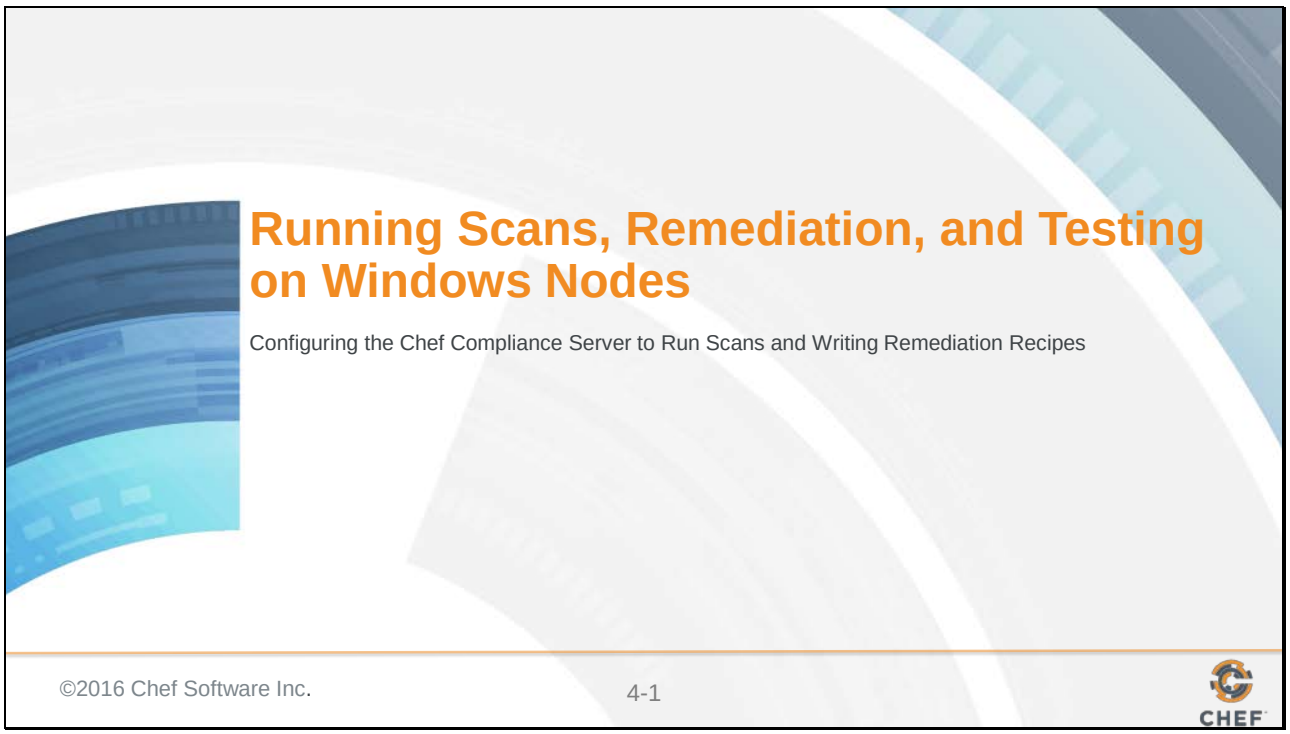
4: Running Scans, Remediation, and Testing on Windows Nodes



Instructor Note: The quiz at the end of this module is virtually identical to the quiz in 03-initial-configuration-scans (Linux version). This is because the concepts are the same so you can skip the quiz in the module if you already covered them in the preceding module.

Slide 2

Objectives

After completing this module, you should be able to:

- Add a Windows node to test for compliance.
- Run a Compliance scan.
- Test for compliance with InSpec from the CLI.
- Remediate a compliance issue.
- Use Test Kitchen to test your remediation.
- Rescan the node and ensure compliance.

Slide 3

EXERCISE

Group Lab: Adding a Node to Scan

Objective:

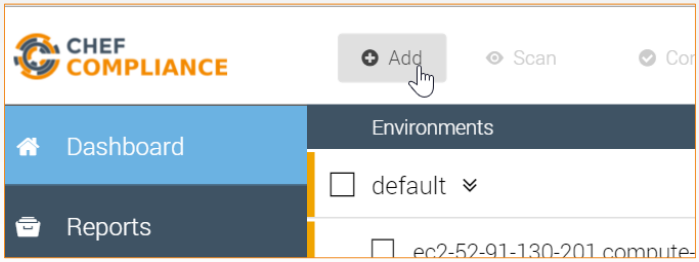
- ❑ Add a Windows Node to Scan
- ❑ Test connectivity

