



CHEF™

Chef Automate

Azure Partner Quickstart Template

Hands-On Lab User Manual

Introduction

The **Continuous Delivery & Compliance with Chef Automate Azure Partner Quickstart Template** launches a DevOps stack that provides an automated provisioning, configuration and integration of Chef Automate that is needed for continuous delivery & compliance of applications, as well as infrastructure code. This is intended as a pilot solution and not production ready.

What You Will Learn

The goal of this solution stack is to provide a continuous delivery & application compliance experience. By walking through the lab in this Launch & Learn session, attendees will learn how this Quickstart template can be used to build and deploy a powerful DevOps solution using Chef products.

About Chef Automate

Chef Automate gives you a full-stack continuous delivery pipeline, automated testing for compliance and security, and visibility into everything that's happening along the way. It builds on Chef for infrastructure automation, InSpec for compliance automation and Habitat for application automation. You can transform your company into a highly collaborative, software-driven organization with Chef Automate as the engine.

About the Compliance feature of Automate

Automate enables you to scan your entire infrastructure for security risks and compliance issues, get reports on risks and issues classified by severity and impact levels, and build automated testing into your deployment pipelines. Chef Compliance includes pre-built profiles that scan for CIS benchmarks to help you get started quickly.

Solution Summary

The Chef Automate Azure test drive is a 30 minute long walkthrough of using Automate's Compliance profiles to rapidly scan a series of Ubuntu 14.04 machines and remediate them to STIG (Security Technical Implementation Guide) specifications.

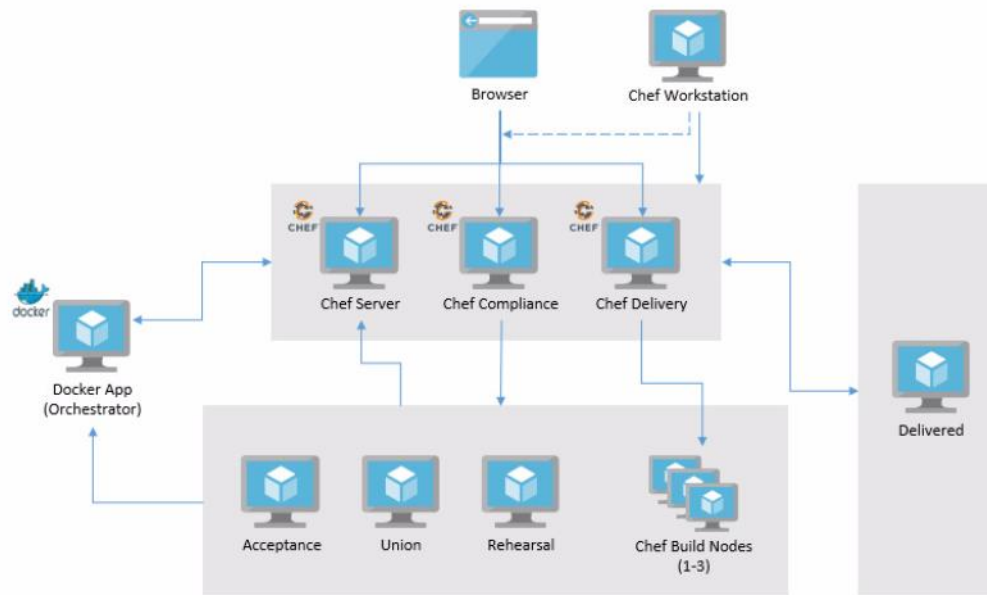
The test drive consists of a Chef Automate cluster, a number of infrastructure nodes and a user's Workstation. The Nodes are managed by Automate, and their policy is configured to scan the node and report scan results back to Automate.

The user will go through the process of triggering a Chef execution on managed machines from the Workstation, using knife-ssh (the remote execution over SSH feature), in the CLI (command-line interface). This simulates the automated periodic Chef execution on nodes in a convergent infrastructure.

Once nodes converge (run chef), they report their status to Automate. The user will examine Automate's visibility dashboards to assess the health and compliance of the node.

The user will then add the STIG hardening cookbook (a configuration policy) to the node's run-list (a list of configuration policies that a node has to process).

Finally, the user will again trigger a Chef execution on the node. The user will observe the STIG policies being applied. Returning back to the Automate dashboard, the user can review the improved state of the node's compliance.



