1: Introduction

Chef Compliance

Installation, Configuration, and Operation

Introduction

1-1

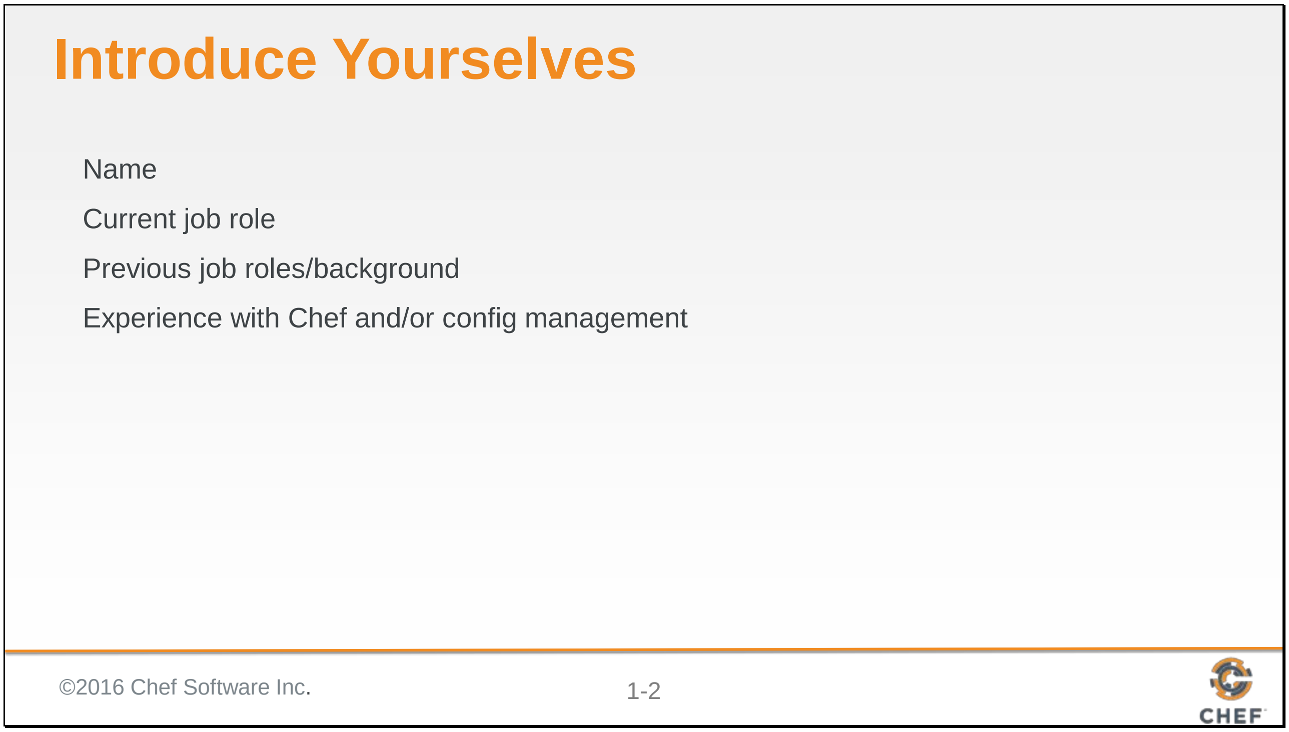
Course v1.0.0

This Chef Compliance course provides an understanding of the capabilities of Chef Compliance. This course covers how to install and initially configure the Chef Compliance server, perform compliance scans against Windows and Linux nodes, and remediate compliance issues with Chef, and run Compliance reports.

In addition, you will learn how to use InSpec to create and modify Chef Compliance profiles and learn how to locate CIS (Center for Internet Security) and DoD (Department of Defense) compliance specifications that you can use to write Chef Compliance profiles.

Instructor Note: **Be sure to read Appendix Z at the end of this instructor guide** for training lab set up notes and additional instructor notes.
Instructor Note: This course has been tested on Compliance Server v0.14.5. The labs have been tested against target Linux and Windows nodes that have ChefDK 0.11.2 and inspec 0.14.7. You must use at least inspec 0.14.7 on the target nodes in order for these labs to work.