CHEF

Slide 4

GL: Adding a Node to Scan

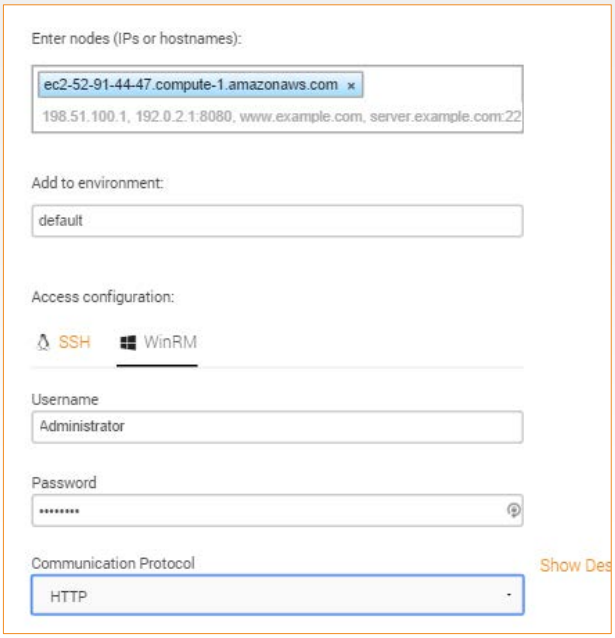
1. From your Chef Compliance Dashboard, click Add Node.



Slide 5

GL: Adding a Node

2. From the resulting page, enter the Windows node's FQDN or IP address.
3. Select the **default** environment.
4. Click the **WinRM** Access configuration.
5. Type **Administrator** in the **Username** field.
6. Type the password (**Cod3Can!**) in the password field.



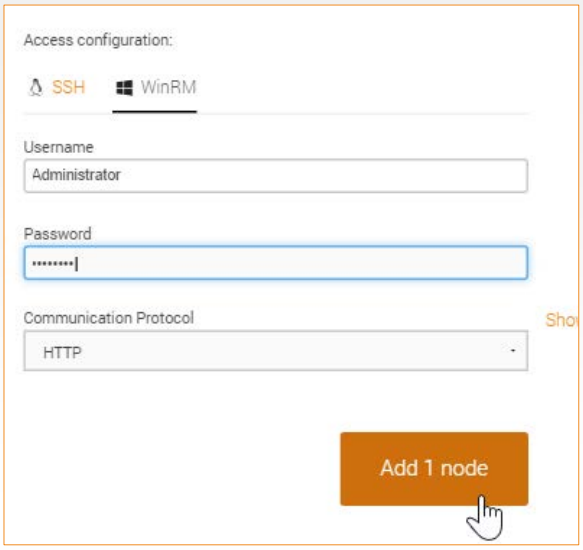
Be sure you are using the hostname of the Windows target node that you noted previously in class.

In the workplace, the target node's username and password will likely be different than shown in this example.

Slide 6

GL: Adding a Node to Scan

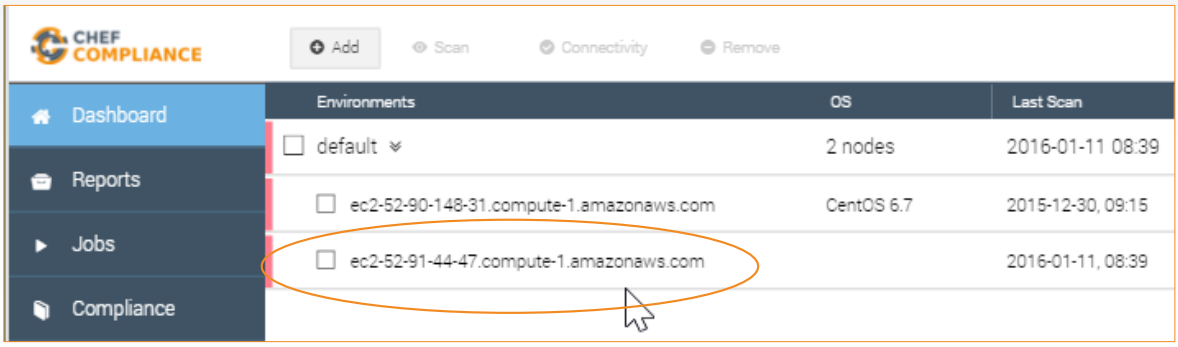
7. Ensure the **HTTP** Communication Protocol is set.
8. Click the **Add 1 node** button.



Slide 7

GL: Adding a Node to Scan

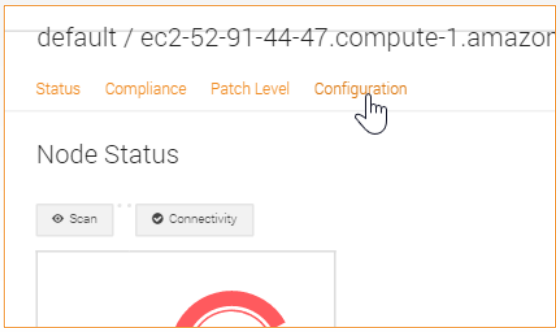
At this point your Compliance Dashboard should list the node you just added. In the next step we'll modify the Windows node name to make it easier to differentiate it from your Linux node.



