Chef Principles Certification Exam Answers – CP101

5th August 2021

CP101 Chef Principles Certification Exam Answers

Question: When a chef-client runs, which of the following is NOT retrieved from the Chef server?
Q01

- Run-list. <-- This is retrieved from the chef-server
- chef-client configuration. <-- This is retrieved from the chef-server
- ✓ Data bag items.
- Cookbooks. <-- This is retrieved from the chef-server

Check Source

Question: What happens when you don't specify a resource's action?
Q02

- ~~You get an error message but the chef-client run continues~~.
- ~~You get an error message and the chef-client run halts~~.
- ✓ The default action is assumed.

Question: What is a Chef Resource?
Q03

- ~~the equivalent of a Chef cookbook~~.
- ~~the equivalent of a Chef recipe~~.
- ✓ an item that can be configured on your system.

Question: Which of the following statements is true regarding nodes?
Q04

- ~~The Chef server dynamically builds each node prior to a chef-client run~~.
- ✓ The chef-client pulls node data in JSON format from the Chef server at the start of the run.
- Nodes are stored on the Chef server as JSON objects that contains just the run-list and node name.
- ~~Nodes are represented on the Chef server as JSON objects that contain all the node data~~.

Check Source: https://docs.chef.io/chef_client_overview/

Question: Which is NOT valid about a run-list?
Q05

- ✗ Every node must have a unique run-list assigned to it.
- ✗ ~~A run-list defines some of the information necessary for Chef to configure a node into the desired state~~.
- ✓ A run-list is a list of roles and/or recipes that are run in the order specified.
- ✗ ~~A run-list is stored as a node object element which can be queried via knife~~.

Question: When must you list a resource's attributes?
Q06

- ~~Immediately after the resource name~~.
- ~~Immediately after the actions~~.
- ✓ You can list them anywhere within the resource block.

Question: Where do you define the source of dependent cookbooks?
Q07

- ✓ Policyfile.rb
- metadata.rb
- Policyfile.lock.json

Question: What Chef Infra command would you use to lock your policies in place by creating a Policyfile.lock.json file?
Q08

- ~~chef push Policyfile.rb~~
- ✓ chef install Policyfile.rb
- ~~chef init Policyfile.rb~~

Question: You would like to run an InSpec test locally which is stored on Github. Which of the following commands would achieve this?
Q09

- ~~inspec test https://github.com/PATH/TO/INSPEC/PROFILE~~
- ✓ inspec exec https://github.com/PATH/TO/INSPEC/PROFILE
- ~~inspec check https://github.com/PATH/TO/INSPEC/PROFILE~~
- ~~It is not possible. The InSpec profile needs to stored locally on the node~~.

Question: You want to use an InSpec profile that is stored at https://github.com/security to scan a docker container. How would you achieve this?
Q10

- ~~inspec exec https://github.com/security -t docker -i ContainerID~~
- ~~inspec profile https://github.com/security -t docker -i ContianerID~~
- ✓ inspec exec https://github.com/security -t docker://ContainerID
- ~~Download the profile from Github, then scan the container as usual. Profiles must be stored locally when scanning containers~~.

Source: https://lollyrock.com/posts/inspec-for-docker/

Question: Where do you define custom InSpec resources?
Q11.

- ~~providers folder~~
- ~~resources folder~~
- ✓ libraries folder <<-- Resources may be added to profiles in the libraries folder
- ~~top directory of the inspec profile~~

Source: https://docs.chef.io/inspec/dsl_resource/

Question: To limit an InSpec run to only certain controls, you would:
Q12.

- ✓ Specify the –controls argument.
- ~~Specify the –limit argument~~.
- ~~grep the output~~.

Example: inspec supermarket exec dev-sec/linux-baseline --controls package-08

Question: You want to make sure that an AWS ec2 instance named 'ec2-instance' is running. What should the InSpec test look like?
Q13.

~~describe ec2('ec2-instance') do~~

~~it { should be_running }~~

~~end~~

describe aws('ec2-instance') do

✓

it { should be_running }

end

~~describe ec2('aws-ec2-instance') do~~

~~it { should_be running }~~

~~end~~

~~describe ami('ec2-instance') do~~

~~it { should_be running }~~

~~end~~

Question: In the following InSpec test, what exactly is being tested?
Q14.

describe file('/etc/sysconfig') do

it { should be_directory }

it { should be_executable.by('owner') }

it { should_not be_writable }

it { should_not be_readable.by_user('Tom') }

end

- ✓ It tests that /etc/sysconfig is a directory, that the directory is executable by the owner, the directory can not have files added or removed, and the contents of the directory cannot be read by a user named Tom.
- ~~It tests that the file /etc/sysconfig is executable by the owner of the file, the file can not modified, and the contents of the file cannot be read by a user named Tom.~~
- ~~It tests that /etc/sysconfig is a directory, that the directory has a mode of 0544, and the contents of the directory cannot be read by a user named Tom~~.
- ~~It tests that the file /etc/sysconfig is executable by the owner, the file has a mode of 0544, contents of the file cannot be read by a user named Tom.~~

Question: When defining custom InSpec resources, what language(s) are available to use?
Q15.

