**Integrate Chef Compliance with Chef Server**

**1)Prepare Chef Compliance:**

To prepare Chef Compliance for integration with the Chef server, do the following:

**Step 1**.From a command shell, run the following command:

**$ sudo -i**

**$ chef-compliance-ctl connect chef-server --non-interactive true -- chef-app-id 'compliance\_server' --auth-id 'Chef Server' --insecure true --compliance-url 'https://compliance.test'**

**Step 2**. Copy the command delimited by ---

---

CHEF\_APP\_ID="compliance\_server" AUTH\_ID="Chef Server" COMPLIANCE\_URL="https://compliance.test"\n

INSECURE\_SSL="true" CHEF\_GATE\_COMPLIANCE\_SECRET="7fef11649f95d4de9e9334b103144f58e3e1fde12f49e\n

5a70579143a7b48f7ebf25a0dab9c58b86460e392cb942a95b345bb" OIDC\_CLIENT\_ID="l0IL\_ak15qZzkQtP\_Orc5\n

E0Gdka\_3CYFVWHIjLKoh5o=@compliance.test" bash <( curl -k https://compliance.test/static/chef-gate.sh )

---

**Step 3**.Now, run the following command:

**$ chef-compliance-ctl reconfigure**

This will create a file under /opt/chef-compliance/sv/core/env/CHEF\_GATE\_COMPLIANCE\_SECRET

**Step 4**.Restart the Chef Compliance core service now:

**$ chef-compliance-ctl restart core**

**2)Configure the Chef Server**

To configure the Chef server for integration with Chef Compliance, do the following:

**Step 1**. From the Chef server shell, run the command delimited by --- from the previous section. For example:

**$ sudo -i**

**$ CHEF\_APP\_ID="compliance\_server" AUTH\_ID="Chef Server" COMPLIANCE\_URL="https://compliance.test"\n**

INSECURE\_SSL="true" CHEF\_GATE\_COMPLIANCE\_SECRET="7fef11649f95d4de9e9334b103144f58e3e1fde12f49e\n

5a70579143a7b48f7ebf25a0dab9c58b86460e392cb942a95b345bb" OIDC\_CLIENT\_ID="l0IL\_ak15qZzkQtP\_Orc5\n

E0Gdka\_3CYFVWHIjLKoh5o=@compliance.test" bash <( curl -k https://compliance.test/static/chef-gate.sh )

This will install a chef-gate service on the Chef server that enables the Chef server to act as an OpenID Connect (OIDC) resource server, plus enables the chef-client to request Chef Compliance profiles, and then report back to Chef Compliance the results of profile scans.

**Step 2.** When finished, a command will be printed at the end of the output similar to:

chef-compliance-ctl auth add --client-id "50b3447fd3db4f59d0160611eb25703f348887b6760482df5\n

bd3ae2303f93c2d" --client-secret "3880ed856a14fce2201459e93d667da8fcd22f8ebbc1ad94d8a0a1195\n

9834b91" --id "Chef Server" --type ocid --chef-url https://chef.compliance.test --insecure true

Copy this line. It will be used in the next section.

**3)Configure Chef Compliance**

To configure Chef Compliance for integration with the Chef server, do the following:

**Step 1**.From the Chef Compliance shell, run the command that was printed at the end of the output while configuring the Chef server. For example:

chef-compliance-ctl auth add --client-id "50b3447fd3db4f59d0160611eb25703f348887b6760482df5\n

bd3ae2303f93c2d" --client-secret "3880ed856a14fce2201459e93d667da8fcd22f8ebbc1ad94d8a0a1195\n

9834b91" --id "Chef Server" --type ocid --chef-url https://chef.compliance.test --insecure true

**Step 2.** When finished, reconfigure Chef Compliance:

**$ sudo -i**

**$ chef-compliance-ctl reconfigure**

**4)Test Integration**

**Step 1.**Go to the Chef Compliance web interface and click the Use a **different provider link.**

**Step 2.**The default provider is Compliance Server. Switch it to **Chef Server**.

**Step 3**.Then accept the **authorization request**

**Step 4.**Only nodes under management by Chef that successfully run **audit::default** will show up in Chef Compliance.

**5) Scan Managed Nodes**

Once the integration is complete, the audit cookbook allows Chef Compliance profiles to be run as part of a chef-client run. Profiles are downloaded from Chef Compliance. Audit results are sent back to Chef Compliance, which uses the Chef server as a proxy.

The audit cookbook must be uploaded to the Chef server, and then added to one (or more) recipes before the chef-client can run profiles on a node.

**6)Download the audit Cookbook**

The **audit** cookbook is available at the following locations:

• https://supermarket.chef.io/cookbooks/audit

• https://github.com/chef-cookbooks/audit

Download it from one of those locations, **audit** cookbook is depend on other cookbooknamed as **compat\_resource**. So download this cookbook also and then upload it to the Chef server using the same workflow as any other cookbook.