Slide 8

GL: Modify the Node Name

1. Click the **Windows node**.
2. From the resulting page, click **Configuration**.



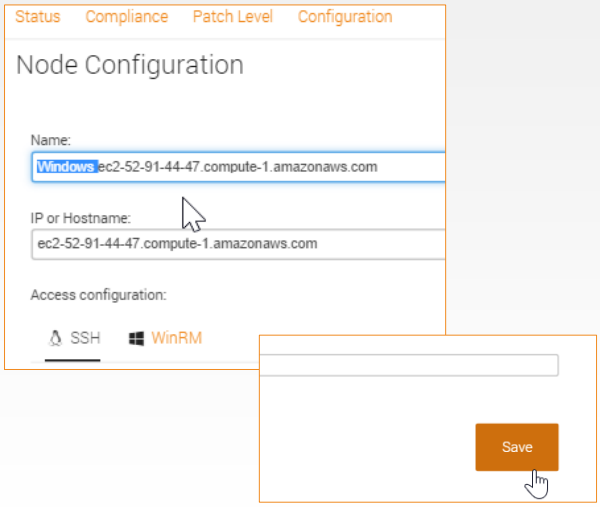
Slide 9

GL: Modify the Node Name

3. Type **Windows** at the beginning of the **Name:** field.

   Important: Do not change the value in the **IP or Hostname** field because that field is used to connect to your node.

4. Click **Save**.



Slide 10

GL: Modify the Node Name

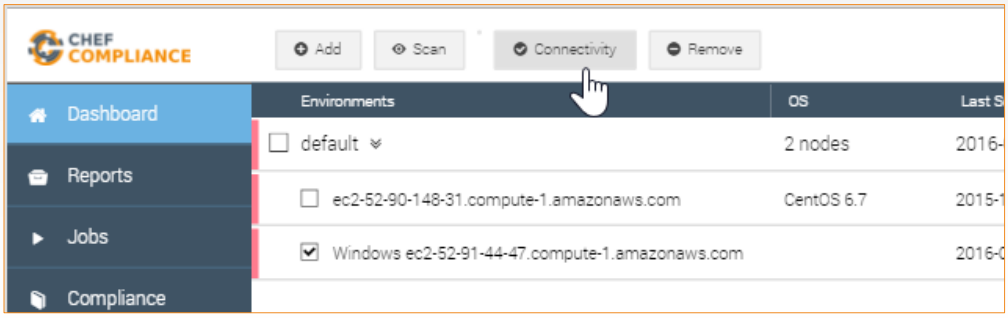
Now you can more easily differentiate your Windows node from your Linux node.

CHEF

Slide 11

GL: Testing Connectivity to your Node

1. Click the **check box** next to your Windows node and then click the **Connectivity** button.

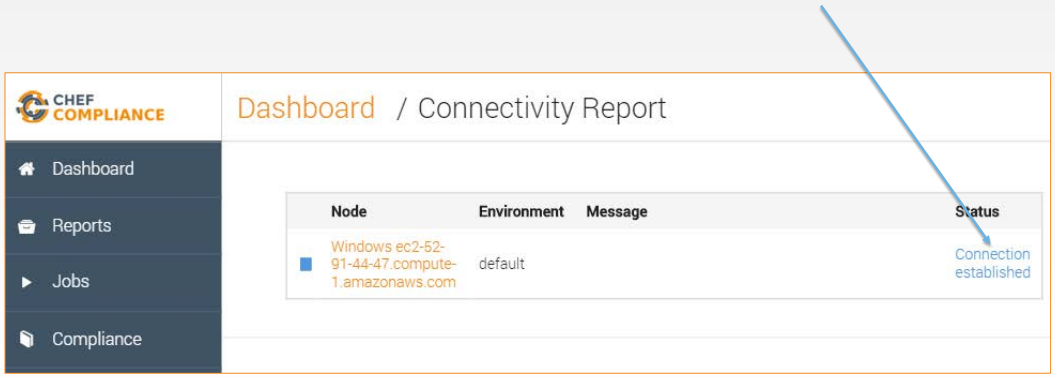


CHEF

Slide 12

GL: Testing Connectivity to your Node

The Status column of your node should now indicate **Connection established**.



If your Status column does not indicate `**Connection established**`, please notify the instructor.

Instructor Note: I have seen where a Windows Connectivity test will fail, but then a scan will work. After the scan is successful, the Connectivity test will start working. Almost like the Windows target was sleepy. Usually happens after the windows node sits idle for a while.

Slide 13

EXERCISE

Group Lab: Running a Scan

Objective:

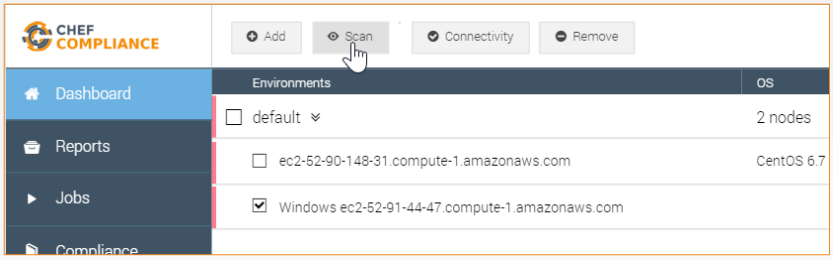
- ❑ Run a Compliance scan.
- ❑ View the output of a scan.