- ~~Ruby~~
- ~~Inspec DSL and Ruby~~
- ✓ Inspec DSL and Custom Resource DSL and Ruby
- ~~Inspec DSL and Chef Recipe DSL and Ruby~~

Question: You would like to run an InSpec test locally which is stored on Github. Which of the following commands would achieve this?
Q16.

- ~~inspec test https://github.com/PATH/TO/INSPEC/PROFILE~~
- ✓ inspec exec https://github.com/PATH/TO/INSPEC/PROFILE
- ~~inspec check https://github.com/PATH/TO/INSPEC/PROFILE~~
- ~~It is not possible. The InSpec profile needs to stored locally on the node.~~

Question: You want to use an InSpec profile that is stored at https://github.com/security to scan a docker container. How would you achieve this?
Q17.

- ~~inspec exec https://github.com/security -t docker -i ContainerID~~
- ~~inspec profile https://github.com/security -t docker -i ContianerID~~
- ✓ inspec exec https://github.com/security -t docker://ContainerID
- ~~Download the profile from Github, then scan the container as usual. Profiles must be stored locally when scanning containers~~.

Question: Where do you define custom InSpec resources?
Q18.

- ~~providers folder~~
- ~~resources folder~~
- ✓ libraries folder
- ~~top directory of the inspec profile~~

Source: https://docs.chef.io/inspec/dsl_resource/

Question: To limit an InSpec run to only certain controls, you would:
Q19.

- ✓ Specify the –controls argument.
- ~~Specify the –limit argument~~.
- ~~grep the output~~.

Question: You want to make sure that an AWS ec2 instance named 'ec2-instance' is running. What should the InSpec test look like?
Q20.

~~describe ec2('ec2-instance') do~~

~~it { should be_running }~~

~~end~~

describe aws('ec2-instance') do

✓

it { should be_running }

end

~~describe ec2('aws-ec2-instance') do~~

~~it { should_be running }~~

~~end~~

~~describe ami('ec2-instance') do~~

~~it { should_be running }~~

~~end~~

Question: In the following InSpec test, what exactly is being tested?
Q21.

describe file('/etc/sysconfig') do

it { should be_directory }

it { should be_executable.by('owner') }

it { should_not be_writable }

it { should_not be_readable.by_user('Tom') }

end

- ✓ It tests that /etc/sysconfig is a directory, that the directory is executable by the owner, the directory can not have files added or removed, and the contents of the directory cannot be read by a user named Tom.
- ~~It tests that the file /etc/sysconfig is executable by the owner of the file, the file can not modified, and the contents of the file cannot be read by a user named Tom.~~
- ~~It tests that /etc/sysconfig is a directory, that the directory has a mode of 0544, and the contents of the directory cannot be read by a user named Tom.~~
- ~~It tests that the file /etc/sysconfig is executable by the owner, the file has a mode of 0544, contents of the file cannot be read by a user named Tom~~.

Question: When defining custom InSpec resources, what language(s) are available to use?
Q22.

- ~~Ruby~~
- ~~Inspec DSL and Ruby~~
- ✓ Inspec DSL and Custom Resource DSL and Ruby
- ~~Inspec DSL and Chef Recipe DSL and Ruby~~

Question: You want to run an inspec test (test.rb) on a remote node with ssh. The remote node does NOT have InSpec or chef-client installed using ssh. How would you do this?
Q23.

- ✓ inspec exec test.rb -t ssh://user@hostname
- ~~It is not possible. The target node must have InSpec installed.~~
- ~~It is not possible. The target node must have chef-client installed.~~
- ~~inspec exec ssh://user@hostname test.rb~~

Question: How are Studio dependencies defined in a Habitat Plan file that should not be included in the package artifict when running build?
Q24.

- ~~pkg_deps~~
- ~~pkg_build_deps~~
- ~~pkg_run_deps~~
- ✓ pkg_deps_ignored

Question: How can you search for a specific file within packages installed inside the Studio?
Q25.

- ✓ The hab pkg provides command
- ~~The hab pkg search command~~
- ~~Examining the package manifest in Builder~~
- ~~Running hab pkg export and opening the artifact with an editor~~

Question: The core Habitat Builder origin:
Q26.

