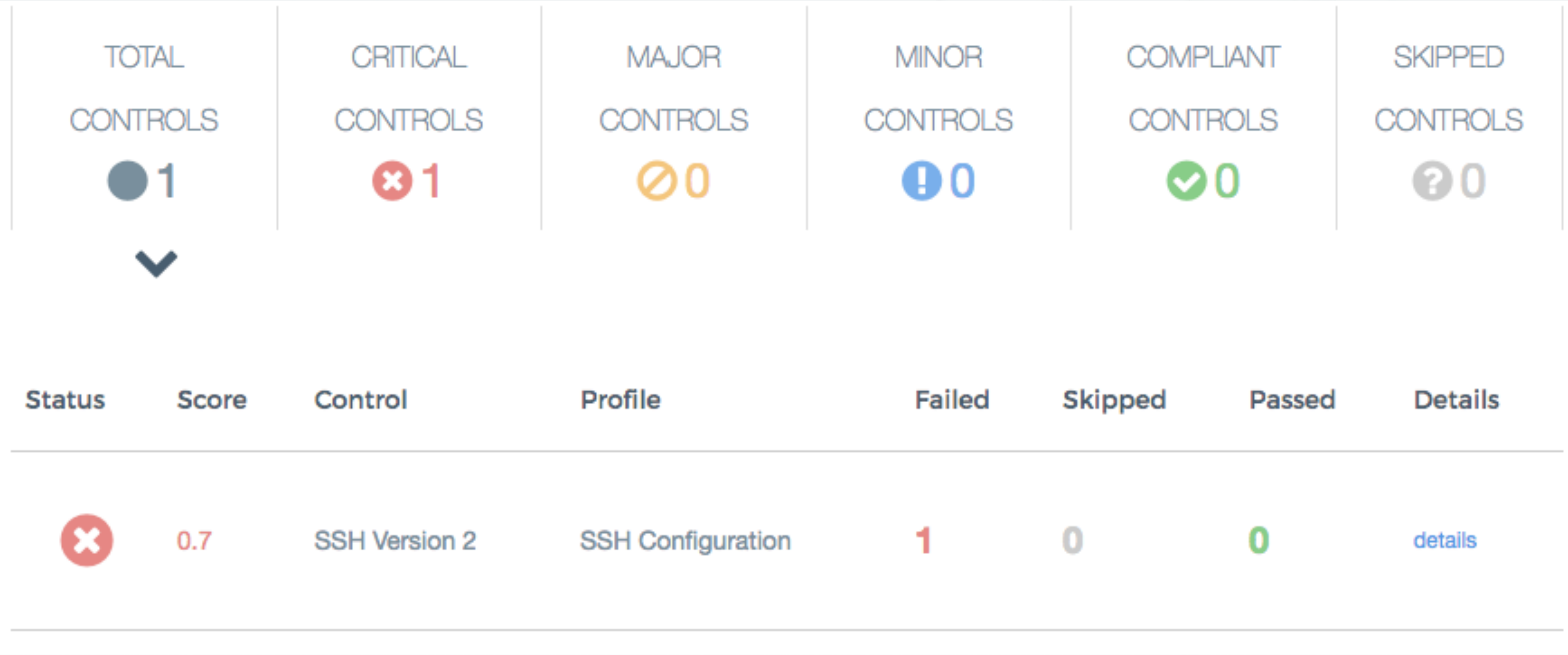
INSPEC VERSION
1.15.0

PROFILES SCANNED
1

PLATFORM(S)
not defined

a few seconds
03/10/17 | 09:10:39 - 09:10:40

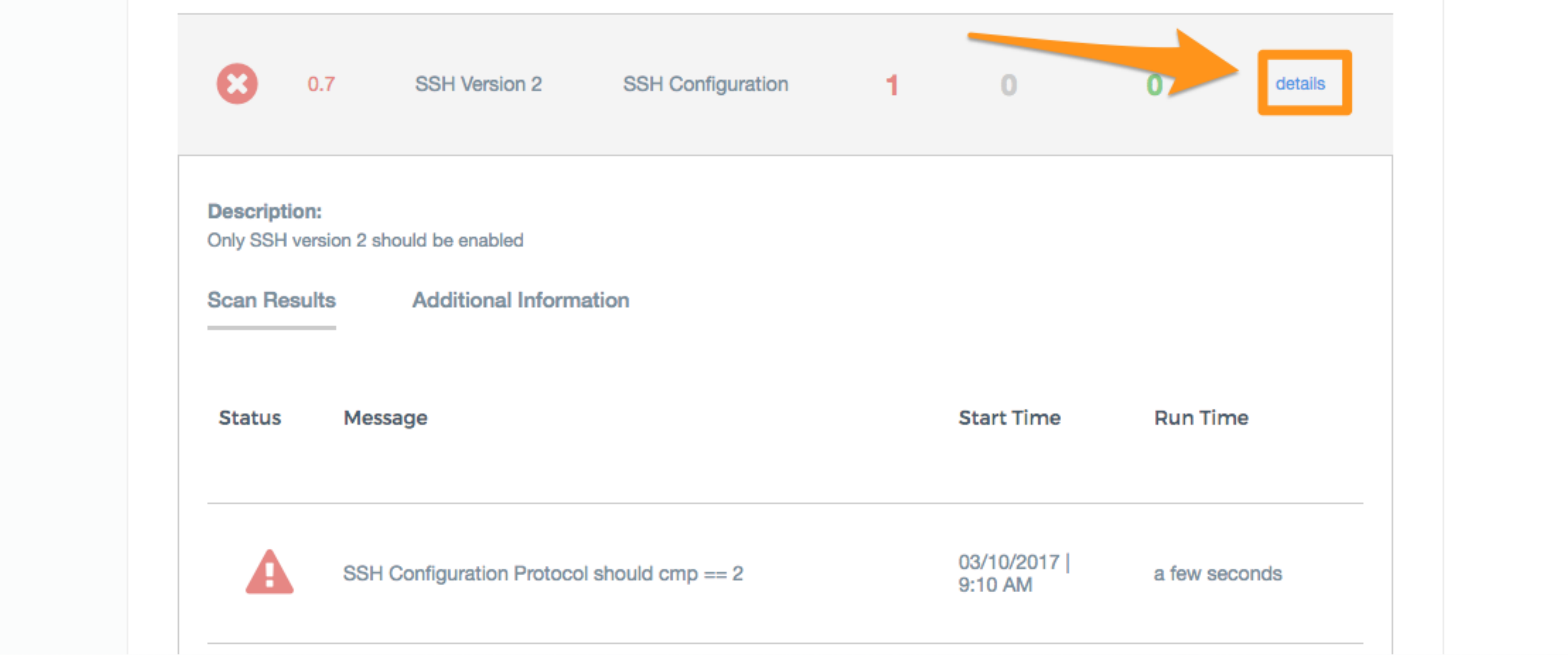
Check the compliance status in Automate



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

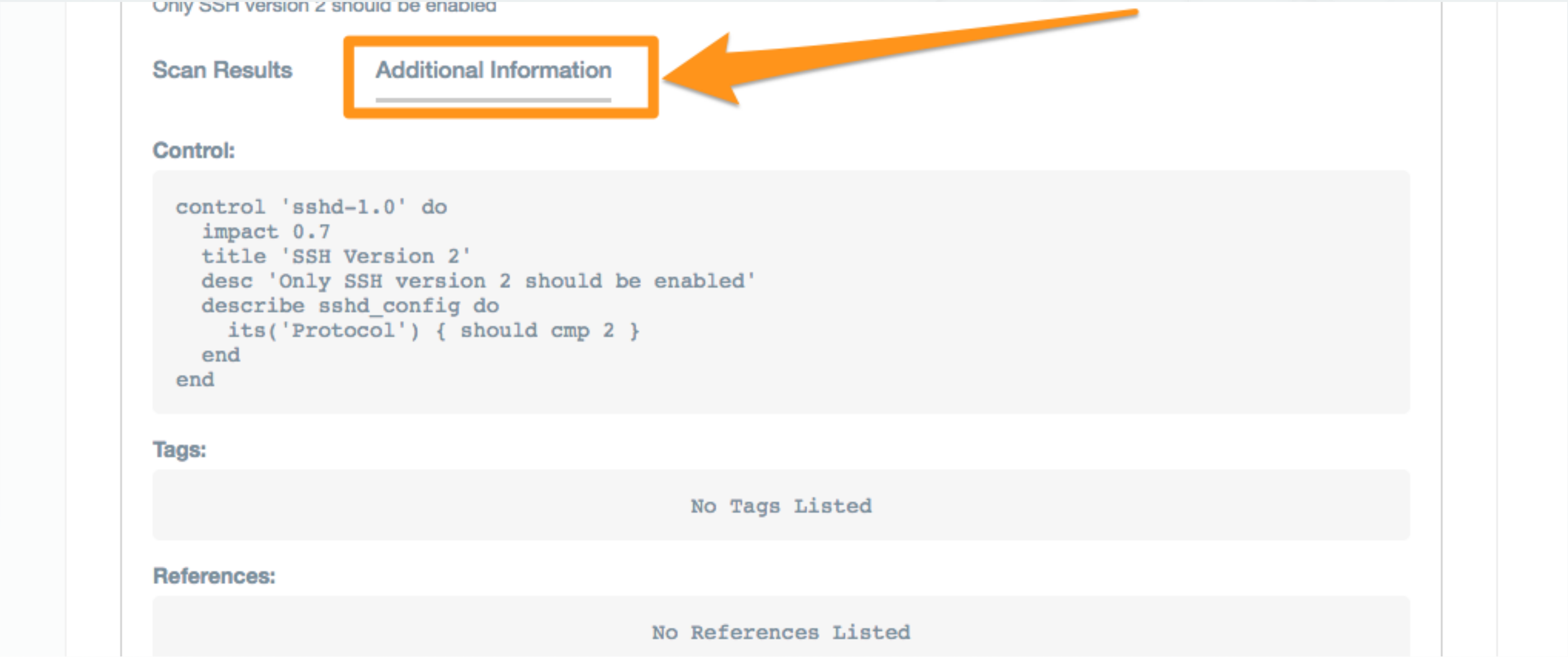


⊗	0.7	SSH Version 2	SSH Configuration	1	0	0	details

Description:
Only SSH version 2 should be enabled

Status	Message	Start Time	Run Time
⚠	SSH Configuration Protocol should cmp == 2	03/10/2017 | 9:10 AM	a few seconds

View details of the failing control



Only SSH version 2 should be enabled

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:

No Tags Listed

References:

No References Listed

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 Visibility

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
```

Next Steps

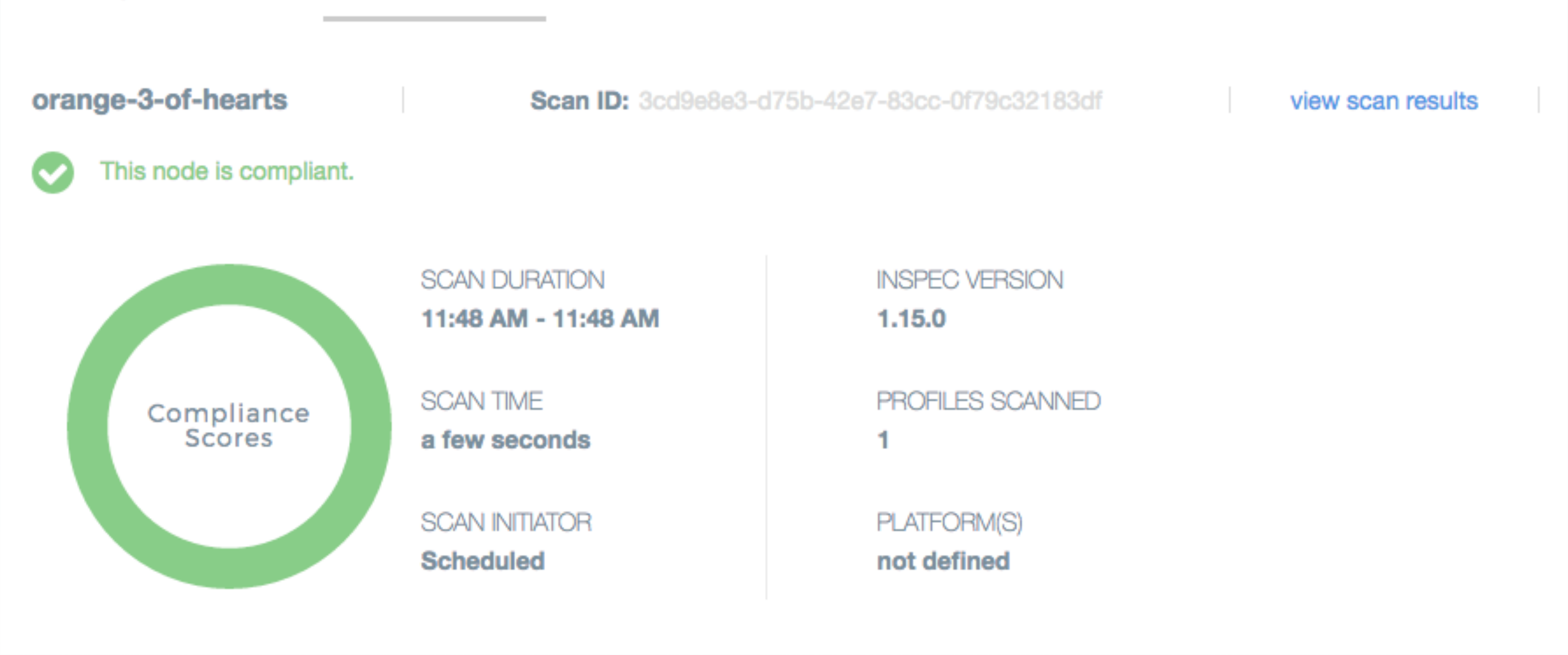
- Remediate the failing control
- Run the audit cookbook to verify the remediation