CHEF

Slide 14

GL: Running a Scan

1. Click the **check box** next to your node and then click the **Scan** button.



CHEF

Slide 15

GL: Running a Scan

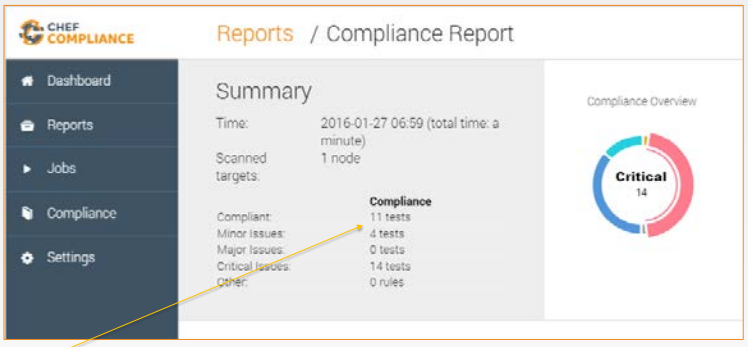
2. From the resulting page, check the **base/windows** profile and uncheck any other check boxes.

3. Click the **Scan now** button.

Slide 16

Scan Results

A Compliance Report should now display and your scan results should be similar to that shown here.



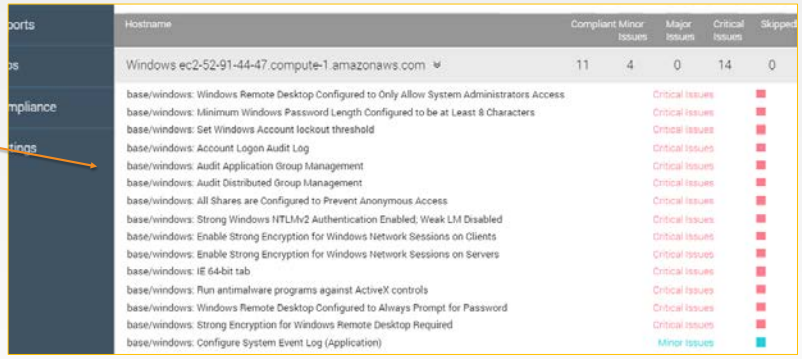
Notice how in the upper Summary section in this example, 11 tests were compliant and 14 tests show critical issues with ssh.

Instructor Note: This and the following slide should be used for a discussion of the scan results. The Group Lab continues after that.

Slide 17

Scan Results

The bottom half of the Compliance Report shown here has a table of details of the scan, similar to what you saw in the Linux example.



Notice how one of the critical issues regards Strong Windows NTMLv2 Authentication Enabled

The bottom half of the Compliance Report has a table of details of test results.

These are sorted by severity so the critical issues are listed at the top and the compliant items are at the bottom of the list.

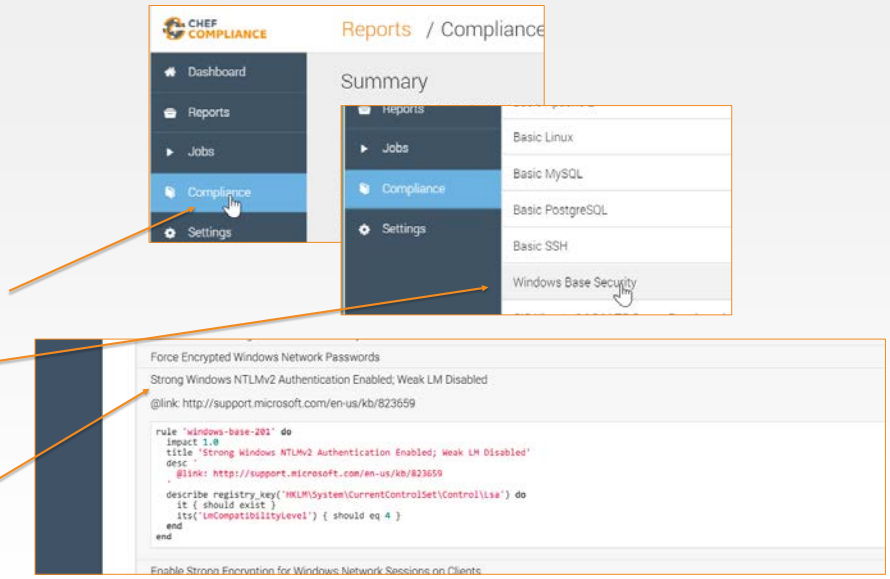
If you click an issue as shown here, a bit more information about the issue displays, but that's not really telling us much.

Slide 18

GL: Profile

To view the InSpec code that comprises this profile, do the following:

1. Click the **Compliance** button.
2. Click the relevant profile category (**Windows Base ...**).
3. Scroll down and click the **Strong Windows NTLMv2...** profile.



