



InSpec Jumpstart Workshop

Anthony Rees

APAC Solutions Architect - Chef

anthony@chef.io

Workshop Details

- Workshop Instructions
 - Register for the Lab
 - Follow the instructions
 - **<http://bit.ly/2Ns9DJu>**
- Register for a Lab Environment
 - Go to the Spreadsheet
 - Add your name
 - **<http://bit.ly/2NXXag6>**

Automated Testing

Integration and Compliance

Many types of test

Is web server listening on tcp/80?

Is web server delivering the correct content?

Using TLS or SSL?

SSH v2 Configured?

User 'foo' has read no write access to /myapp?

User 'foo' exists?

User 'foo' has read access to /myapp?

User 'foo' does not have sudo access?

User 'foo' does not have read access to /etc?

SSH v1 Configured?

There is zero consistency when testing infrastructure

- All configuration files are proprietary
- All commands have different syntaxes & command line switches
- They're platform specific (RHEL, Debian, Windows, ...)

Introducing...



What is InSpec?

- InSpec provides **consistent** DSL that is **platform agnostic** to check status of **any** component
 - packages
 - files
 - users
 - AWS IAM users
 - AWS S3 Buckets
 - ...
- Complex implementation code abstracted out
- May InSpec profiles exist in the community, and Chef provide key profiles matching industry specific compliance regulations

Bash vs InSpec for testing

- For example, SSH supports two different protocol versions. The original version, SSHv1, was subject to a number of security issues. Please use SSHv2 instead to avoid these.

Scripting Tools

```
> grep "^Protocol" /etc/ssh/sshd_config | sed 's/Protocol //'
```

InSpec

```
describe sshd_config do
  its('Protocol') { should cmp 2 }
end
```

InSpec for AWS

```
describe aws_iam_user(name: 'test_user') do
  it { should have_mfa_enabled }
  it { should have_console_password }
end
```



InSpec for Azure

```
describe azure_virtual_machine(group_name: 'InSpec-Azure', name:
'Linux-Internal-VM') do
  its('size') {should eq 'Standard_DS2_v2' }
  its('location') {should eq 'westeurope' }
  its('admin_username') {should eq 'azure' }
end
```



InSpec is cross platform

- One Language



Oracle Solaris 11



- InSpec for Windows

```
control '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
```

InSpec is Agentless

- InSpec was born out of Rspec and ServerSpec
- No agent needs installed on the target node
- Requires
 - SSH access for Linux nodes
 - WinRM access for Windows



Integration (functional) vs Compliance (security) Tests

Is web server listening on tcp/80?	Integration Test
Is web server delivering the correct content?	Integration Test
Using TLS or SSL?	Compliance Test
SSH v2 Configured?	Integration Test / Compliance Test
User 'foo' has read no write access to /myapp?	Compliance Test
User 'foo' exists?	Integration Test
User 'foo' has read access to /myapp?	Integration Test
User 'foo' does not have sudo access?	Compliance Test
User 'foo' does not have read access to /etc?	Compliance Test
SSH v1 Configured?	Compliance Test