Slide 2



Introduce Yourselves

Name

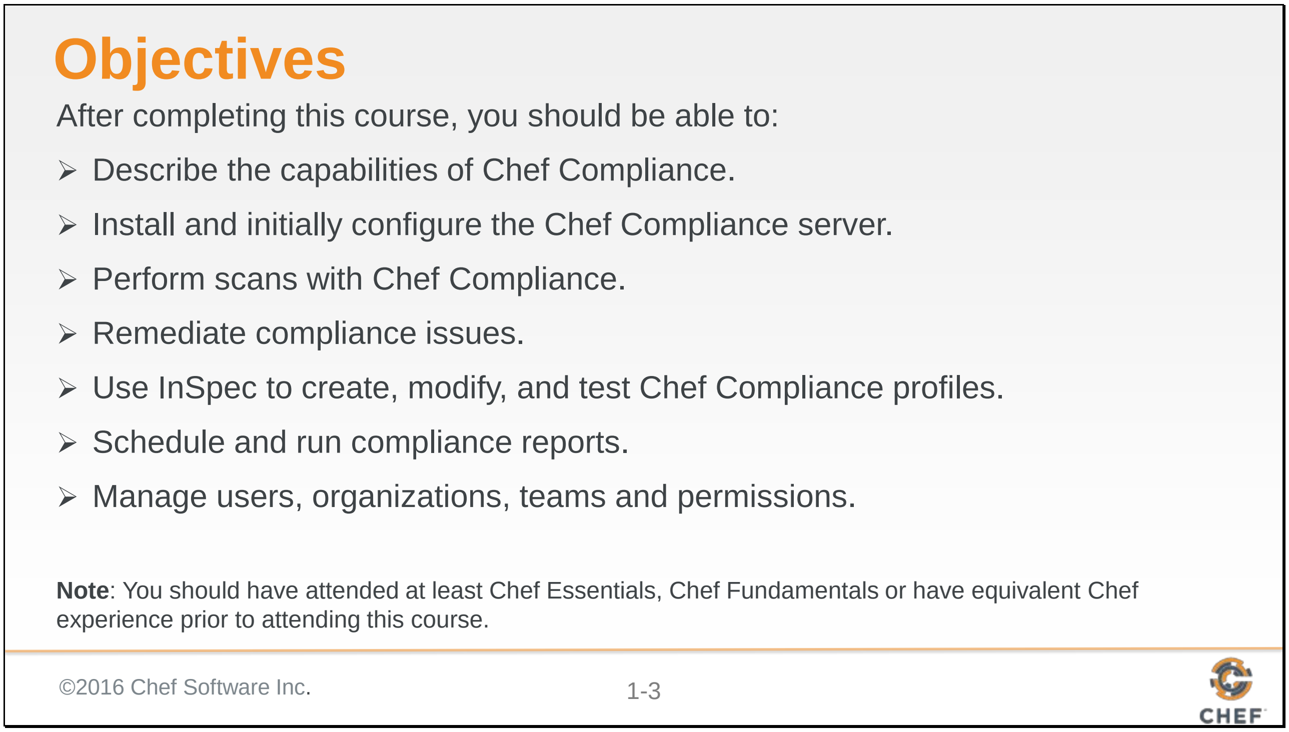
Current job role

Previous job roles/background

Experience with Chef and/or config management

1-2

Slide 3



Objectives

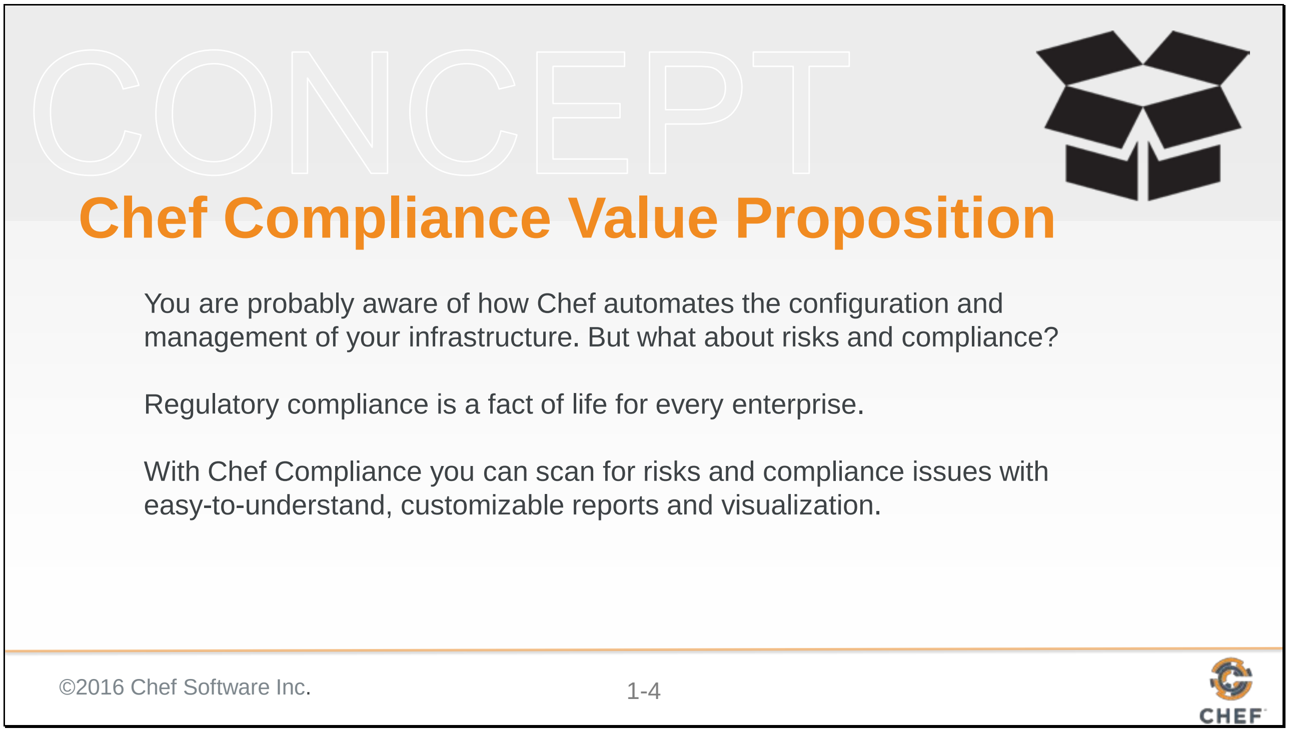
After completing this course, you should be able to:

- Describe the capabilities of Chef Compliance.
- Install and initially configure the Chef Compliance server.
- Perform scans with Chef Compliance.
- Remediate compliance issues.
- Use InSpec to create, modify, and test Chef Compliance profiles.
- Schedule and run compliance reports.
- Manage users, organizations, teams and permissions.

Note: You should have attended at least Chef Essentials, Chef Fundamentals or have equivalent Chef experience prior to attending this course.

Instructor Note: You can tell the students that this course covers scanning and remediating both Linux and Windows nodes. For example, module 03 covers scanning and remediating Linux nodes and module 04 covers scanning and remediating Windows nodes. However, the Compliance server runs only on Linux.

Slide 4



CONCEPT

Chef Compliance Value Proposition

You are probably aware of how Chef automates the configuration and management of your infrastructure. But what about risks and compliance?

Regulatory compliance is a fact of life for every enterprise.

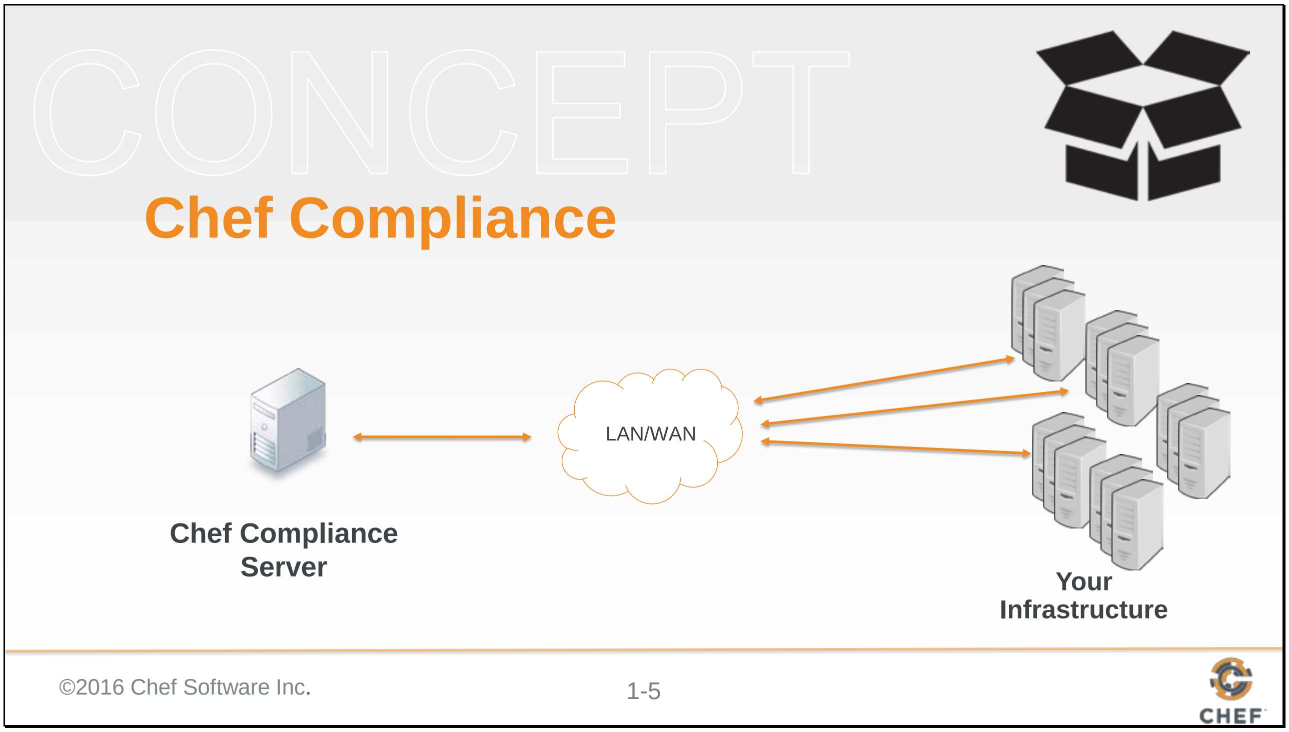
With Chef Compliance you can scan for risks and compliance issues with easy-to-understand, customizable reports and visualization.