Note that the `rule` designation will be changed to `control` in an upcoming release.

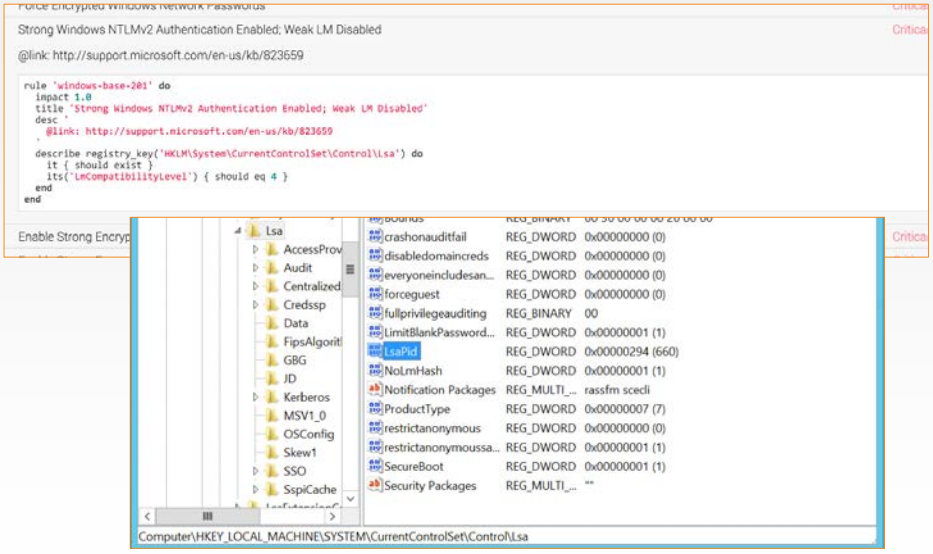
Instructor Note: Now we continue the Group Lab but you should stop as needed to explain what this code means.

Slide 19

Discussion: InSpec Profile Code

You can see in the bottom image where the Registry Key is not set.

In a production environment you'd want to write a Chef recipe to remediate this issue.



Slide 20

PROBLEM

Let's Remediate the Issue

Now that we've identified the issue, let's write a recipe on the target node to remediate the issue.

Then we'll run the compliance scan again to see if we successfully remediated the issue.

Note: In this course we will write a recipe directly on the node that we're running scans on. Of course in a production environment you will likely write such recipes locally and upload them to Chef Server. Then the nodes would converge the recipes on their next chef-client run.

CHEF

Slide 21

EXERCISE

GL: Remediating the Issue

Objective:

- ❑ Write a remediation recipe on that node
- ❑ Test for compliance with InSpec from the command line interface (CLI)
- ❑ Converge the recipe
- ❑ Rescan the node and ensure compliance

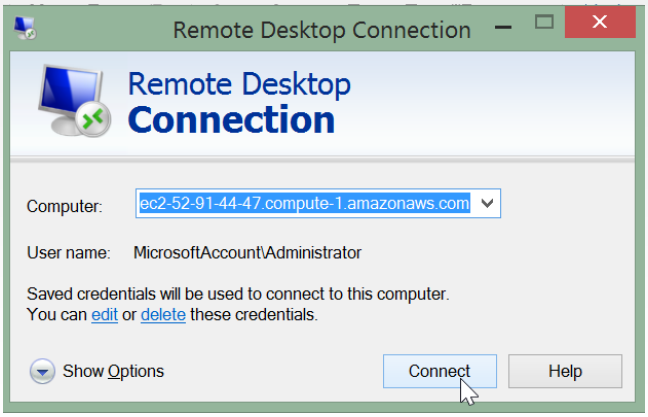
CHEF

Slide 22

GL: Remediating the Issue

Log in to your target node (not your compliance server node) using your RPD client.

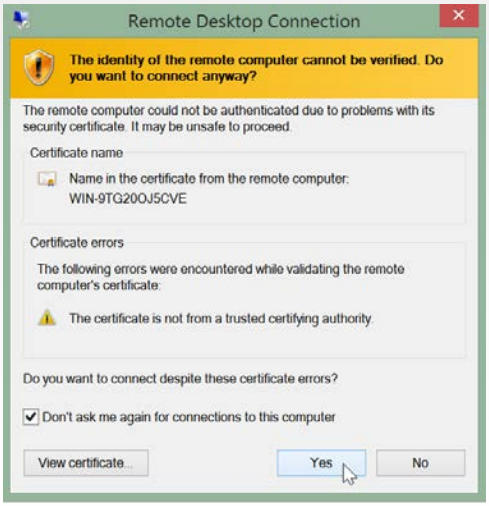
You can use only the IP address instead of the FQDN that this image shows.



Slide 23

GL: Remediating the Issue

If you get a warning like this, click **Yes**.



