



# OPEN SOURCE SYSTEMS FOR SECRETS STORAGE



SuperGIRL: Irina Hristova



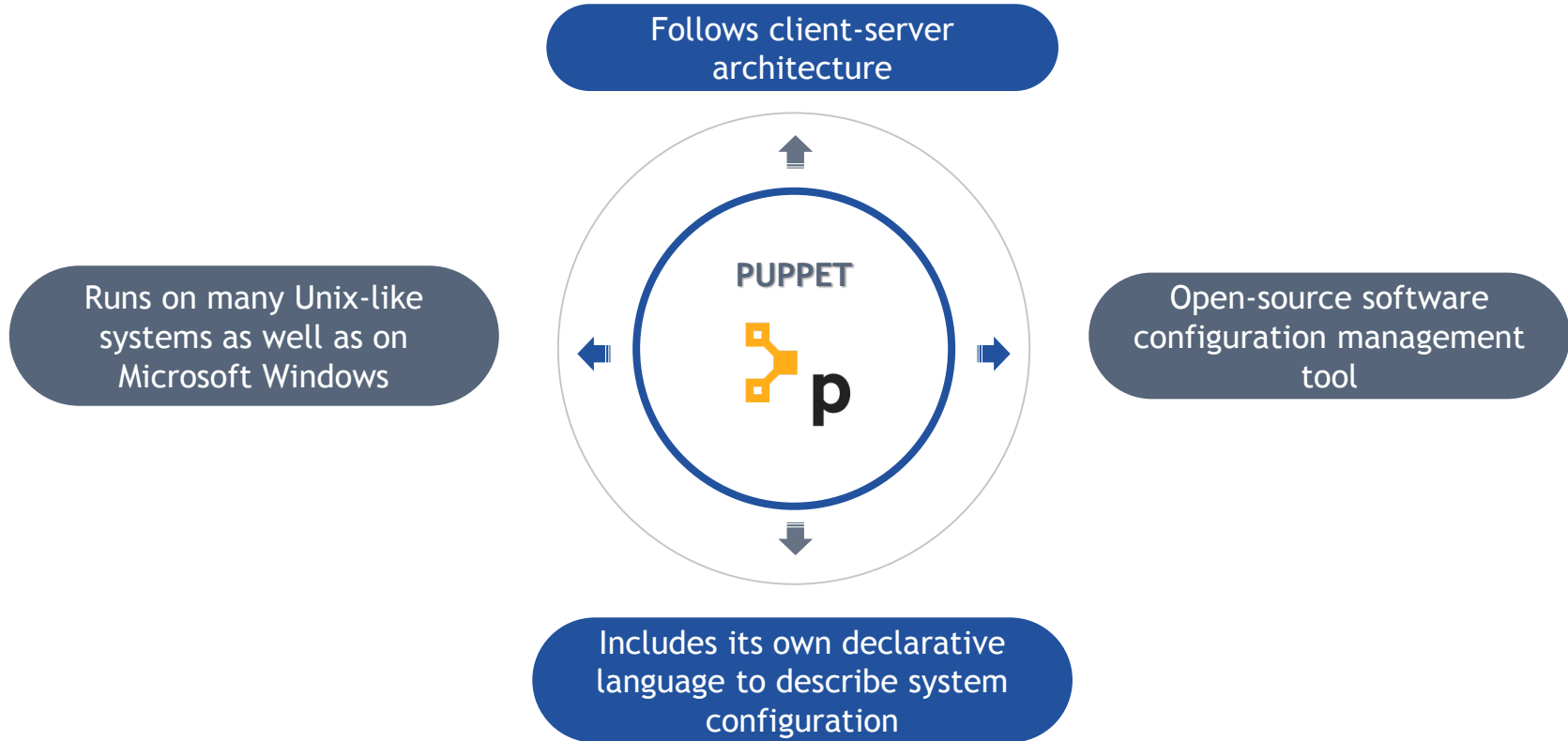
SuperBOY: Dimitar Oparlakov



SuperCAPTAIN: Zhechka Toteva

# CERN COMPUTING CENTER MANAGEMENT SYSTEM

---



# POTENTIAL REPLACEMENTS OF THE SECRETS STORAGE TOOLS

*SUMMARY OF OUR WORK*



# VAULT

*THE BEST DECISION SO FAR*





SECURES

STORES

TIGHTLY CONTROLS ACCESS

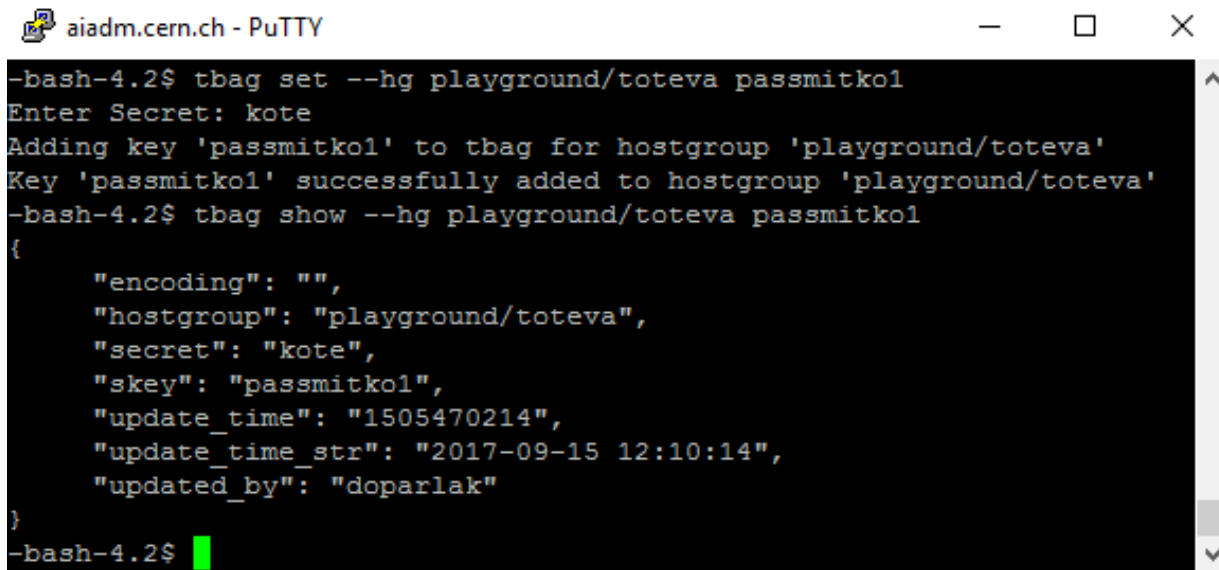
TOKENS

PASSWORDS

CERTIFICATES

API KEYS

OTHER SECRETS IN  
MODERN COMPUTING



```
aiadm.cern.ch - PuTTY
-bash-4.2$ tbag set --hg playground/toteva passmitkol
Enter Secret: kote
Adding key 'passmitkol' to tbag for hostgroup 'playground/toteva'
Key 'passmitkol' successfully added to hostgroup 'playground/toteva'
-bash-4.2$ tbag show --hg playground/toteva passmitkol
{
  "encoding": "",
  "hostgroup": "playground/toteva",
  "secret": "kote",
  "skey": "passmitkol",
  "update_time": "1505470214",
  "update_time_str": "2017-09-15 12:10:14",
  "updated_by": "doparlak"
}
-bash-4.2$
```