By now you are probably aware of how Chef automates the configuration and management of your infrastructure. But what about risks and compliance issues of your infrastructure?

Regulatory compliance is a fact of life for every enterprise. With Chef Compliance you can scan for risks and compliance issues with easy-to-understand, customizable reports and visualization.

You can then use Chef to automate the remediation of issues and use Chef Compliance to implement a continuous audit of applications and infrastructure.

Slide 5



CONCEPT

Chef Compliance

©2016 Chef Software Inc.

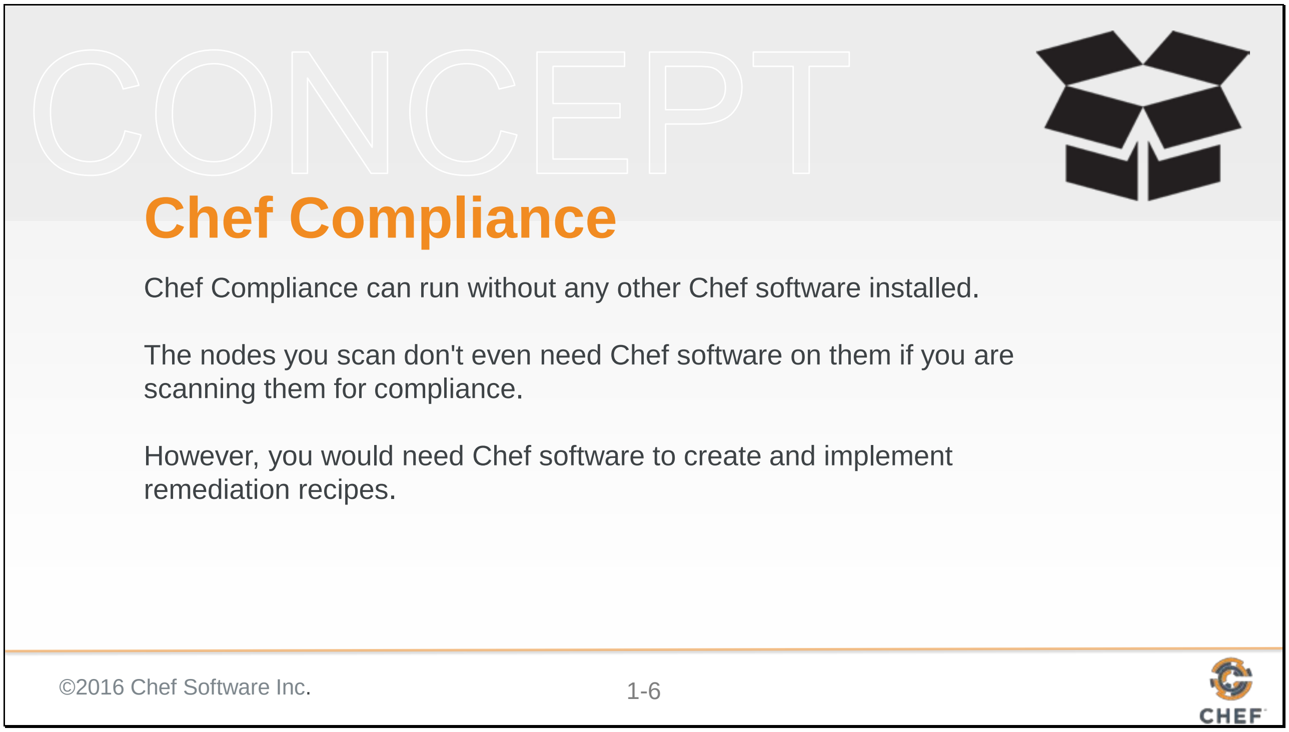
1-5

The Chef Compliance server is a centralized location from which all aspects of the state or your infrastructure’s compliance can be managed.

With Chef Compliance you can test any node in your infrastructure, including all of the common UNIX and Linux platforms and most versions of Microsoft Windows.

Chef Compliance can continuously test any node against the goals of your organization’s security management lifecycle for risks and compliance issues.

Slide 6



CONCEPT

Chef Compliance

Chef Compliance can run without any other Chef software installed.

The nodes you scan don't even need Chef software on them if you are scanning them for compliance.

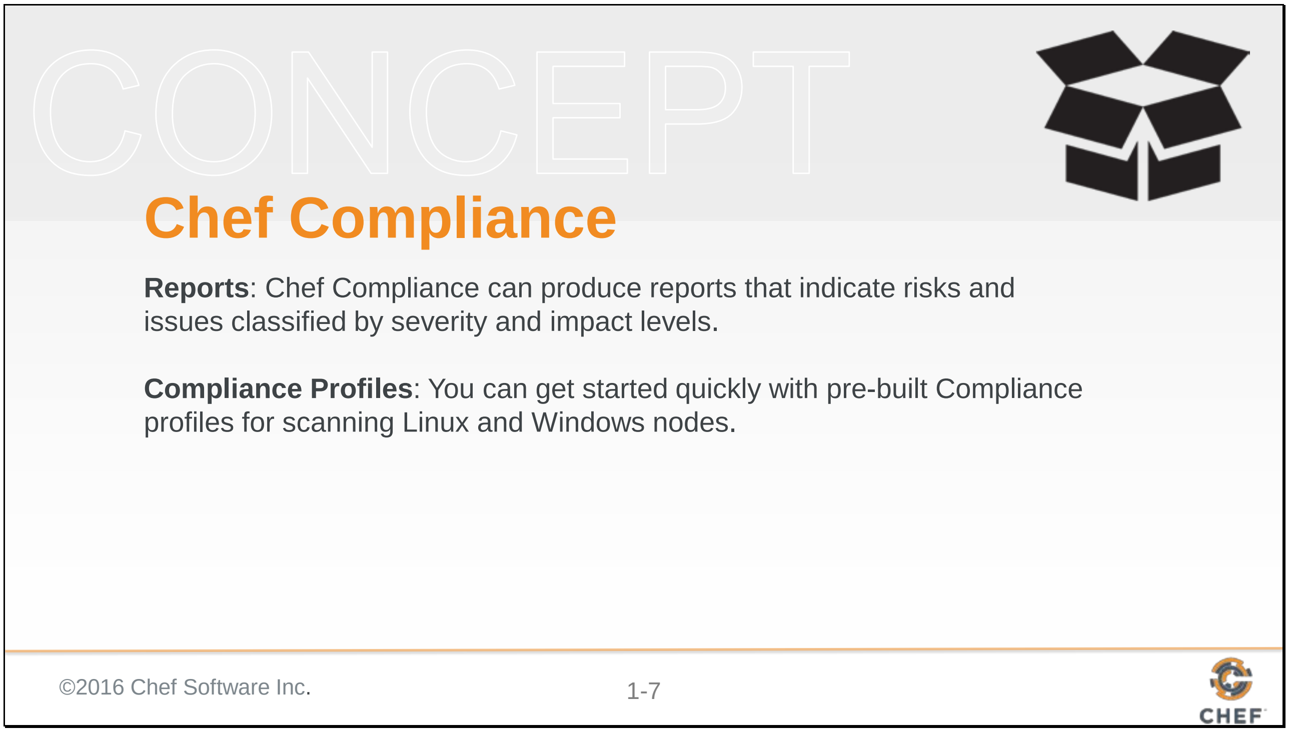
However, you would need Chef software to create and implement remediation recipes.