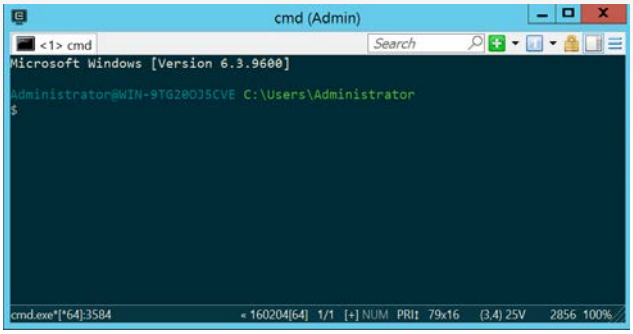
Slide 24

GL: Remediating the Issue

Double-click the ConEmu(x64) icon on the Windows desktop to start that terminal.

At this point the ConEmu terminal should display and you should be in the home directory.

C:\Users\Administrator



CHEF

GL: Create and Change to a 'cookbooks' Directory

```
$ mkdir cookbooks
$ cd cookbooks
```

From the home directory (C:\Users\Administrator\), create a `**cookbooks**` directory and navigate into it.

CHEF

Slide 26

GL: Create a Windows Access Cookbook

```
$ chef generate cookbook windows_access
```

```
Compiling Cookbooks...
Recipe: code_generator::cookbook
  * directory[C:/Users/Administrator/cookbooks/windows_access] action create
    - create new directory C:/Users/Administrator/cookbooks/windows_access
  * template[C:/Users/Administrator/cookbooks/windows_access/metadata.rb] action
create_if_missing
    - create new file C:/Users/Administrator/cookbooks/windows_access/metadata.rb
    - update content in file C:/Users/Administrator/cookbooks/windows_access/metadata.rb from
none to 18be67
    (diff output suppressed by config)
  * template[C:/Users/Administrator/cookbooks/windows_access/README.md] action
create_if_missing
    - create new file C:/Users/Administrator/cookbooks/windows_access/README.md
    - update content in file C:/Users/Administrator/cookbooks/windows_access/README.md from
none to 481e5e
```


CHEF

Slide 27

GL: Create an Authentication Recipe

```
$ chef generate recipe windows_access authentication
```

```
Compiling Cookbooks...
Recipe: code_generator::recipe
  * directory[./windows_access/spec/unit/recipes] action create (up to date)
  * cookbook_file[./windows_access/spec/spec_helper.rb] action create_if_missing (up to date)
  * template[./windows_access/spec/unit/recipes/authentication_spec.rb] action
create_if_missing
    - create new file ./windows_access/spec/unit/recipes/authentication_spec.rb
    - update content in file ./windows_access/spec/unit/recipes/authentication_spec.rb from
none to 021637
    (diff output suppressed by config)
  * template[./windows_access/recipes/authentication.rb] action create
    - create new file ./windows_access/recipes/authentication.rb
    - update content in file ./windows_access/recipes/authentication.rb from none to 11d9b9
    (diff output suppressed by config)
```


CHEF

Slide 28

GL: Write the Authentication Recipe

~/cookbooks/windows_access/recipes/authentication.rb

```
# Cookbook Name:: windows_access
# Recipe:: authentication
# Copyright (c) 2016 The Authors, All Rights Reserved.

lsa_key = 'HKLM\System\CurrentControlSet\Control\Lsa'

registry_key lsa_key do
  values [{
    :name => 'LmCompatibilityLevel',
    :type => :dword,
    :data => 4
  }]
end
```


You can use Atom to edit this file.

Slide 29

EXERCISE

GL: Remediating the Issue

Objective:

- ✓ Write a remediation recipe on that node
- ❑ Test for compliance with InSpec from the command line interface (CLI)
- ❑ Converge the recipe
- ❑ Rescan the node and ensure compliance

CHEF

Slide 30

GL: Create the `inspec` Directory

```
$ mkdir windows_access\test\integration\authentication
$ mkdir windows_access\test\integration\authentication\inspec
```

```
    Directory:

C:\Users\Administrator\cookbooks\windows_access\test\integration\authentica...


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
d----          2/9/2016   9:06 PM            inspec
```


CHEF

You should still be in the C:\Users\Administrator\cookbooks\ directory prior to running these commands.

Slide 31

GL: Create the `auth` Specification File

~/cookbooks/windows_access/test/integration/authentication/inspec/auth_spec.rb

```
rule 'windows-base-201' do
  impact 1.0
  title 'Strong Windows NTLMv2 Authentication Enabled; Weak LM Disabled'
  desc '
    @link: http://support.microsoft.com/en-us/kb/823659
  '
  describe registry_key('HKLM\System\CurrentControlSet\Control\Lsa') do
    it { should exist }
    its('LmCompatibilityLevel') { should eq 4 }
  end
end
```


CHEF

You can use Atom to create this file.

Slide 32

GL: Run InSpec from the CLI

```
$ inspec exec
windows_access\test\integration\authentication\inspec\auth_spec.rb
```

```
.F

Failures:

  1) Registry Key HKLM\System\CurrentControlSet\Control\Lsa
LmCompatibilityLevel should eq 4
     Failure/Error: its('LmCompatibilityLevel') { should eq 4 }

       expected: 4
            got: nil
```


CHEF

This command assumes you are still at C:\Users\Administrator\cookbooks\ when you run it.