- View the compliant node in Automate

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



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

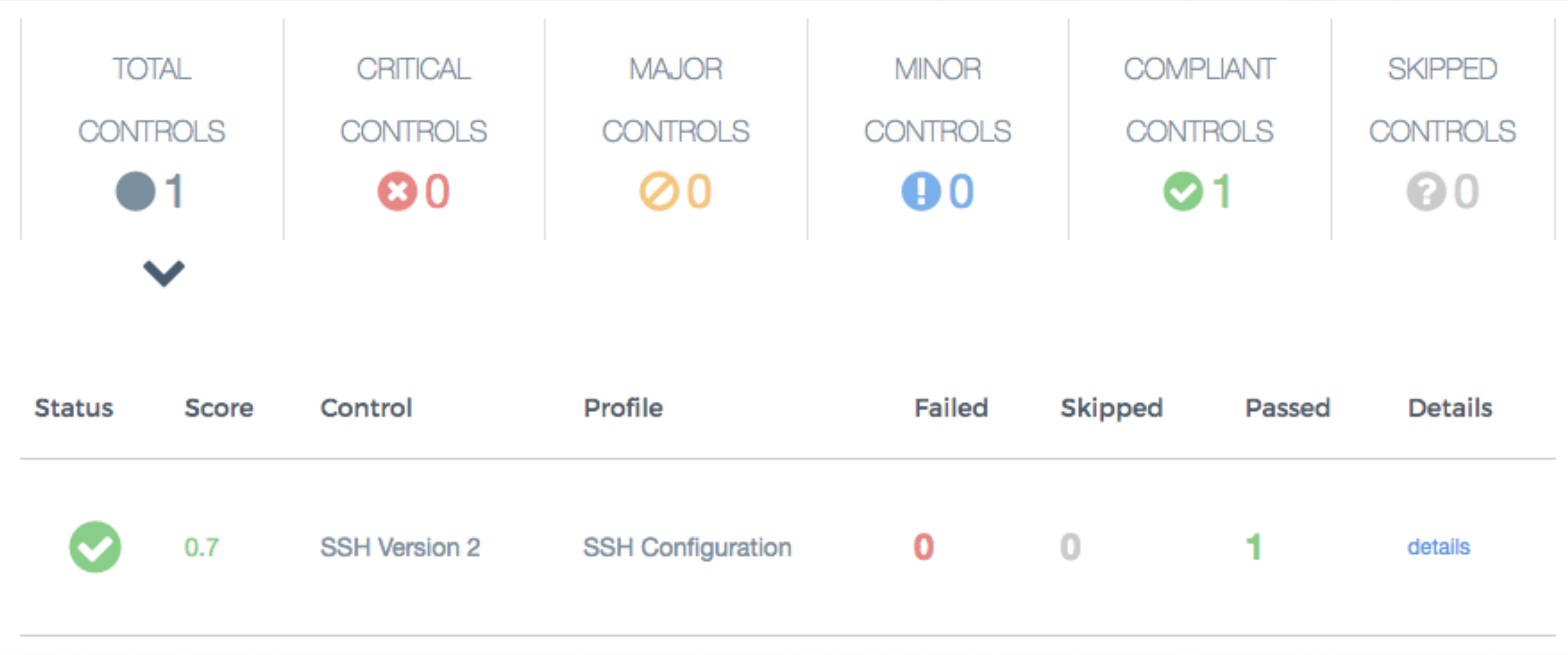
SCAN INITIATOR
Scheduled

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