Chef Compliance can run without any other Chef software installed on the Chef Compliance server machine.

The nodes you scan don't even need Chef software on them if you are scanning them for compliance.

However, you would need Chef software to create and implement remediation recipes if you choose to use recipes to remediate compliance issues.

Slide 7



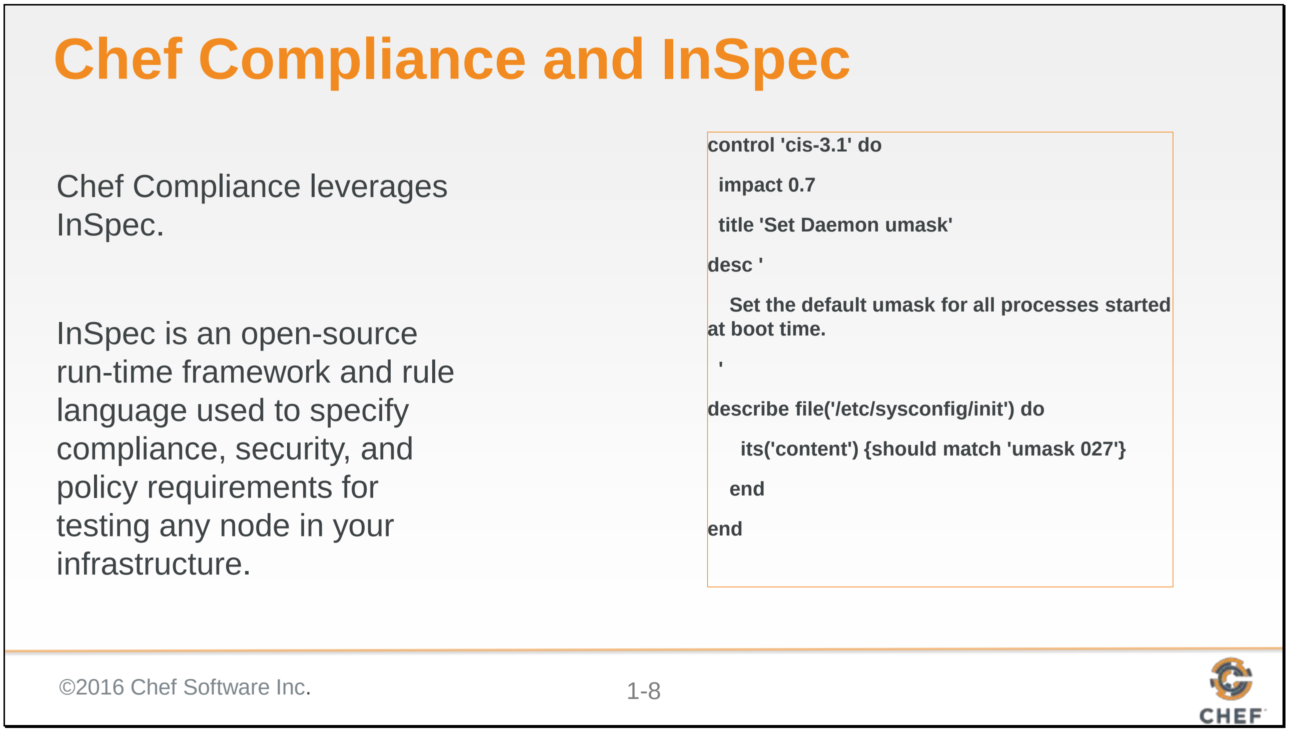
CONCEPT

Chef Compliance

Reports: Chef Compliance can produce reports that indicate risks and issues classified by severity and impact levels.

Compliance Profiles: You can get started quickly with pre-built Compliance profiles for scanning Linux and Windows nodes.

Slide 8



Chef Compliance and InSpec

Chef Compliance leverages InSpec.

InSpec is an open-source run-time framework and rule language used to specify compliance, security, and policy requirements for testing any node in your infrastructure.

```
control 'cis-3.1' do
 impact 0.7
 title 'Set Daemon umask'
desc '
   Set the default umask for all processes started
at boot time.
 '
describe file('/etc/sysconfig/init') do
    its('content') {should match 'umask 027'}
   end
end
```

©2016 Chef Software Inc. 1-8

Chef Compliance leverages InSpec.

InSpec is an open-source run-time framework and rule language used to specify compliance, security, and policy requirements for testing any node in your infrastructure. The InSpec name refers to “infrastructure specification

InSpec includes a collection of resources to help you write auditing rules quickly and easily using the Compliance DSL.

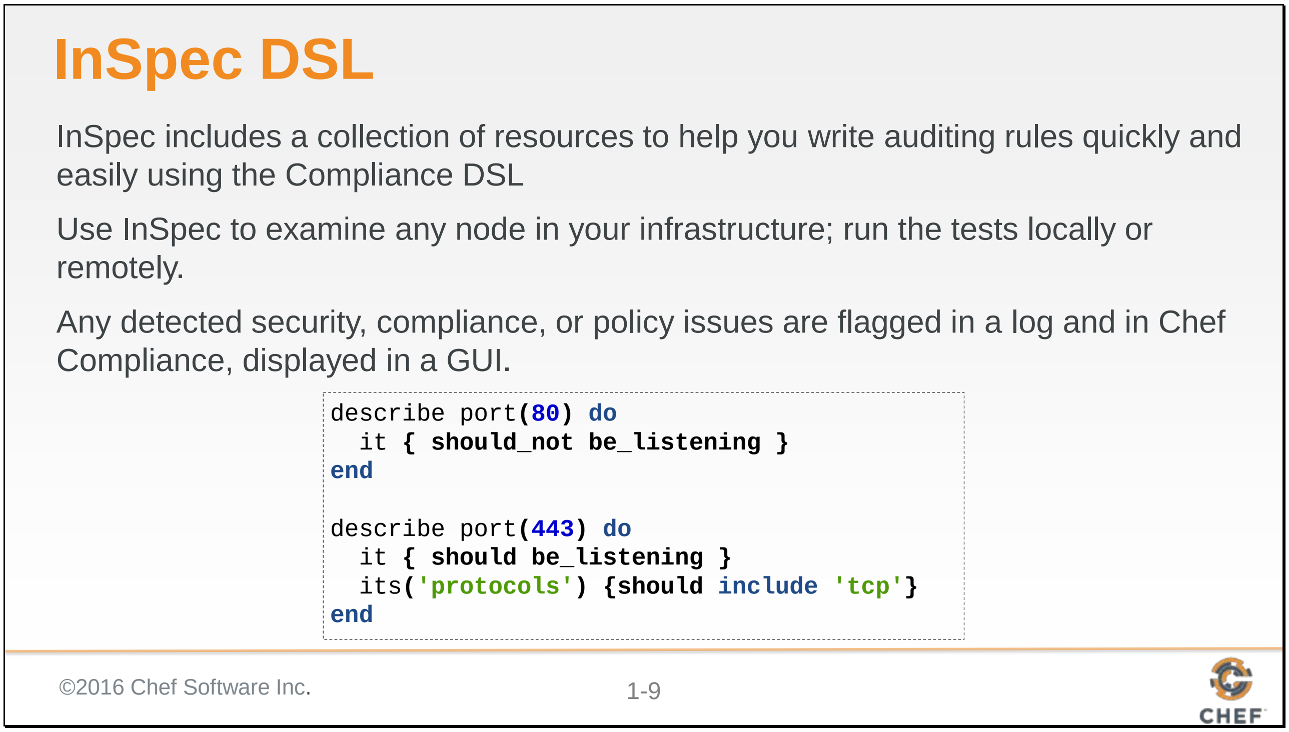
Use InSpec to examine any node in your infrastructure; run the tests locally or remotely.