Slide 33

EXERCISE

GL: Remediating the Issue

Objective:

- ✓ Write a remediation recipe on that node
- ✓ Test for compliance with InSpec from the command line interface (CLI)
- ❑ Converge the recipe
- ❑ Rescan the node and ensure compliance

CHEF

Slide 34

GL: Converge the Recipe

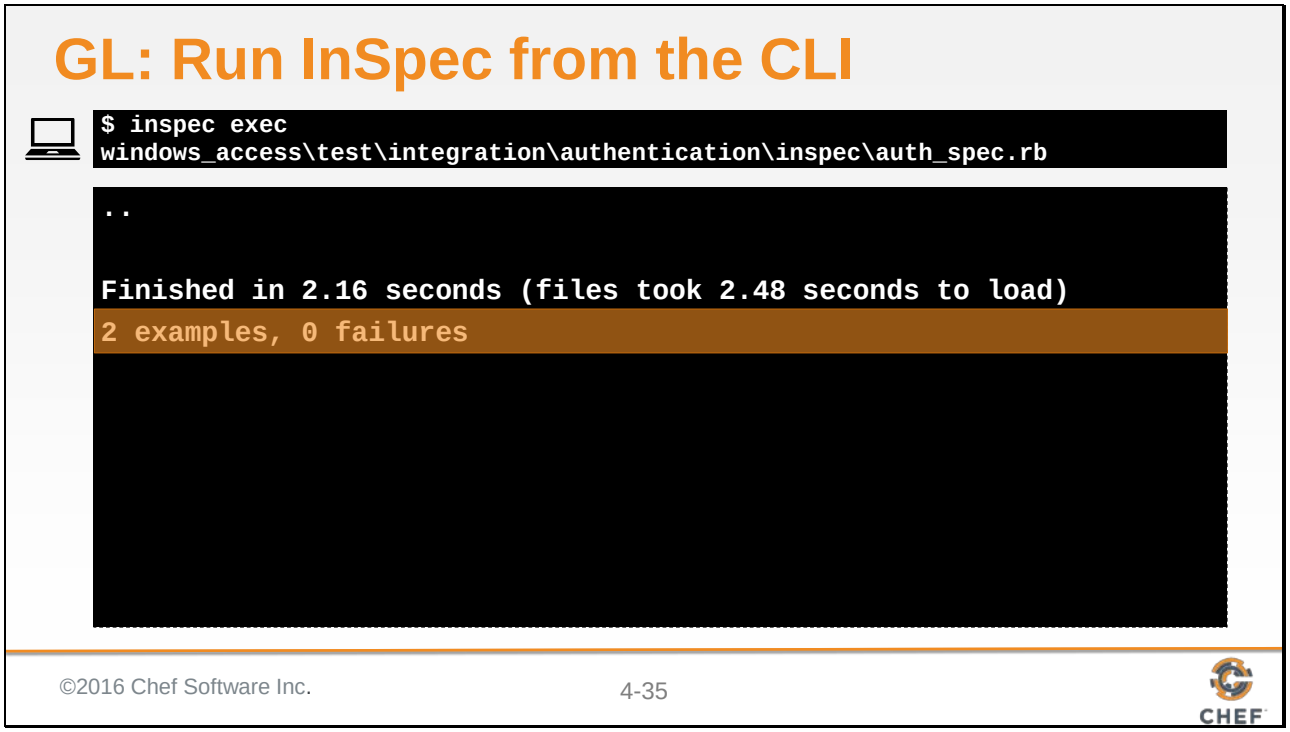
```
$ chef-client --local-mode -r 'recipe[windows_access::authentication]'
```

```
Synchronizing Cookbooks:
  - windows_access (0.1.0)
Compiling Cookbooks...
Converging 1 resources
Recipe: windows_access::authentication
  * registry_key[HKLM\System\CurrentControlSet\Control\Lsa] action create
    - set value {:name=>"LmCompatibilityLevel", :type=>:dword, :data=>4}

Running handlers:
Running handlers complete
Chef Client finished, 1/1 resources updated in 11 seconds
```


This command assumes you are still at C:\Users\Administrator\cookbooks\ when you run it.

Slide 35



This command assumes you are still at C:\Users\Administrator\cookbooks\ when you run it.

