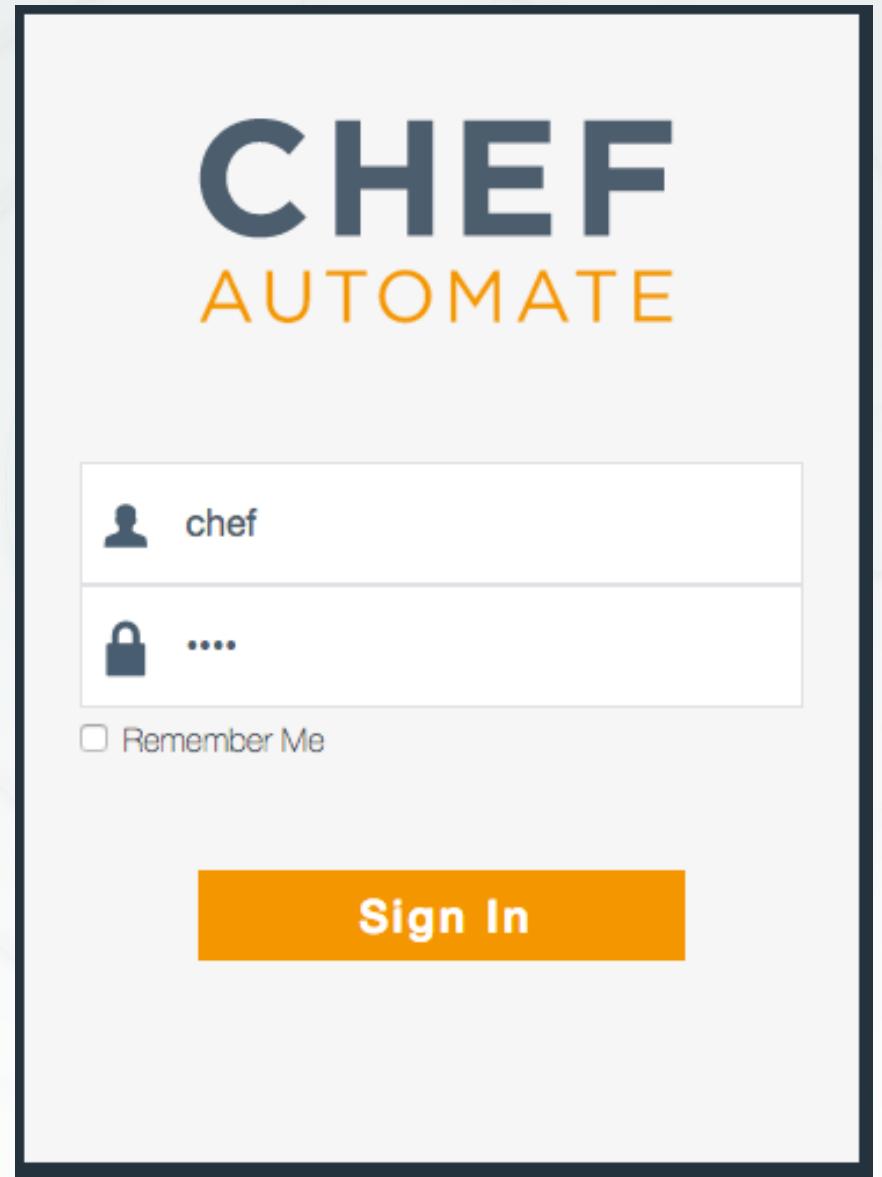


Continuous Compliance

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" and "Runner Activity".

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 square icon)
- WORKFLOW CHANGES ***: 0 (purple square 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	
Converge 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](#)

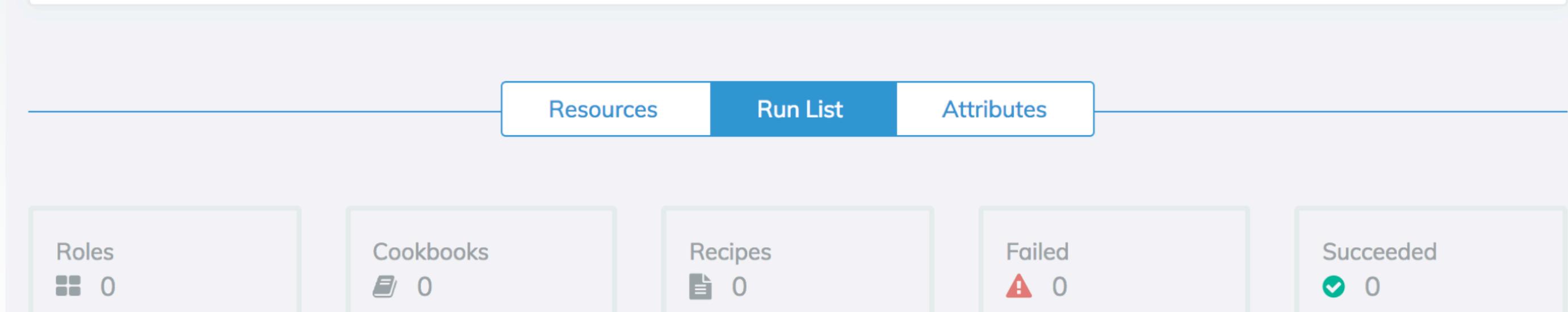
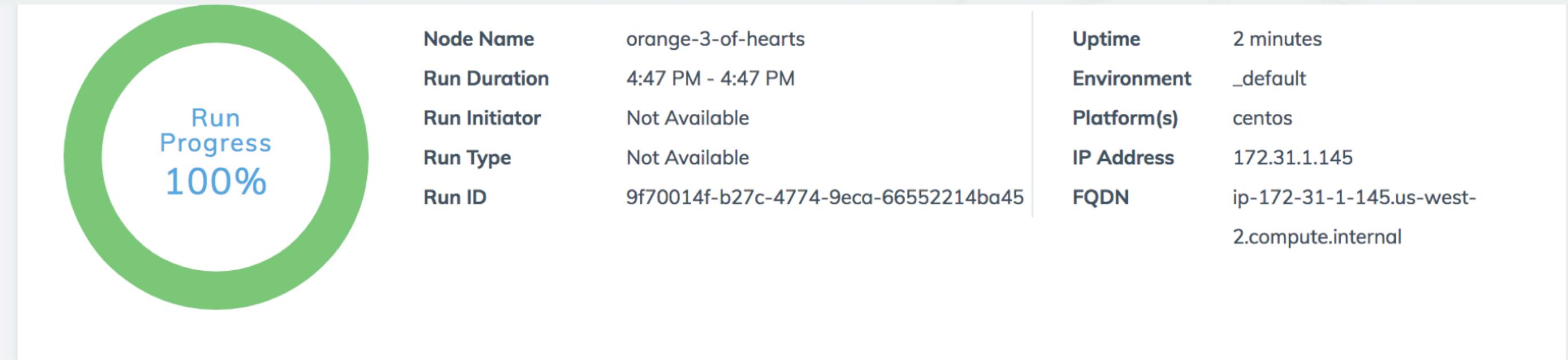
Run History