Lab Steps: Scan a Server with Chef Compliance for Registry values

OBJECTIVE

- Connect to the Workstation
- Remotely trigger chef execution on one, or many nodes
- Log in to Automate
- Review the nodes' compliance state in Automate
- Modify the node's run-list to also run the **stig** cookbook
- Remotely trigger chef execution, again
- Review the improved state of the node's compliance

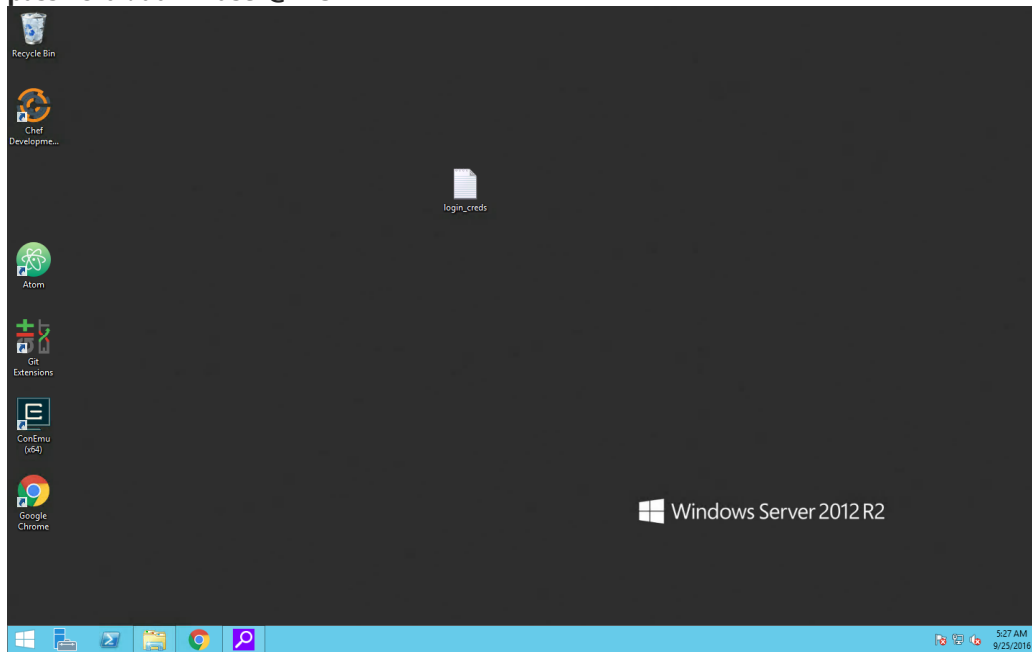
This is what would be good at a high level view.

1.1 Connect to the Workstation

Use your preferred Microsoft Remote Desktop client to connect to the Workstation with the following credentials:

username : adminuser

password : adminuser@123

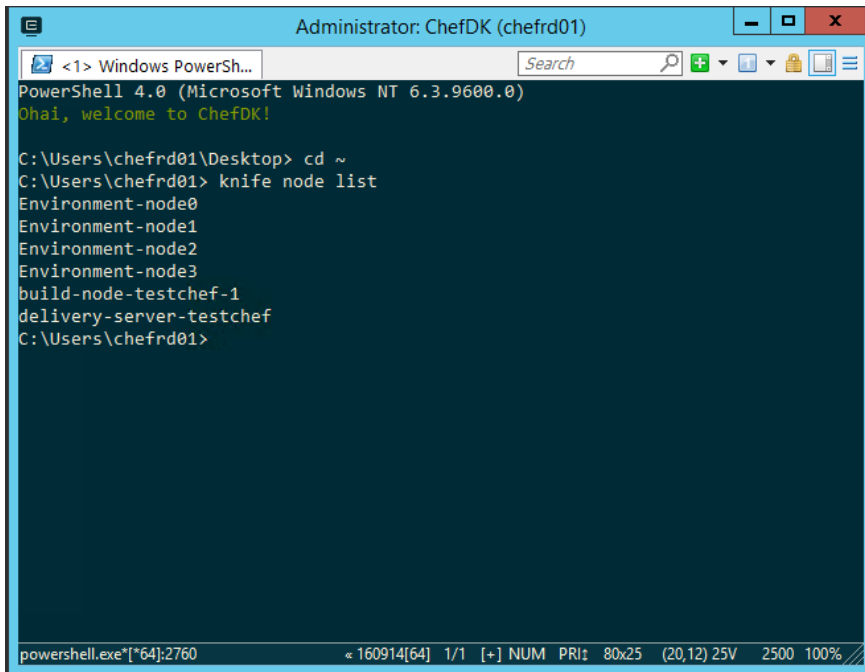


Once logged in, double-click the Chef Development Kit shortcut on the Desktop. Press OK on the ConEmu prompt.