**7) Use the audit Cookbook**

There are two ways to use the audit cookbook:

* Use the custom resources in the audit cookbook directly in recipes.
* Add the audit::default recipe to the run-list.

The default recipe requires a **node['audit']['profiles']** attribute to be set. For example, defined as part of a JSON-based role or environment file.below are the following steps to create role:

**Step 1**.Create a chef role using the command :

**$ knife role create myrole**

Here, myrole is the name of role

**Step 2**. Edit myrole :

{

"audit": {

"collector": "chef-compliance",

"server": "https://itsusmplsd03870.jnj.com/api",

"owner": "admin",

"refresh\_token": "24/5QWH1YexPkEcVklk-YofwD4EmrW4Q3aNoBoCBuJOBpzRn\_o4EWtUy4T9ldm0R2djo2eWVOZLzpv5oV3ZMmB5rw==",

"insecure": true,

"profiles": [

{

"name": "avecto",

"compliance": "admin/avecto\_test"

},

{

"name": "nbu",

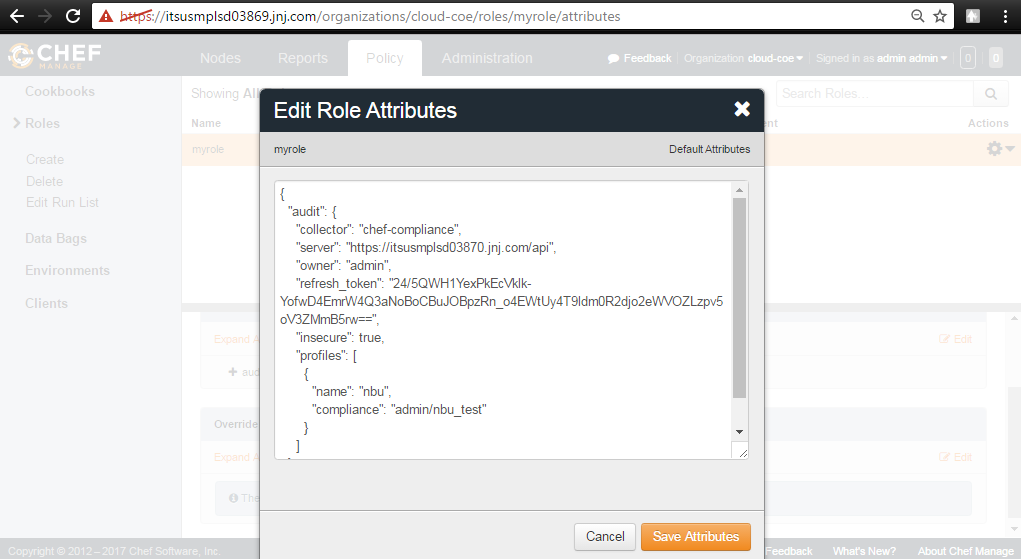
"compliance": "admin/nbu\_test"

}

]