Any detected security, compliance, or policy issues are flagged in a log and displayed in reports.

The InSpec audit resource framework is fully compatible with Chef Compliance.

Instructor note: InSpec is similar to ServerSpec but learners who have no experience with Serverspec may be confused by the reference.

Slide 9



InSpec DSL

InSpec includes a collection of resources to help you write auditing rules quickly and easily using the Compliance DSL

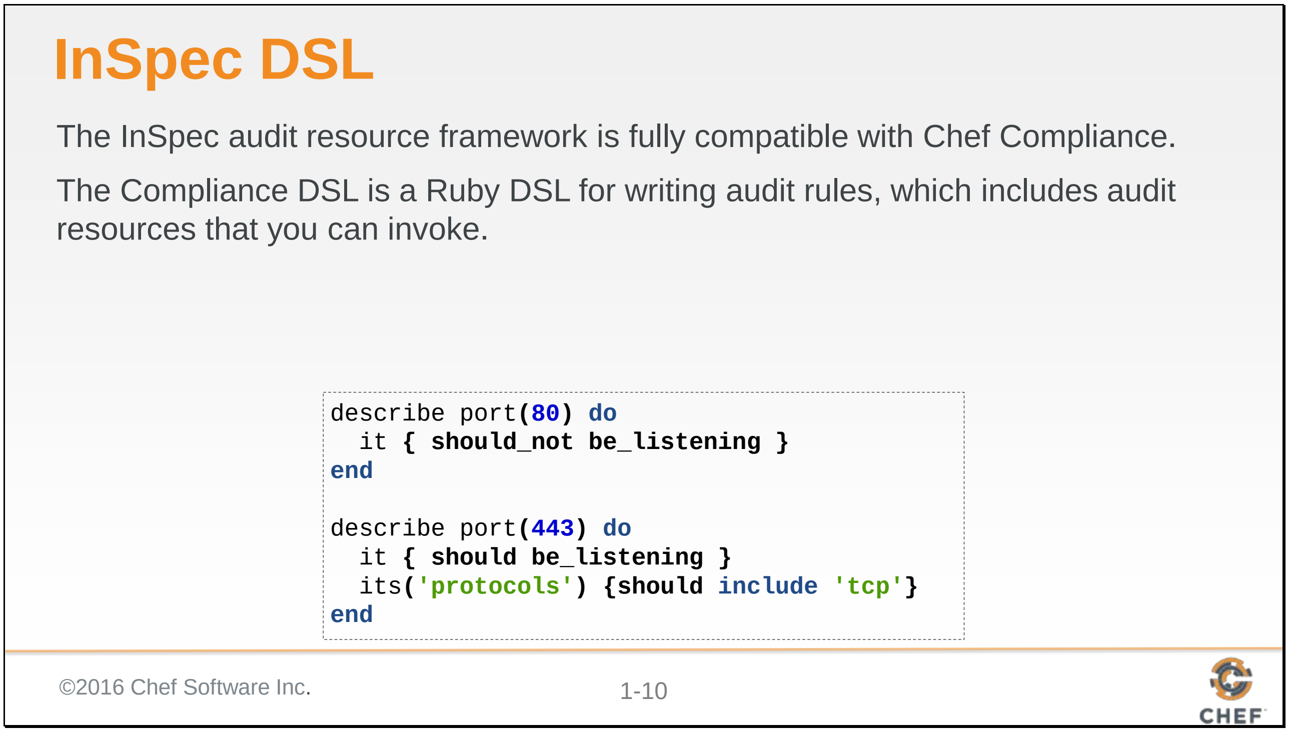
Use InSpec to examine any node in your infrastructure; run the tests locally or remotely.

Any detected security, compliance, or policy issues are flagged in a log and in Chef Compliance, displayed in a GUI.

```
describe port(80) do
  it { should_not be_listening }
end

describe port(443) do
  it { should be_listening }
  its('protocols') {should include 'tcp'}
end
```

Slide 10



InSpec DSL

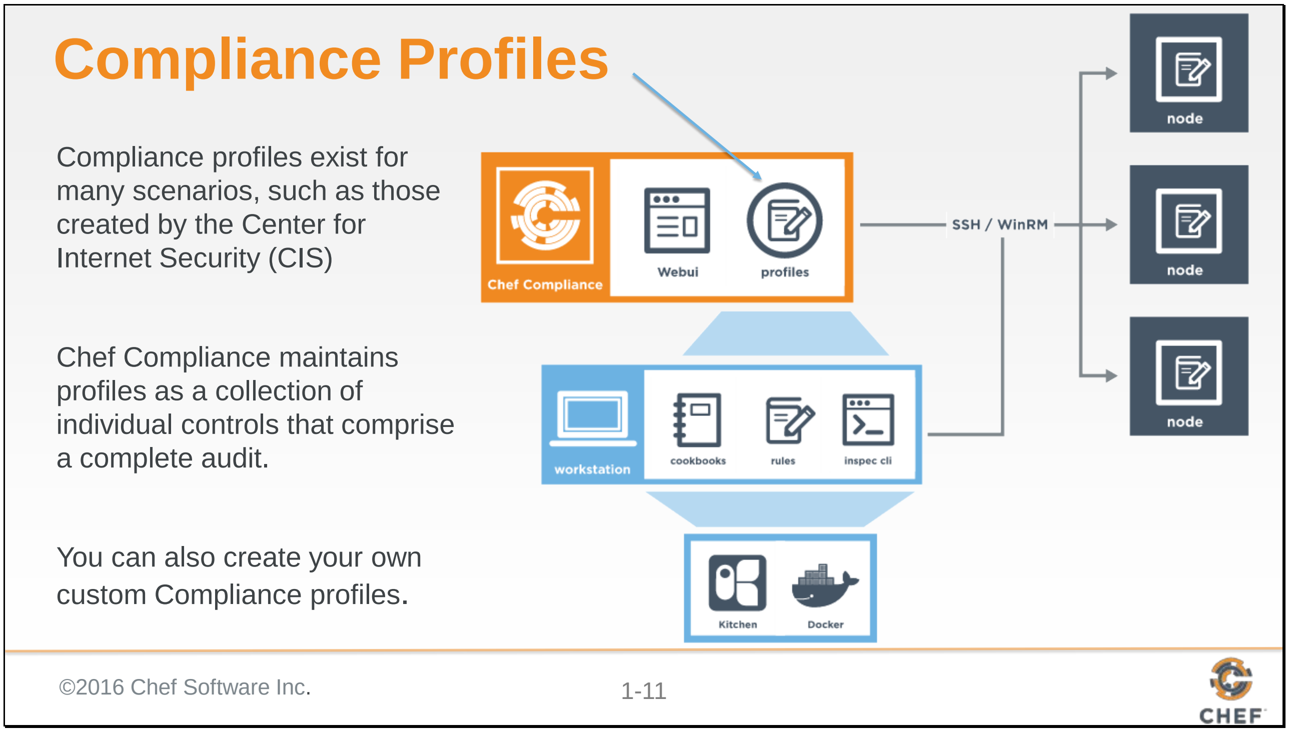
The InSpec audit resource framework is fully compatible with Chef Compliance.

