InSpec for Network Devices:
Extending Compliance-as-Code to the Network Administrator

Julian C. Dunn
Director of Product Marketing, Chef Software Inc.
jdunn@chef.io | @julian_dunn
Agenda

• What is InSpec and Compliance as Code?
• InSpec Basics
• InSpec for Cloud Networking Compliance
• InSpec for Network Device Compliance
• How to get started
You have a lot of things in your network: servers, containers, network devices, clouds, Kubernetes, etc.

How do you know they’re installed and configured correctly?
Compliance is Often A Communication Problem
Introducing InSpec

InSpec helps express security & compliance requirements as code and incorporate it directly into the delivery process.

Systems shall have a Mandatory Access Control system installed and enabled.

```ruby
control 'ensure_selinux_installed' do
  impact 1.0
  title 'Ensure SELinux is installed'
  desc <<-EOD
    SELinux provides Mandatory Access Control
    EOD
  describe package('libselinux') do
    it { should be_installed }
  end
end
```
Traditional Compliance Versus InSpec

BEFORE:
- DEV
- QA
- STAGING
- SECURITY REVIEW
- PRODUCTION

AFTER:
- DEV
- QA
- STAGING
- SECURITY INSPECTION
- PRODUCTION

CONTINUOUS COMPLIANCE

Compliance and policy configuration throughout the SDLC
InSpec 1.0: Servers & Containers

control "cisecurity.benchmarks_rule_5.2.9_Ensure_SSH_PermitEmptyPasswords_is_disabled" do
  title "Ensure SSH PermitEmptyPasswords is disabled"
  desc "The PermitEmptyPasswords parameter specifies if the SSH server allows login to accounts with empty password strings. Rationale: Disallowing remote shell access to accounts that have an empty password reduces the probability of unauthorized access to the system"
  impact 1.0
  tag "cis-rhel7-2.1.1": "5.2.9"
  tag "level": "1"
  tag "type": ["Server", "Workstation"]
  describe ssqd_config do
    its(' PermitEmptyPasswords') { should eq ' no' }
  end
end
A Quick Primer on InSpec Terminology

- Resources
- Controls
- Profiles
- Nodes
- Scan Jobs
Network Automation is Necessary for Business Agility

"Network teams are realizing that they often lag behind other domain groups in embracing automation as a way to meet growing business demand. Hence, they're seeking methods to address the delta as rapidly as possible."

Fewer than 10% of network teams use any automation tools today.

Source: Gartner Market Guide for Network Automation (March 2018)
InSpec 2.0: Networks and Clouds

Write compliance policies for all aspects of cloud configuration:
• Virtual machines
• Security groups
• Block storage security policies
• Networking
• Identity and access management
• Log management

AWS and Microsoft Azure are supported; Google Cloud Platform support in beta.
Example: Microsoft Azure Server Policy

control 'azure-virtual-machine-policy-1.0' do
  impact 1.0
  title 'Ensure that the webserver has been set up as expected'

  describe azure_virtual_machine(group_name: 'Inspec-Azure', name: 'webserver') do
    its('location') { should cmp 'westeurope' }
    its('tags') { should include 'Description' }
    its('disk_size_gb') { should be >= 25 }
  end
end
Example: Avoid AWS S3 Mistakes

describe aws_s3_bucket(bucket_name: 'secret_files') do
  it { should exist }
  it { should_not be_public }
  it { should have_access_logging_enabled }
end
Example: Microsoft Azure Network Policy

control 'azure-generic-virtual-network-2.0' do
  impact 1.0
  title 'Ensure that the virtual network has been created with the correct address space and subnet'
  describe azure_generic_resource(group_name: 'Inspec-Azure', name: 'Inspec-VNet') do
    its('type') { should cmp 'Microsoft.Network/virtualNetworks' }
    its('location') { should cmp 'westeurope' }
    its('properties.addressSpace.addressPrefixes') { should include '192.168.14.0/24' }
    its('properties.subnets.count') { should eq 1 }
  end
end
Extending InSpec to Traditional Network Devices

- Recently extended InSpec to certain Cisco network devices (IOS 12.x and 15.x) with support for others soon.
- Commercial product (Chef Automate) includes agentless scanner & premium content (e.g. CIS Benchmarks for Cisco IOS)
General Use on Cisco IOS

# Verify the contents of the running configuration
describe cisco_ios_running_config do
  it { should have_line 'no ip http server' } end

# Validate the output of arbitrary commands
describe cisco_ios_command('show cdp') do
  its('output') { should match /CDP is not enabled/ } end
Example: Auditing Interfaces

# Verify that at least one Loopback interface exists
describe cisco_ios_interfaces.where(name: /Loopback/) do
  its('entries') { should_not be_empty }
end

# Verify that the FastEthernet0/0 interface has the correct IP
describe cisco_ios_interface('FastEthernet0/0') do
  its('ip_address') { should eq '10.2.3.1' }
end
Verify SNMP User and Group Configuration

# Verify that no SNMP users are using the MD5 privacy protocol
describe cisco_ios_snmp_users.where(privacy_protocol == 'MD5') do
  its('entries') { should be_empty }
end

# Verify that all SNMP groups are using the 'v3 priv' security model
describe cisco_ios_snmp_groups.where(security_model != 'v3 priv') do
  its('entries') { should be_empty }
end
Disable Cisco Discovery Protocol (CDP) service at device level. Rationale: The Cisco Discovery Protocol is a proprietary protocol that Cisco devices use to identify each other on a LAN segment. It is useful only in network monitoring and troubleshooting situations but is considered a security risk because of the amount of information provided from queries. In addition, there have been published denial-of-service (DoS) attacks that use CDP. CDP should be completely disabled unless necessary.

Cisco IOS Command 'show cdp' stdout should match /.*CDP is not enabled$/

```
expected "Global CDP information:
	Sending CDP packets every 60 seconds\r\n	Sending a holdtime value of 180 seconds\r\n	Sending CDPv2 advertisements is enabled"
```

```
Demo
Coming Soon: InSpec 3.0

- New custom resources (types)
- New device types and clouds (e.g. Alibaba Cloud, NETCONF-compatible devices, etc.)
Summary

- InSpec is an open-source language for compliance-as-code
- Compliance-as-code approaches can be used for security/audit verification as well as validation of configuration correctness
- InSpec >=2.0 can validate configurations of servers, clouds, network devices
- Get started today at www.inspec.io
Thank You

jdunn@chef.io | @julian_dunn
https://www.inspec.io/