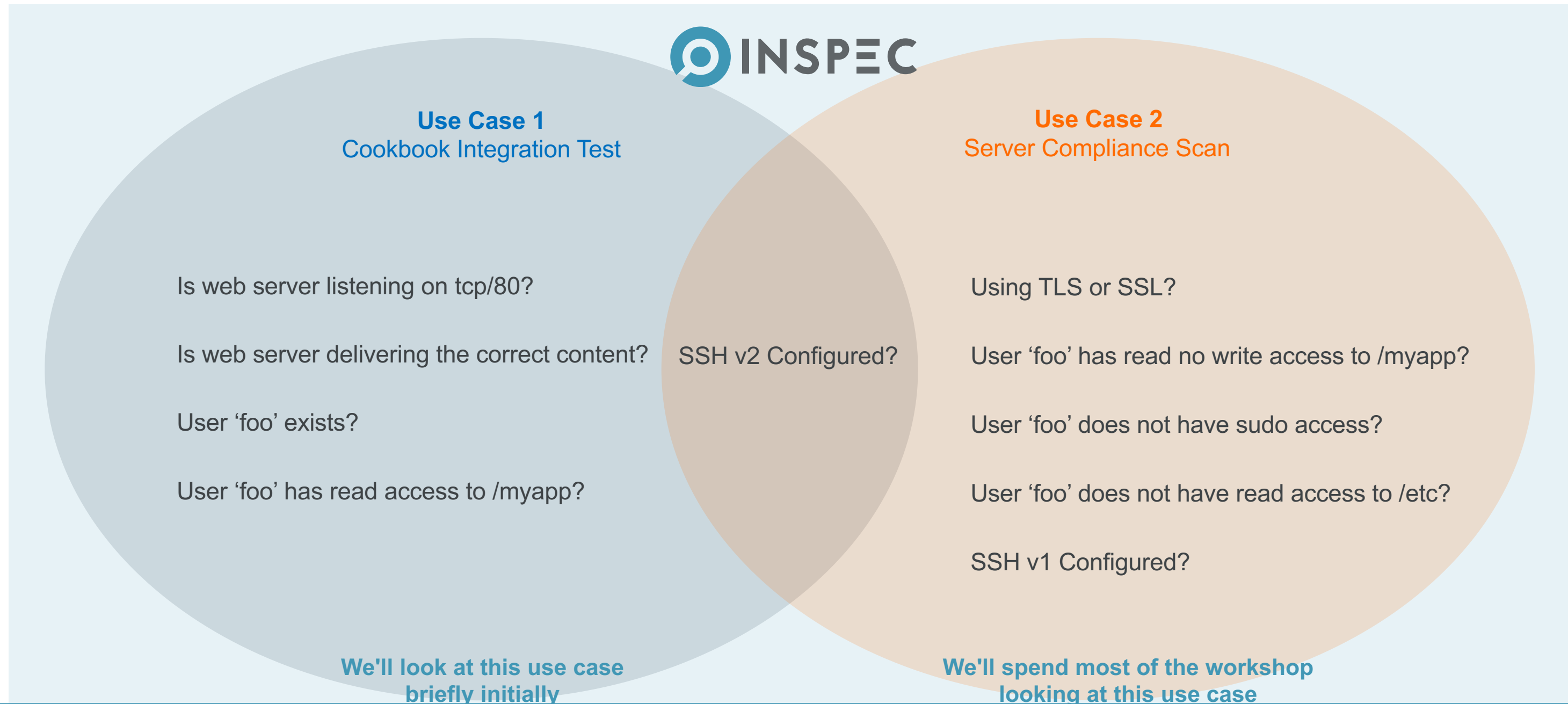
Integration (functional) vs Compliance (security) Tests

Is web server listening on tcp/80?	Integration Test
Is web server delivering the correct content?	Integration Test
User 'foo' exists?	Integration Test
User 'foo' has read access to /myapp?	Integration Test
SSH v2 Configured?	Integration Test / Compliance Test
Using TLS or SSL?	Compliance Test
User 'foo' has read no write access to /myapp?	Compliance Test
User 'foo' does not have sudo access?	Compliance Test
User 'foo' does not have read access to /etc?	Compliance Test
SSH v1 Configured?	Compliance Test

Integration (functional) vs Compliance (security) Tests

Is web server listening on tcp/80?	Integration Test	 Integration Tests (Does the thing work?) <ul style="list-style-type: none">• Tests usually maintained within a cookbook• Invoked by Test Kitchen
Is web server delivering the correct content?	Integration Test	
User 'foo' exists?	Integration Test	
User 'foo' has read access to /myapp?	Integration Test	
SSH v2 Configured?	Integration Test / Compliance Test	 Compliance Scan (Is the thing secure?) <ul style="list-style-type: none">• Tests collated in InSpec profiles and maintained externally, e.g. GitHub, Compliance server• Invoked by `inspec` cli or from Chef Automate Compliance
Using TLS or SSL?	Compliance Test	
User 'foo' has read no write access to /myapp?	Compliance Test	
User 'foo' does not have sudo access?	Compliance Test	
User 'foo' does not have read access to /etc?	Compliance Test	
SSH v1 Configured?	Compliance Test	

Integration AND Compliance Tests – Two Separate Use Cases



InSpec for Integration vs Compliance Testing

Same language - two Distinct Use Cases

InSpec Rules	Integration tests	Compliance scan
Types of Rules	Governed by the application (cookbook) requirements	Generic rules defined by industry security requirements (not governed by the application requirements)
Location of Rules	Shipped with a cookbook	Stored centrally (Compliance server, GitHub)
Invocation	Use Test Kitchen to provision a sandbox environment to perform functional tests of the cookbook	Use InSpec CLI or Chef Automate Compliance to perform compliance tests during development, or in production



Further Resources

Where to go for additional help

Community Resources

- **InSpec** Website, includes tutorials and docs - <http://inspec.io/>
- **#inspec** channel of the **Chef Community Slack** - <http://community-slack.chef.io/>
- InSpec category of the Chef Mailing List - <https://discourse.chef.io/c/inspec>
- Compliance Profiles on the Supermarket - https://supermarket.chef.io/tools?type=compliance_profile
- Open Source Project - <https://github.com/chef/inspec>