The Compliance DSL is a Ruby DSL for writing audit rules, which includes audit resources that you can invoke.

```
describe port(80) do
  it { should_not be_listening }
end

describe port(443) do
  it { should be_listening }
  its('protocols') {should include 'tcp'}
end
```

Slide 11



Compliance Profiles

Compliance profiles exist for many scenarios, such as those created by the Center for Internet Security (CIS)

Chef Compliance maintains profiles as a collection of individual controls that comprise a complete audit.

You can also create your own custom Compliance profiles.

Compliance profiles exist for many scenarios, such as those created by the Center for Internet Security (CIS), a non-profit organization that is focused on enhancing the cyber security readiness and response of public and private sector entities.

Chef Compliance maintains profiles as a collection of individual controls that comprise a complete audit. For example, CIS benchmark 8.1.1.1 recommends testing for the maximum size of the audit log.

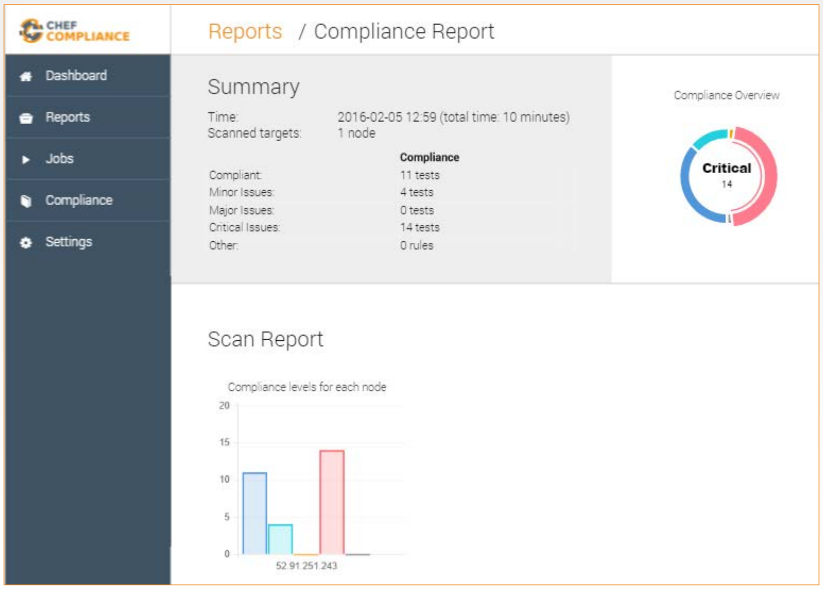
You can also create your own custom Compliance profiles.

Slide 12

Compliance Web UI

The Chef Compliance web UI provides views into compliance scan results as well as views of Chef Compliance profiles.

You execute scans via the Compliance web UI as well.



Reports / Compliance Report

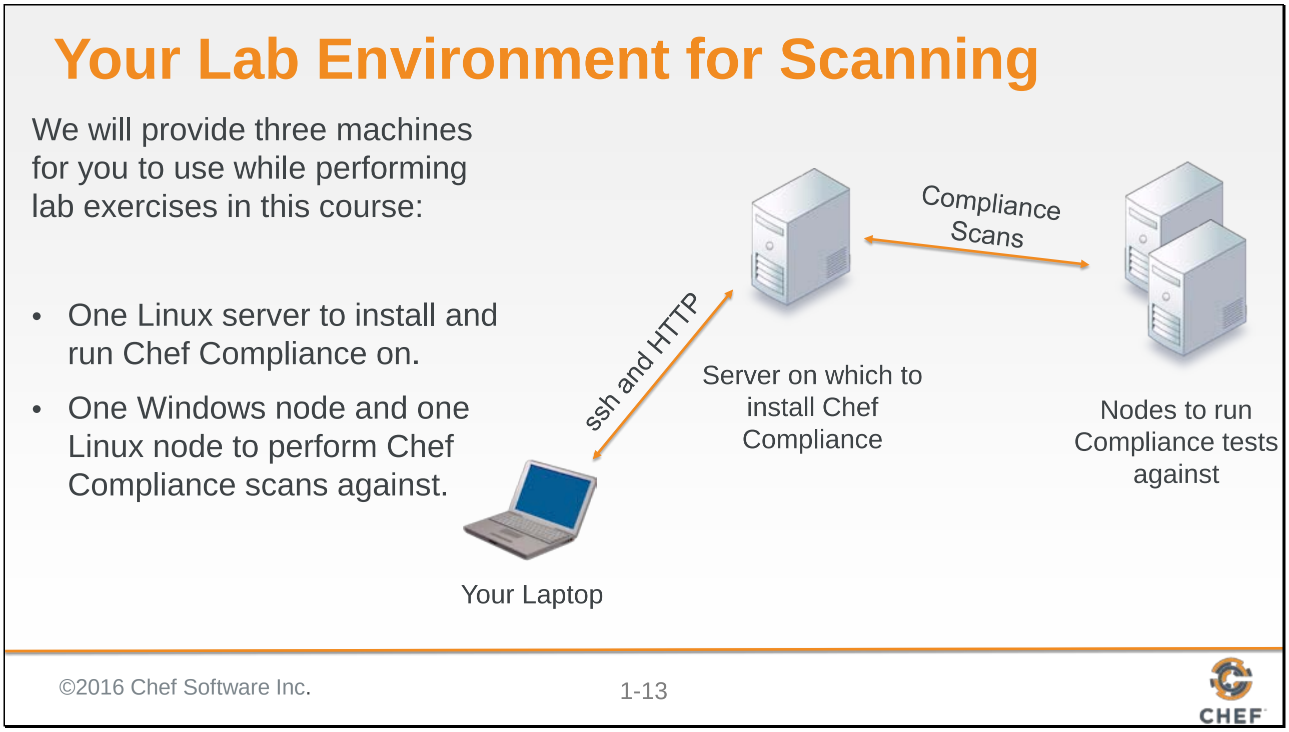
Summary

Time: 2016-02-05 12:59 (total time: 10 minutes)
Scanned targets: 1 node

	Compliance
Compliant:	11 tests
Minor Issues:	4 tests
Major Issues:	0 tests
Critical Issues:	14 tests
Other:	0 rules

Scan Report

Slide 13



Your Lab Environment for Scanning

We will provide three machines for you to use while performing lab exercises in this course:

- One Linux server to install and run Chef Compliance on.
- One Windows node and one Linux node to perform Chef Compliance scans against.

