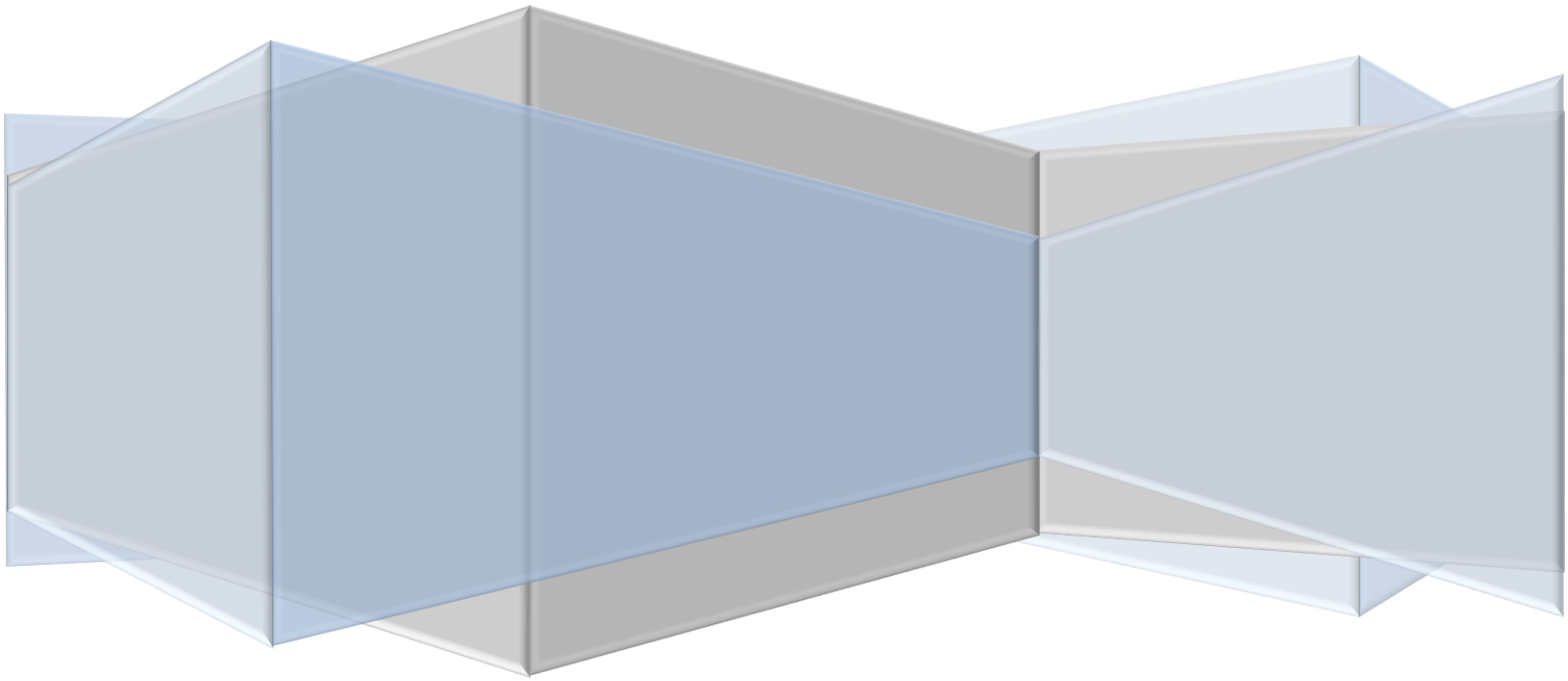
Automation Factory

Using Chef Data bags

Chef Security

Ganesh Palnitkar



Using Chef Data Bags

A data bag is used for storing sensitive information in **JSON** format.

This is a **global variable** that can be accessed within a recipe or accessed during a search outside a cookbook.

Typically a data bag can contain any sort of information that one find it to be kept away from general public access, e.g. password, certificate, private key, user specific information etc.

To **test** the functionality, first create a cookbook for creating users.

The recipe would have code to create a user. This will also have to pass the password in secured format.

```
user 'ganeshhp' do
  comment 'developer user'
  uid 1000
  home '/home/ganeshhp'
  shell '/bin/bash'
  password '$1$ganeshhp$pSqym47BHC33Dypg/UNQ/1'
end
```

Here the highlighted text indicates the hashed password generated using 'openssl' utility.

```
$ openssl passwd -1 –salt yoursalt

Password:
```

…. Here the password entered is not echoed. This will provide a hashed password string as written below. This password string then can be copied to the recipe file.

```
$1$yoursalt$Nh.AtxcC/6PsRIdSAc4zN.
```

---------- Some help on generating a password Hash ----------

How To Generate a /etc/passwd password hash via the Command Line on Linux

$ openssl passwd -1
Password:
Verifying - Password:
$1$3JUKmV3R$vZVeb51f1t6QZUecwuRHX0

If you want to pass along a salt to your password;

$ openssl passwd -1 -salt yoursalt
Password:
1yoursalt$5WA5NN0quMJ62v5LCu8kj1

The above examples all prompt your password, so it won't be visible in the history of the server or in the process listing. If you want to directly pass the password as a parameter, use one of these examples.

$ openssl passwd -1
Password:
Verifying - Password:
1rr7ygbpo$v.zYy4J3/B73NF/qsrDZJ0

To avoid writing the password in plain text or hashed format directly into the recipe file we make use of the data bags where the password is written and then referred as a variable in the recipe. As explained below.

A data bag is a variable stored in JSON format. The data inside the data bag can be accessed with in a recipe or from outside the cookbook.

A data bag is created using the command,

```
$ knife data bag create <data bag_name>
```

Once a data bag is created the data can be entered from a file or using command line. Entering data using a file is done using below command. Before that a file with '.JSON' extension is created to hold the secret data that we want to pass to the recipe or keep secured.

```
{
        "id": "ganeshhp",
        "password": "$1$yoursalt$Nh.AtxcC/6PsRIdSAc4zN.",
        "department": "development",
        "role": "associate"
}
```

`$ knife data bag from file <data bag_name> <file name>` …. This will create / update a data bag on the chef server using the .JSON file with info mentioned in it.

We can use the $ knife data bag list command to list down all data bags.

```
$ knife data bag list
```

We can also use the command to show data bag items using below command,

```
$ knife data bag show <data bag_name>
```

We can also use command to show details about the info inside the data bag items as well. This can be done using below command.

```
$ knife data bag show <data bag_name> <data bag_item>
```

```
WARNING: Unencrypted data bag detected, ignoring any provided secret options.
department: development
id:       ganeshhp
password:   $1$ganeshhp$pSqym47BHC33Dypg/UNQ/1
role:      associate
```

In the recipe file the data bag variable then can be called in below syntax.

```
userinfo = data_bag_item('user_info','ganeshhp')

user 'ganeshhp' do
   comment 'developer user'
   uid 2010
   home '/home/ganeshhp'
   shell '/bin/bash'
   password userinfo['password']
end
```

The above recipe is used for creating a user on the targeted server. For referring the data bag variable first define a variable as stated above.

- In this the ‘userinfo’ is the variable.
- A data bag item is called as ‘data_bag_item’
- Declare the data bag name from which the data bag item is to be called as ‘user_into’
- Specify the data bag item as ‘ganeshhp’