Let's change to our home directory and run a test:

```
cd ~
```

```
knife node list
```



```
Administrator: ChefDK (chefrd01)
PowerShell 4.0 (Microsoft Windows NT 6.3.9600.0)
Ohai, welcome to ChefDK!

C:\Users\chefrd01\Desktop> cd ~
C:\Users\chefrd01> knife node list
Environment-node0
Environment-node1
Environment-node2
Environment-node3
build-node-testchef-1
delivery-server-testchef
C:\Users\chefrd01>
```

1.2 Remotely trigger Chef execution on one or many nodes

Run this command:

```
knife ssh name:Environment-node0 -a ipaddress -x adminuser 'sudo chef-client'
```

and enter **adminuser@123** when prompted for the password.

This establishes an ssh connection to the node named Environment-node0, over its IP address, as the user adminuser, to run the command sudo chef-client.

```
C:\Users\chefrd01> knife ssh name:Environment-node0 -a ipaddress -x adminuser 'sudo chef-client'
adminuser@10.7.4.6's password:
10.7.4.6 Starting Chef Client, version 12.14.89
10.7.4.6 resolving cookbooks for run list: ["audit_wrapper", "stig"]
10.7.4.6 Synchronizing Cookbooks:
10.7.4.6   - audit_wrapper (0.1.0)
10.7.4.6   - audit (0.14.4)
10.7.4.6   - stig (0.5.4)
10.7.4.6   - sysctl (0.7.5)
10.7.4.6   - logrotate (1.9.2)
10.7.4.6   - ohai (3.0.1)
10.7.4.6 Installing Cookbook Gems:
10.7.4.6 Compiling Cookbooks...
10.7.4.6 Converging 122 resources
10.7.4.6 Recipe: audit::inspec
10.7.4.6   * inspec[inspec] action install
10.7.4.6   * chef_gem[inspec] action install (up to date)
10.7.4.6     - install/update inspec
10.7.4.6     - verifies the inspec version
10.7.4.6   * chef_gem[inspec] action install (up to date)
10.7.4.6
10.7.4.6 Recipe: audit::default
10.7.4.6   * ruby_block[exchange_refresh_token] action run
10.7.4.6     - execute the ruby block exchange_refresh_token
10.7.4.6   * directory[/var/chef/cache/compliance] action create (up to date)
10.7.4.6   * file[/var/chef/cache/compliance/cis-ubuntu14.04lts-level1] action nothing (skipped due to
powershell.exe[*64]:2760
```

This simulates the automated periodic Chef execution on nodes in a convergent infrastructure.