Slide 36

EXERCISE

GL: Remediating the Issue

Objective:

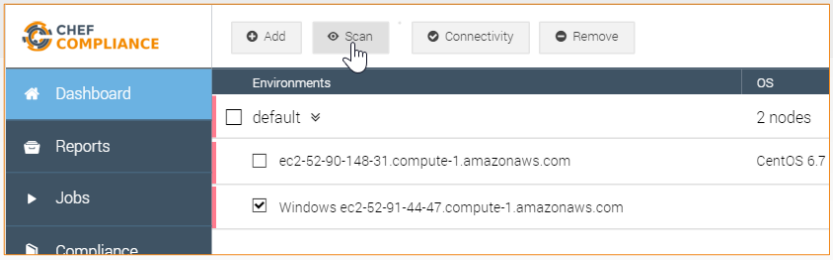
- ✓ Write a remediation recipe on that node
- ✓ Test for compliance with InSpec from the command line interface (CLI)
- ✓ Converge the recipe
- ❑ Rescan the node and ensure compliance

CHEF

Slide 37

GL: Running a Scan

1. Click the **check box** next to your node and then click the **Scan** button.

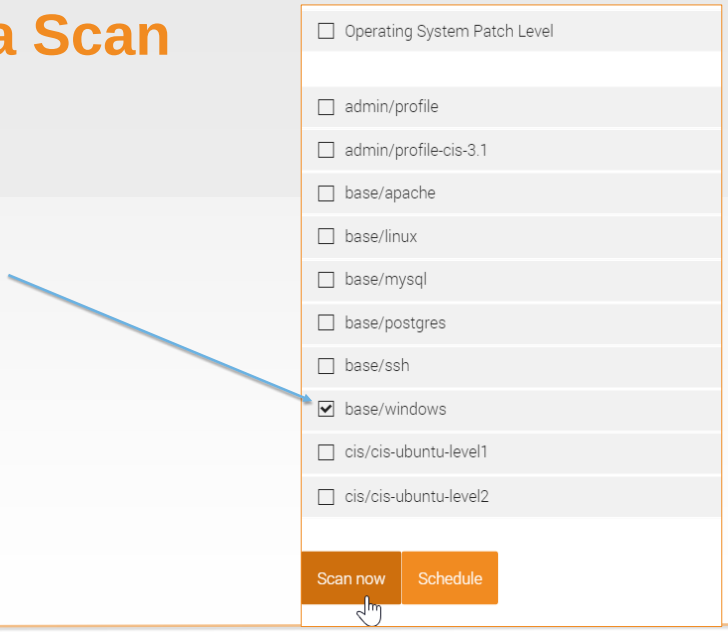


Slide 38

GL: Running a Scan

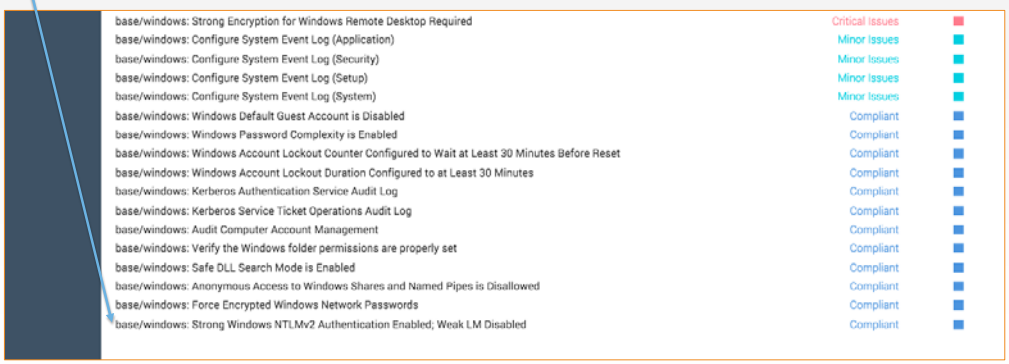
2. From the resulting page, check the **base/windows** profile and uncheck any other check boxes.

3. Click the **Scan now** button.



GL: Results of this Exercise

Your scan should show that the **Strong Windows NTLMv2 Authentication Enabled; Weak LM Disabled** is now compliant.



CHEF

Slide 40

EXERCISE

GL: Remediating the Issue

Objective:

- ✓ Write a remediation recipe on that node.
- ✓ Test for compliance with InSpec from the command line interface (CLI)
- ✓ Converge the recipe.
- ✓ Rescan the node and ensure compliance.

CHEF

Slide 41

Review Questions

1. When adding a node to the Compliance server's dashboard, should you use the node's FQDN or just its IP address?
2. What can `inspec exec` be used for?
3. How are compliance severities defined?
4. Using the image on the right, what section is the actual test?

Instructor Note: This quiz is virtually identical to the quiz in 03-initial-configuration-scans (Linux version). This is because the concepts are the same so you can skip this quiz if you already covered them in the preceding module.
Instructor Note Answers:
1. It doesn't matter...you could use the node's FQDN or just its IP address.
2. `inspec exec` can be used to test a compliance profile against remote hosts, including docker containers.
3. The `impact` value in a Compliance Profile defines severity. See slide 3-22 through slide 3-24 for examples.
4. The `describe` section is the actual test.

Slide 42

Review Questions

5. If a compliance scan tells you that a node is unreachable, what might you use to troubleshoot the connection?

6. What language is used to define controls?

Instructor Note Answers:
5. You could use the Dashboard's "check the connectivity" test, ssh into the target, and/or check the node's configuration in the Web UI (IP address, login credentials.)
6. InSpec.

Slide 43