Your Laptop

ssh and HTTP

Server on which to install Chef Compliance

Compliance Scans

Nodes to run Compliance tests against

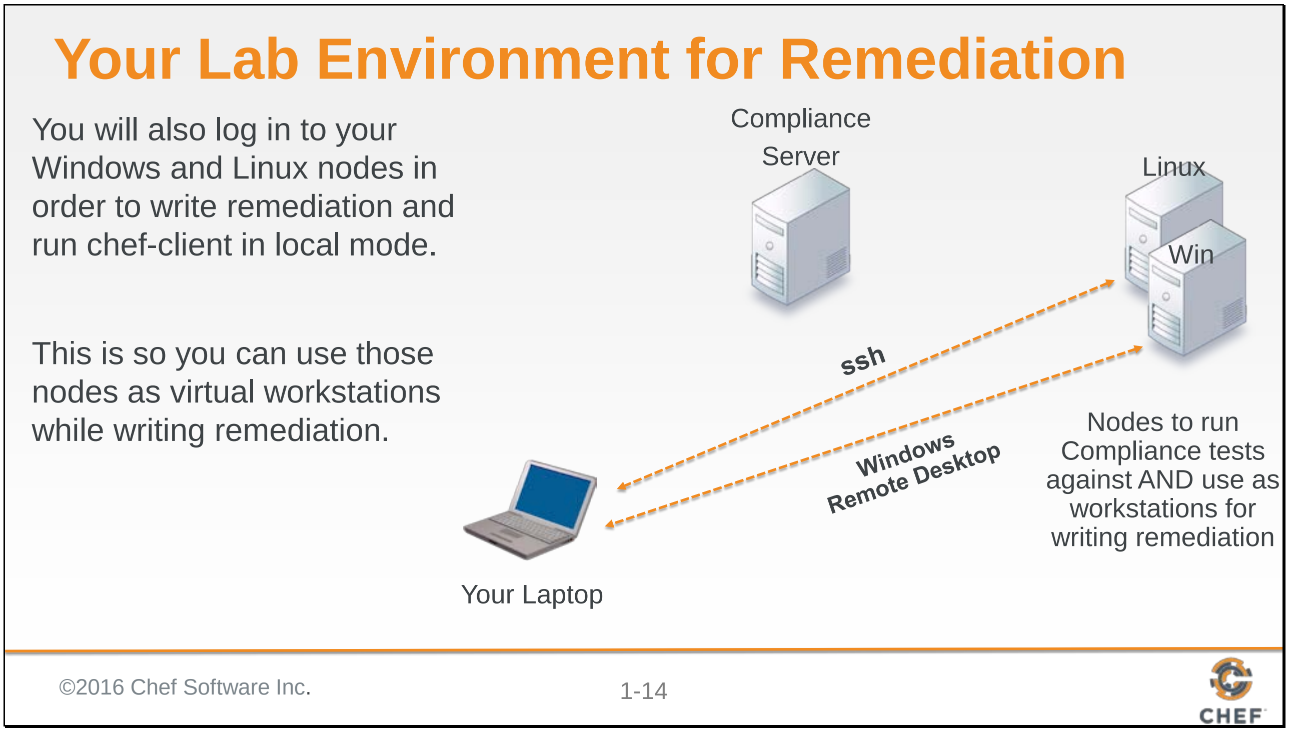
1-13

These are basic AWS AMIs that we use for Chef training. They have ChefDK installed on them although Chef does not actually need to be installed on these instances in order to run scans.

Instructor Note: Now would be a good time to distribute the hostnames of the three nodes you will assign to each student. You should ask the students to note which one they will use as their Compliance Server and which ones they will use as the target nodes for scans.
For example:
ec2-52-91-31-125.compute-1.amazonaws.com = Compliance server.
ec2-54-164-54-218.compute-1.amazonaws.com = Linux Target node.
ec2-54-164-54-210.compute-1.amazonaws.com = Windows Target node.

The login credentials for the Linux nodes is chef/chef.
The login credentials for the Windows nodes is Administrator/Cod3Can!

Slide 14



Your Lab Environment for Remediation

You will also log in to your Windows and Linux nodes in order to write remediation and run chef-client in local mode.

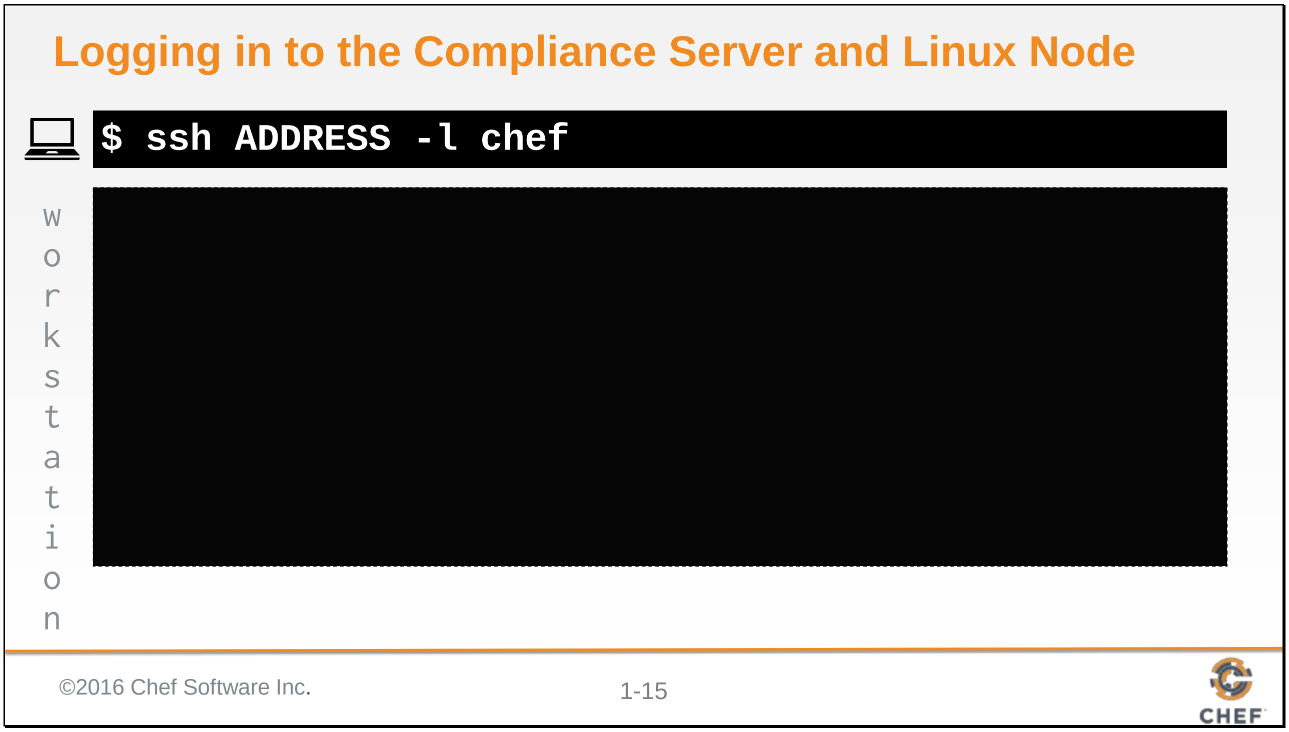
This is so you can use those nodes as virtual workstations while writing remediation.