Check all that apply

- ~~Only includes build tools, like curl~~
- ✓ Is a set of foundation packages
- ✓ Is managed and versioned by the Habitat maintainers
- ~~Provides packages that cover every use-case~~
- ~~Can be used as dependencies for custom pacakges~~

Question: Where is Habitat package metadata defined?
Q27.

- ~~The metadata.rb file~~ this is only for the Chef Infra
- ~~Habitat Builder~~
- ✓ The Plan file in habitat/plan.sh file we define pkg_version, pkg_name, pkg_release. these are the metadata
- ~~Within the package source repository~~

Question: What kind of file is generated within the Habitat Studio when running build?
Q28.

- ~~Plan.sh~~
- ✓ .hart
- ~~.tar~~
- ~~.rpm~~

Question: What package export formats are available within the Habitat Studio?
Q29.

Select all that apply.

- ~~.hart~~
- ✓ .tar.gz
- ~~.rpm~~
- ~~.msi~~
- ✓ Apache Mesos
- ✓ Cloud Foundry
- ✓ docker

Source: https://docs.chef.io/habitat/pkg_exports/

Question: You have just uploaded a package to Habitat Builder and wish to pull it into your Studio for testing. On running hab pkg install, you receive an error that no suitable package candidate can be found. What is a potential reason for this error?
Q30.

- ~~A package release channel wasn't specified in the install command~~
- ✓ The package hasn't been promoted to the stable channel
- ~~You are not logged into the correct Builder origin~~
- ~~You need to authenticate your Studio session with Builder~~

Question: What is the purpose of the Habitat Supervisor?

Q31.

Select all that apply.

- ✓ Starts and monitors child services
- ~~Retrieve resource metadata from cloud providers~~
- ✓ Monitor information from other Supervisors
- ✓ Reconfigure services with lifecycle hooks

The Supervisor is a process manager that has two primary responsibilities.
- First, it starts and monitors child services defined in the plan it is running.
- Second, it receives and acts upon information from the other Supervisors to which it is connected.

*** A service will be reconfigured through application lifecycle hooks if its configuration has changed.

Source: https://docs.chef.io/habitat/sup/

Question: You would like to run an InSpec test locally which is stored on Github. Which of the following commands would achieve this?

Q32.

- ~~inspec test https://github.com/PATH/TO/INSPEC/PROFILE~~
- ✓ inspec exec https://github.com/PATH/TO/INSPEC/PROFILE
- ~~inspec check https://github.com/PATH/TO/INSPEC/PROFILE~~
- ~~It is not possible. The InSpec profile needs to stored locally on the node~~.

Question: Which of the following is a valid way to install InSpec on a node?

Q33.

- ~~gem install kitchen-inspec~~
- ~~gem install serverspec~~
- ✓ Install Chef Workstation
- ~~gem install chefspec~~

Source: https://github.com/inspec/inspec

Question: Manually scanning for compliance is often:

Q34.

- Time-consuming.
- Error-prone.
- Non-portable.
- ✓ All of these.

Question: In the Automate Compliance dashboard, what language are compliance tests written in?

Q35.

- Chef
- Ruby
- ✓ InSpec

Question: You want to run an InSpec test locally that is stored locally on the node. How would you do this?

Q36.

- ~~inspec test /PATH/TO/PROFILE~~
- ~~inspec compliance /PATH/TO/PROFILE~~
- ✓ inspec exec /PATH/TO/PROFILE
- ~~inspec check /PATH/TO/PROFILE~~

Question: Where are compliance profiles stored?

Q37.

- ~~On target nodes~~.
- ✓ On the Chef Automate Compliance server.
- ~~On Chef Infra Server~~.

Question: You want to run an inspec test (test.rb) on a remote node with ssh. The remote node does NOT have InSpec or chef-client installed using ssh. How would you do this?

Q38.

- ✓ inspec exec test.rb -t ssh://user@hostname
- ~~It is not possible. The target node must have InSpec installed.~~
- ~~It is not possible. The target node must have chef-client installed.~~
- ~~inspec exec ssh://user@hostname test.rb~~

Question: You can log in to the compliance scanner with

Q39.

- ✓ inspec compliance login.
- ~~chef compliance login.~~
- ~~chef exec compliance login.~~

inspec compliance login

Source: https://docs.chef.io/inspec/cli/

Question: In the following Chef Compliance package, choose the correct specification for control 5.2.4 from the CIS Sample Linux benchmark that enables both scanning and remediation.

Q40.