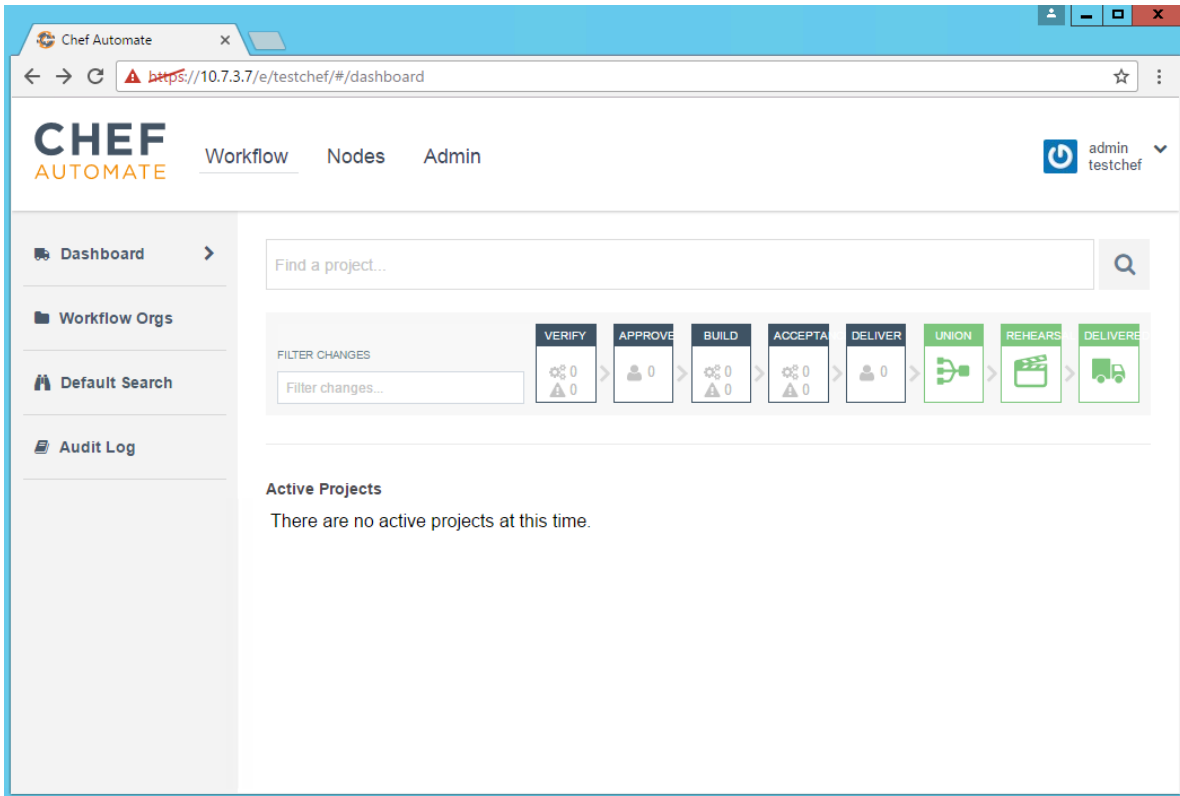
1.3 Log in to Automate

Double-click the Chrome shortcut on the Desktop to open a web browser.

In its address bar enter the following address:

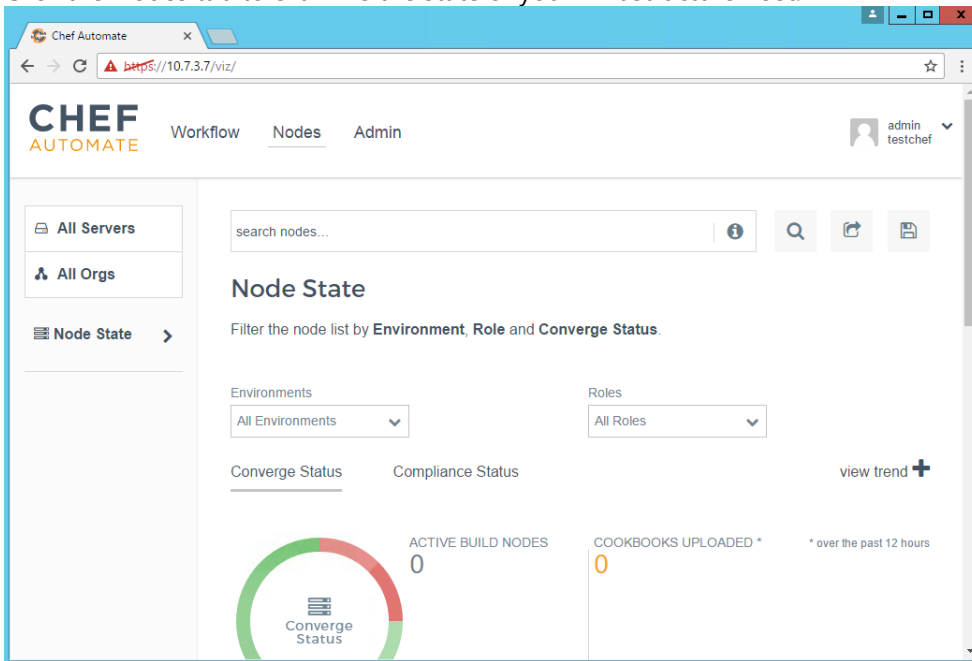
10.7.3.7

This should automatically log you in and open the Workflow dashboard:



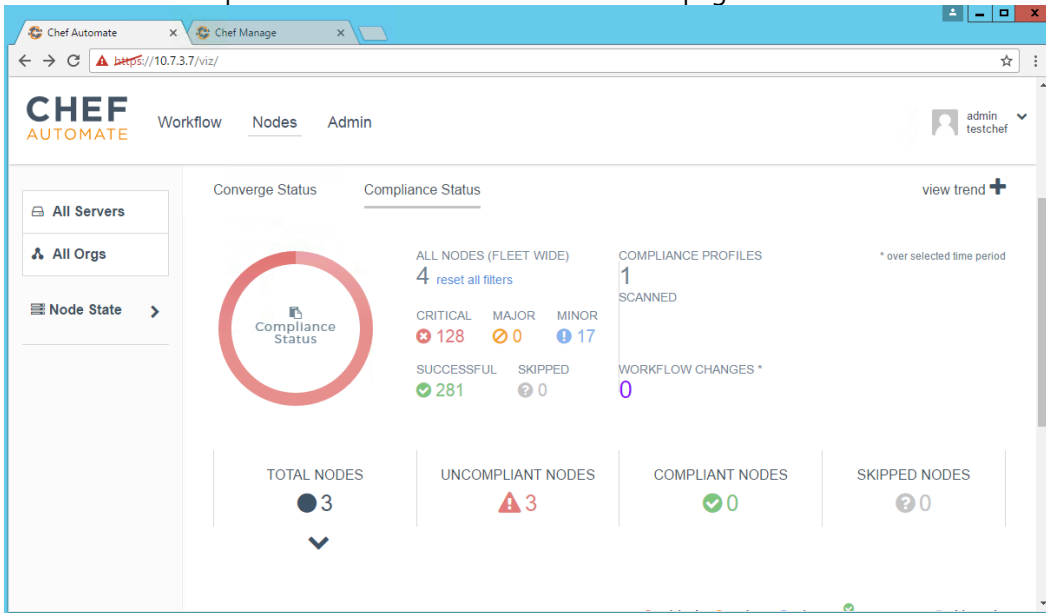
1.4 Review the nodes' compliance state in Automate

Click the Nodes tab to examine the state of your infrastructure fleet.



You should see the state of your node.

Now click the Compliance Status link in the middle of the page:



Scroll down and find your node in the list. Notice the number of Critical failures on your node. Click on your node to be able to examine specific audit controls that failed:

The screenshot shows the Chef Automate interface with the 'Nodes' tab selected. The main content area displays a 'Compliance Scores' donut chart and a summary of scan results. The summary includes the following data:

Category	Count
TOTAL CONTROLS	156
CRITICAL CONTROLS	51
MAJOR CONTROLS	0
MINOR CONTROLS	8
COMPLIANT CONTROLS	83
SKIPPED CONTROLS	14

Additional scan details shown include: SCAN DURATION (5:38 PM - 5:38 PM), SCAN TIME (a few seconds), SCAN INITIATOR (Scheduled), INSPEC VERSION (0.27.1), PROFILES SCANNED (1), and PLATFORM(S) (not defined). On the right, the 'Scan History' sidebar shows a list of recent scans with status indicators (13 failed, 13 critical, 0 major, 0 minor).

The screenshot shows the 'Node Details' page for a specific node. It displays a list of failed audit controls, including 'Set nodev option for /tmp Partition' and 'Set nosuid option for /tmp Partition'. The 'Set nosuid option for /tmp Partition' control is expanded, showing the following details:

Description: The nosuid mount option specifies that the filesystem cannot contain set userid files.

Scan Results:

Status	Message	Start Time	Run Time
Failed	Bash command egrep "[^#]" /etc/fstab awk '{S2 == "/tmp"} { print \$4 }' stdout should match /nosuid/	09/25/2016 5:38 PM	a few seconds

1.5 Modify the node's run-list to also run the stig cookbook

Let's go back to your command prompt and issue a Chef API command to add the **stig** recipe to the node's run list:

```
knife node run list add Environment-node0 recipe[stig]
```

The command should confirm to you that the recipe is now in the list:

```
C:\Users\chefrd01> knife node run list add Environment-node0 recipe[stig]
Environment-node0:
  run_list:
    recipe[audit_wrapper]
    recipe[stig]
C:\Users\chefrd01> |
```

1.6 Remotely trigger chef execution, again

Now that we modified the configuration policy for our node, let's once again simulate what a convergent node would do automatically in production – execute Chef:

```
knife ssh name:Environment-node0 -a ipaddress -x adminuser sudo chef-client
```

and enter **adminuser@123** when prompted for the password.