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

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

Run History

Last 24 hours

3	0	3
---	---	---

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
```

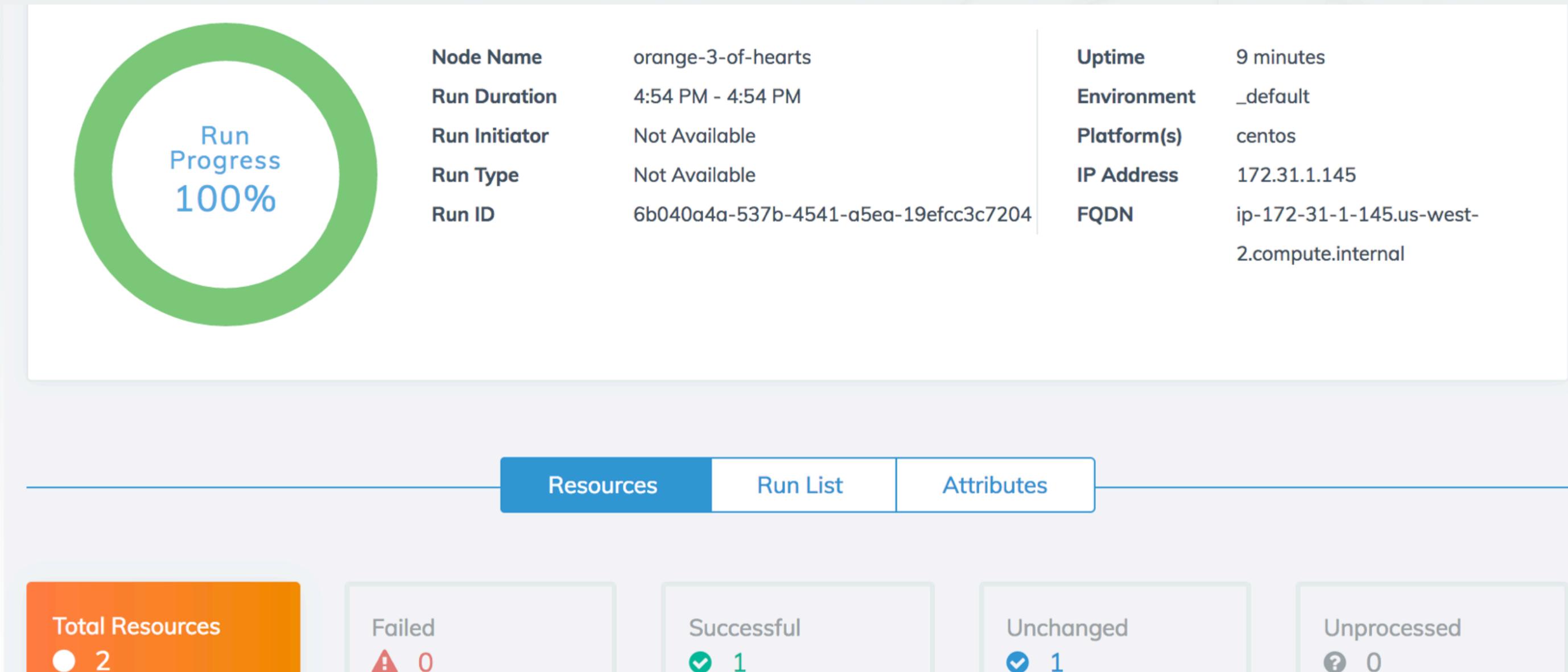
Running handlers:

```
[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



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**

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

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

Total Controls ● 1

Critical Controls ✖ 1

Major Controls ⚡ 0

Minor Controls ! 0

Compliant Controls ✓ 0

Skipped Controls ? 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
✖	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

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://

  × 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

Converge Status **Compliance Status**

✓ This node is compliant. View scan results

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

Node Name	orange-3-of-hearts	Inspec Version	1.15.0
Scan Duration	5:03 PM - 5:03 PM	Profiles Scanned	1
Scan Time	a few seconds	Platform(s)	not defined
Scan Initiator	Scheduled		
Scan ID	6076b098-e02c-4b6e-8731- 8c63217e8733		

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	details