—

✗ (a) provider: Chef

benchmark: CIS Sample Linux

provider_version: v.1.0.0

controls:

– id: 5.2.4_Ensure_SSH_Protocol_is_set_to_2

scan:

run: true

remediate:

~~run: false~~

—

✗ (b) provider: Chef

benchmark: CIS Sample Linux

provider_version: v.1.0.0

controls:

– id: 5.2.4_Ensure_SSH_Protocol_is_set_to_2

scan:

run: true

remediate:

** justification missing

run: true

—

✓ (c) provider: Chef

benchmark: CIS Sample Linux

provider_version: v.1.0.0

controls:

– id: 5.2.4_Ensure_SSH_Protocol_is_set_to_2

scan:

run: true

remediate:

run: true

justification: “ACME corporation requires strict compliance standards for SSH”

—

(d) provider: Chef

benchmark: CIS Sample Linux

provider_version: v.1.0.0

controls:

– id: 5.2.4_Ensure_SSH_Protocol_is_set_to_2

scan:

run: true

remediate:

run: true

~~overlay: “ACME corporation requires strict compliance standards for SSH”~~

Question: What feature is used within a Chef Compliance control to ignore a scan, permanently or for a defined time period?

Q41.

- ✓ Waivers
- ~~Justifications~~
- ✓ Overlays
- ~~Exceptions~~

Question: In the following Chef Compliance package, choose the correct specification for control 5.2.14 from the CIS Sample Linux benchmark that grants a waiver until July 1st, 2023.

Q42.

—

(a) provider: Chef

benchmark: CIS Sample Linux

provider_version: v.1.0.0

controls:

– id: 5.2.14_Ensure_SSH_access_is_limited

scan:

run: true

expiration_date: 2023-07-01

remediate:

run: false

waiver:

start_date_utc: “— 2020-12-01 08:25:57.571436000 Z\n”

expiration_date_utc: “— 2023-07-01 08:25:57.571522000 Z\n”

identifier: ticket_14500

justification: “Security waiver granted until expiration date”

—

(b) provider: Chef

benchmark: CIS Sample Linux

provider_version: v.1.0.0

controls:

– id: 5.2.14_Ensure_SSH_access_is_limited

scan:

run: false

expiration_date: 2023-07-01

remediate:

run: false

waiver:

start_date_utc: “— 2020-12-01 08:25:57.571436000 Z\n”

expiration_date_utc: “— 2023-07-01 08:25:57.571522000 Z\n”

identifier: ticket_14500

justification: “Security waiver granted until expiration date”

—

(c)

provider: Chef

benchmark: CIS Sample Linux

provider_version: v.1.0.0

controls:

– id: 5.2.14_Ensure_SSH_access_is_limited

scan:

~~run: true~~

expiration_date: 2023-07-01

remediate:

run: false

waiver:

~~begin_date_utc~~: “— 2020-12-01 08:25:57.571436000 Z\n”

expiration_date_utc: “— 2023-07-01 08:25:57.571522000 Z\n”

identifier: ticket_14500

reasoning: “Security waiver granted until expiration date”

—

(d) provider: Chef

benchmark: CIS Sample Linux

provider_version: v.1.0.0

controls:

– id: 5.2.14_Ensure_SSH_access_is_limited

scan:

run: false

expiration_date: 2023-07-01

remediate:

run: false

waiver:

begin_date_utc: “— 2020-12-01 08:25:57.571436000 Z\n”

expiration_date_utc: “— 2023-07-01 08:25:57.571522000 Z\n”

identifier: ticket_14500

reasoning: “Security waiver granted until expiration date”

Question: How is remediation enabled for a Chef Compliance control?

Q43.

- In bulk, within the Habitat package’s config.yml file
- In bulk, within the InSpec benchmark code
- ✓ Per-control, within the Habitat package’s config.yml file
- Per-control, within the InSpec benchmark code

Question: Where are Chef Compliance profiles customized and turned into consumable packages?

Q44.

- ~~The Chef Habitat Workspace~~
- ✓ The Chef Habitat Studio
- ~~The Chef Habitat Builder~~
- ~~The Automate Compliance Dashboard~~

Question: What components comprise the Chef Compliance solution?

Q45.

- Chef Premium Compliance Profiles
- Chef Audit
- Chef Remediation
- ✓ All of the above

Question: What open-source Chef tool is used to package Chef Compliance profiles and controls into consumable artifacts?

Q46.

- ~~Chef Workstation~~
- ~~Chef InSpec~~
- ✓ Chef Habitat
- ~~Chef Automate~~

Question: What language does Chef Compliance use to provide a common language for security stakeholders to collaborate?

Q47.

- ~~CIS~~
- ~~InSpector~~
- ✓ InSpec
- ~~ServerSpec~~

Er Priya Dogra