Watch as the chef execution hardens the node to stig specifications. It will take a few minutes. Your chef execution may fail with the message below:

```
10.7.4.8      service_name "sshd"
10.7.4.8      pattern "sshd"
10.7.4.8      declared_type :service
10.7.4.8      cookbook_name "stig"
10.7.4.8      recipe_name "sshd_config"
10.7.4.8      end
10.7.4.8
10.7.4.8      Platform:
10.7.4.8      -----
10.7.4.8      x86_64-linux
10.7.4.8
10.7.4.8      Running handlers:
10.7.4.8      - AzureExtension::ExceptionHandler
10.7.4.8      Running handlers complete
10.7.4.8      Chef Client failed. 63 resources updated in 04 minutes 34 seconds
C:\Users\chefrd01>
```

Fear not. Simply hit the Up arrow key on your keyboard to show the previous command and hit Enter to run it again:

```
knife ssh name:Environment-node0 -a ipaddress -x adminuser sudo chef-client
```

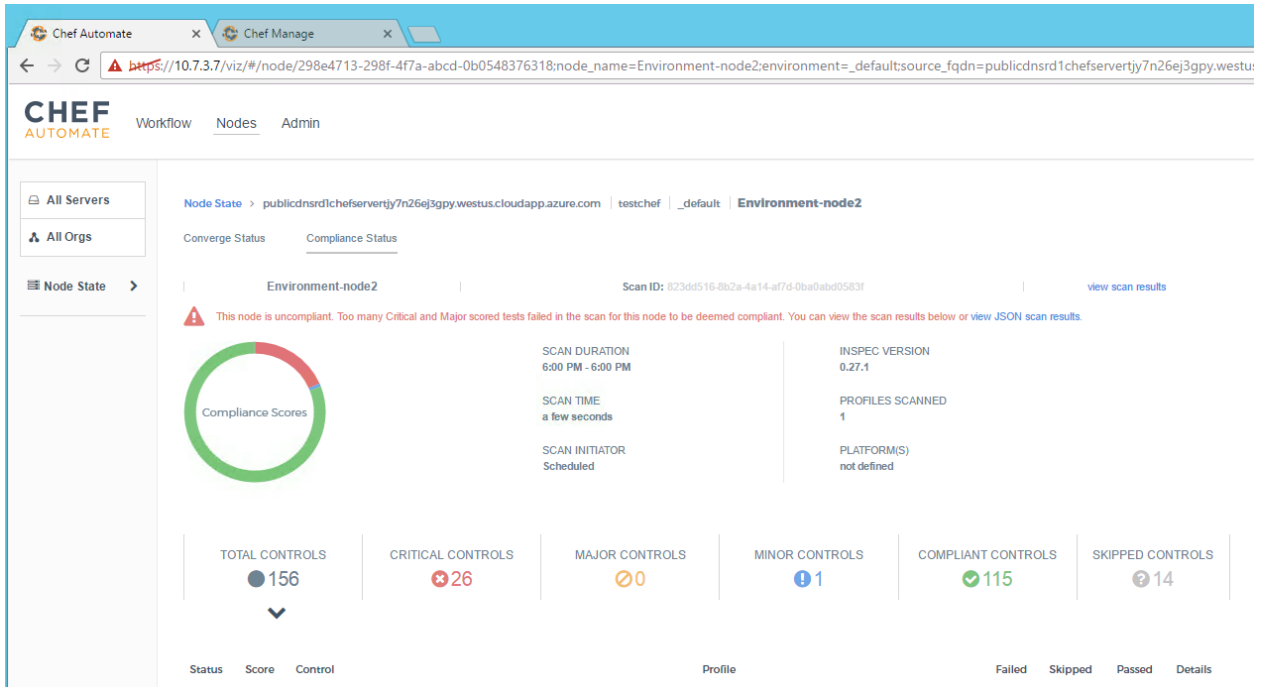
and enter **adminuser@123** when prompted for the password.

You will notice that the second execution is significantly faster. When Chef runs, it only configures the items that have not been properly configured yet:

```
10.7.4.8
10.7.4.8 Chef Client finished, 13/136 resources updated in 23 seconds
C:\Users\chefrd01> |
```

1.7 Review the improved state of the node's compliance

Alright, let's go back to our browser. Refresh the Automate page, hit the Nodes tab, click on Compliance Status. We should now be able to see our node with an improved compliance profile:



2 Key Takeaways

With Chef Automate, it's easy to maintain the integrity of your infrastructure and keep track of any security or compliance issues. The platform enables automatic remediation and continuous audit capabilities for any vulnerabilities that the system detects.

3 Conclusions & Next Steps

You should now have a better understanding of how Chef Automate can maintain and improve your infrastructure and delivery process.

You will find many other Chef tutorials on <https://learn.chef.io>

If you'd like to learn more about Chef products that can help improve your delivery process, or if you'd like to speak to an official Chef representative, please visit <https://chef.io> or contact us at azuretestdrive@chef.io.

4 Contact Information

To get in touch with Chef, please send us an email at azuretestdrive@chef.io, or select the "Contact Me" button on the test drive launch page.