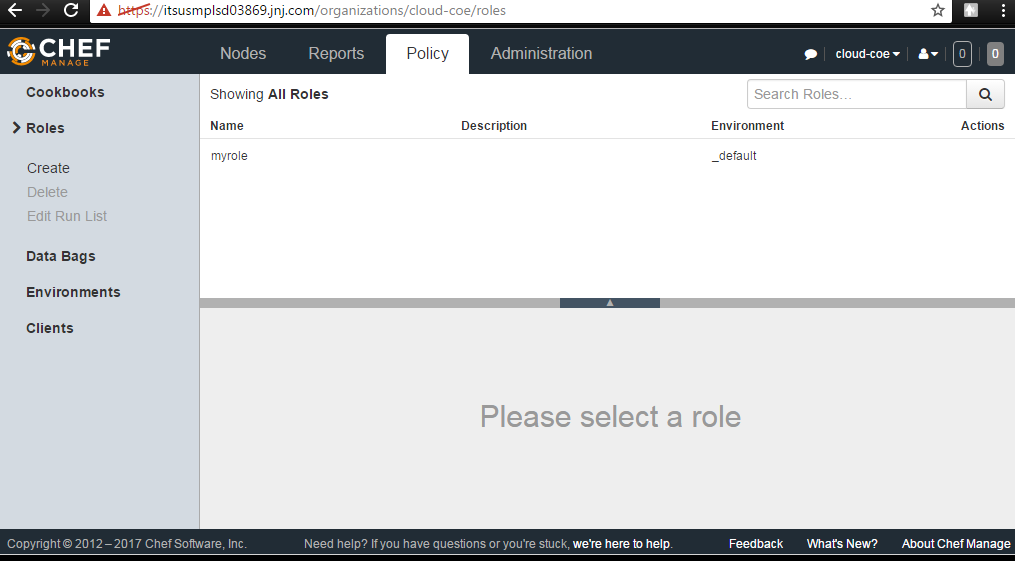
}

}

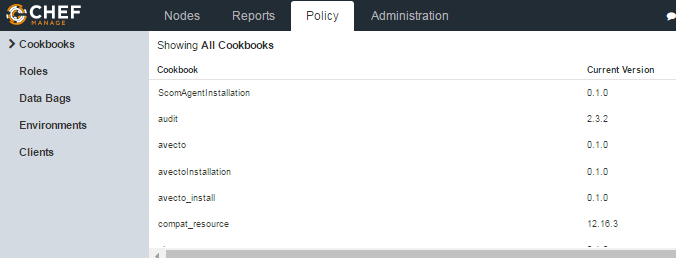


**Step 3**. upload role to server using the following command:

**$ knife upload roles**

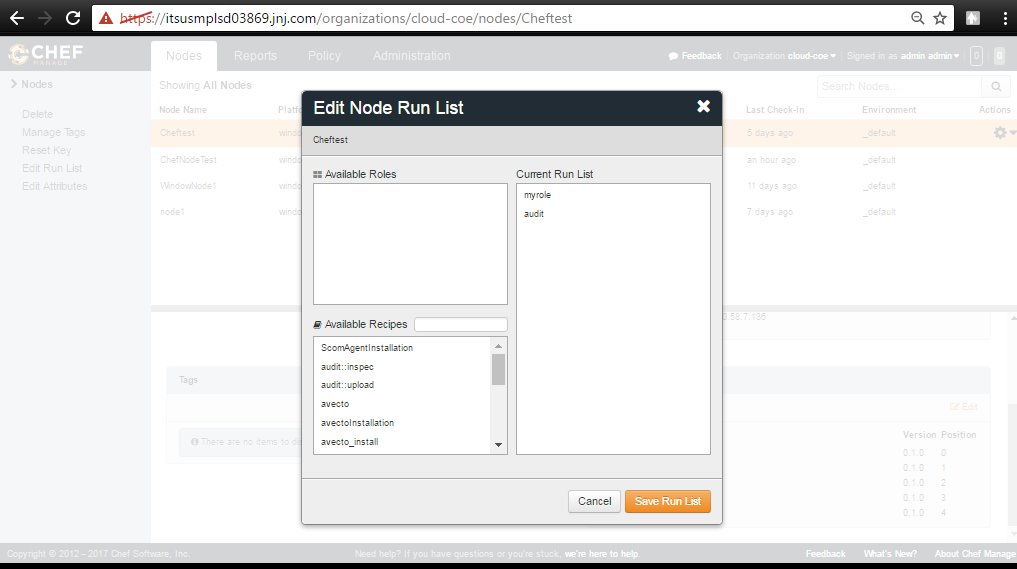
****

**Step 4.**upload the **audit** cookbook from chef-workstation to chef-server.

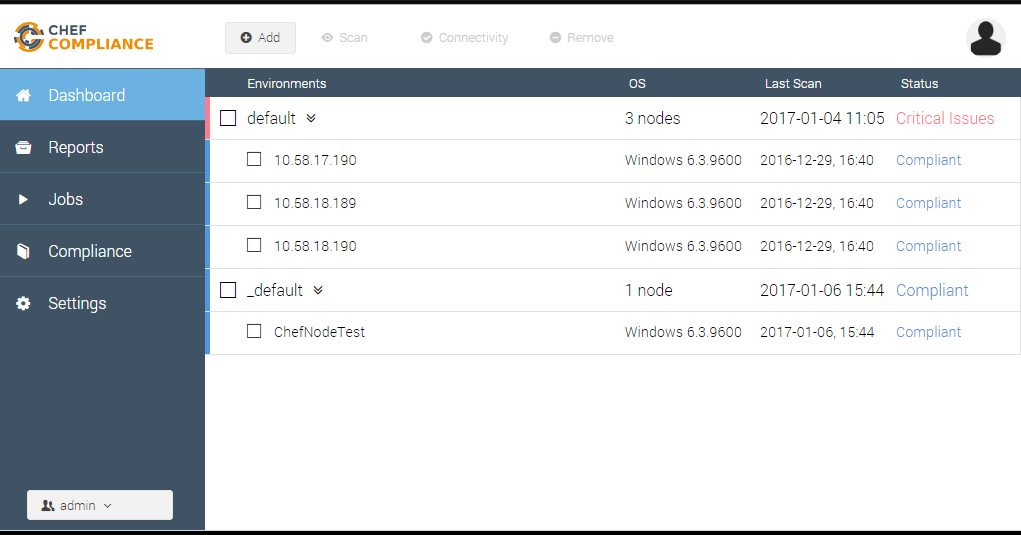


**Step 5**. goto chef server and edit the run-list of the role. Add the cookbooks you want to execute on the node. (eg: avecto, nbu etc.)

**Step 6**. edit the run\_list of the node and add the role (myrole) and audit cookbook to it.



**Step 7**. run chef-client on the node.



The **chef-client** run will do the following:

* Download the targeted profiles from Chef Compliance, and then run them locally on the node via InSpec.
* Log a summary of the audit execution.
* Submit the full report back to the Chef Compliance server. These reports are saved in a Chef Compliance Organization that has the same name as the Organization to which the node belongs on the Chef server.