Nodes to run Compliance tests against AND use as workstations for writing remediation

The dotted lines indicate that those sessions will only be used to write and test remediation. In this scenario, your target nodes will act as virtual workstations.

But all scans will only be run via the Compliance server as indicated in the previous slide.

Slide 15



Logging in to the Compliance Server and Linux Node

```
$ ssh ADDRESS -l chef
```

workstation

1-15

This is just an explanation. You don't need to log in to these machines at this time.

You should use an ssh client like PuTTY or a local command prompt to connect to the remote workstation that we assign to you.

Instead of the command shown in this slide, you could also use this command:

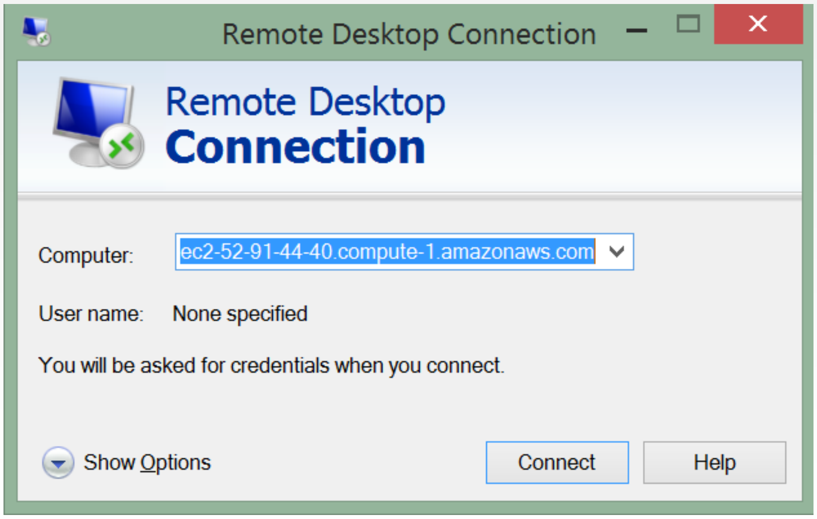
ssh chef@IPADDRESS

For example: ssh chef@52.90.140.22

Slide 16

Logging in to the Remote Windows Node

workstation



Computer: ec2-52-91-44-40.compute-1.amazonaws.com

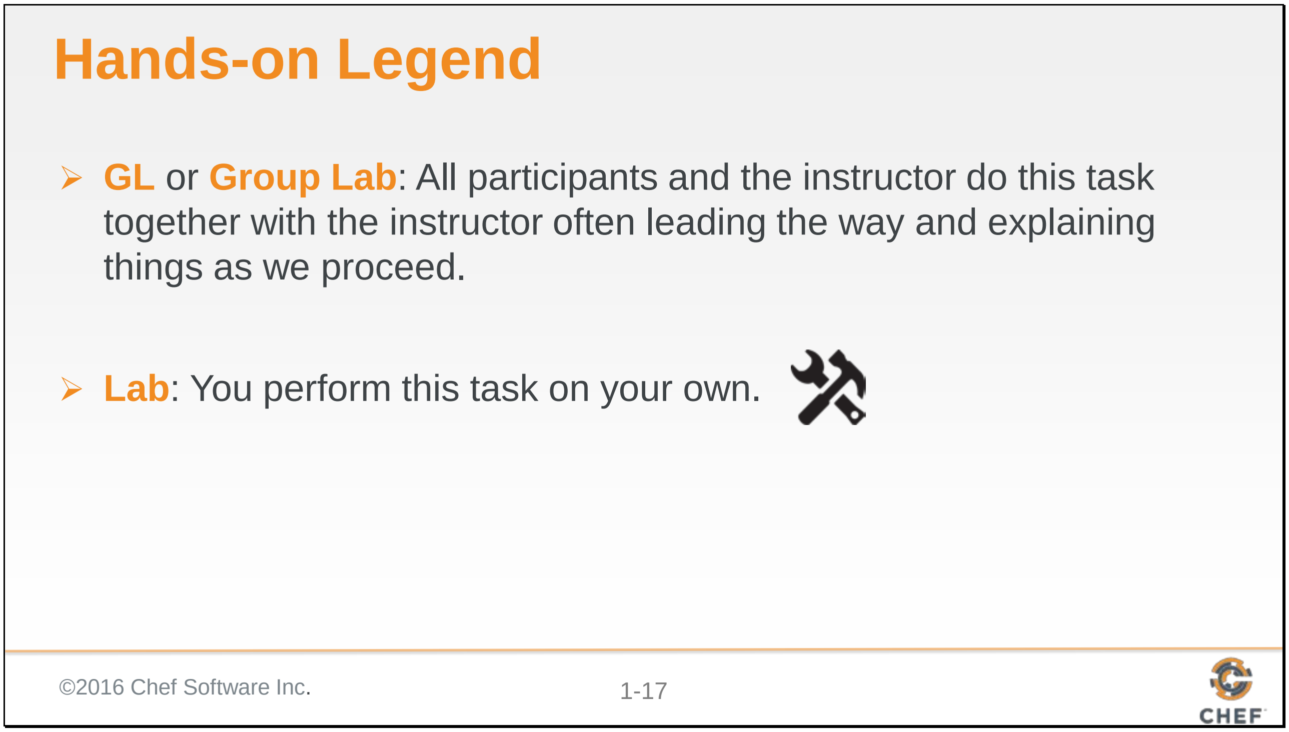
User name: None specified

You will be asked for credentials when you connect.

This is just an explanation. You don't need to log in to these machines at this time.

You should have installed on your laptop a Windows Remote Desktop Connection which you'll only use to write Windows remediation later in this course.

Slide 17



Hands-on Light Legend

- **GL** or **Group Lab**: All participants and the instructor do this task together with the instructor often leading the way and explaining things as we proceed.
- **Lab**: You perform this task on your own. 🛠

Slide 18

CHEF™