# THE PROCESS

## STEP 2

LEARNT BASIC COMMANDS, CREATED PASSWORD IN *tbag* AND INSTALLED THEM

```
root@zaio-baio:~  
[root@zaio-baio ~]# cat /tmp/testpass  
#passForMitko=""  
passForMitko = kotka  
passFromZhechka = thisisverysecret  
passFromPlayground = foo  
[root@zaio-baio ~]# puppet agent -tv  
Info: Using configured environment 'playground_oparlak'  
Info: Retrieving pluginfacts  
Info: Retrieving plugin  
Info: Loading facts  
Info: Caching catalog for zaio-baio.cern.ch  
Info: Applying configuration version '1505470395'  
Notice: Hello Ika  
Notice: /Stage[main]/Hg_playground::Toteva/Notify[Hello Ika]/message: def  
Notice: Applied catalog in 8.42 seconds  
[root@zaio-baio ~]# cat /tmp/testpass  
#passForMitko=""  
passForMitko = kote  
passFromZhechka = thisisverysecret  
passFromPlayground = foo  
[root@zaio-baio ~]#
```

# THE PROCESS

---

STEP 3

**STARTED *VAULT* IN DEVELOPMENT MODE**

STEP 4

**DECLARED SECRETS IN DEVELOPMENT MODE**

STEP 5

**STUDDIED DIFFERENT BACKENDS**

STEP 6

**INSTALLED CONSUL BACKEND**

STEP 7

**STARTED *VAULT* IN PRODUCTION MODE**

STEP 8

**TRIED DIFFERENT USER AUTHENTICATIONS**



```
root@ika ~]# curl -X GET -H "X-Vault-Token:c1b2695d-8fba-9e04-4d4e-e732f5bd4abe" http://127.0.0.1:8200/v1/secret/ika.cern.ch | json_reformat
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left   Speed
100    220    100    220     0     0    243k    0  --:--:-- --:--:-- --:--:--   214k
{
  "request_id": "f610a9f9-8aa9-a5f0-3e8f-267dc6690088",
  "lease_id": "",
  "renewable": false,
  "lease_duration": 2764800,
  "data": {
    "passkeyVault1": "passFirst",
    "zcheckaplay": "passSecond"
  },
  "wrap_info": null,
  "warnings": null,
  "auth": null
}
root@ika ~]# curl -X PUT -H "X-Vault-Token:c1b2695d-8fba-9e04-4d4e-e732f5bd4abe" -d '{"passkeyVault1": "passFirst", "zcheckaplay": "passSecondPrim"}' http://127.0.0.1:8200/v1/secret/ika.cern.ch
root@ika ~]# curl -X GET -H "X-Vault-Token:c1b2695d-8fba-9e04-4d4e-e732f5bd4abe" http://127.0.0.1:8200/v1/secret/ika.cern.ch | json_reformat
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left   Speed
100    224    100    224     0     0    251k    0  --:--:-- --:--:-- --:--:--   218k
{
  "request_id": "1c981e38-d36c-eb3e-3edd-005a9789e5d4",
  "lease_id": "",
  "renewable": false,
  "lease_duration": 2764800,
  "data": {
    "passkeyVault1": "passFirst",
    "zcheckaplay": "passSecondPrim"
  },
  "wrap_info": null,
  "warnings": null,
  "auth": null
}
```

# THE PROCESS

## STEP 10

## REPLACED RIAK WITH VAULT ON LOCAL NODE

ai / it-puppet-module-teigi - [This project] Search

Project: Repository Issues Merge Requests Pipelines Settings

Files Commits Branches Tags Contributors Graph Compare Charts

from qa to br:ika Compare Create merge request

Commits (3)

- Added file  
Inna Valentinova Hristova committed a day ago ae88342 Browse Files
- Change sub\_file to use vault  
Inna Valentinova Hristova committed 18 minutes ago cd82b7ea
- Remove debug logging  
Dimitar Vasenov Oparjakov committed 7 minutes ago cbe7c1a1

Showing 2 changed files with 11 additions and 11 deletions

Hide whitespace changes Inline Side-by-side

```
code/lib/puppet/provider/teigisecret/ruby.rb
...
75: 75: 76: 76: @@ Puppet::Type.type(:teigisecret).provider(:ruby) do
77: 77: 77: 77:   if url_args.empty?
78: 78: 78: 78:     uri = URI("#{resource[:url].to_s}/#{resource[:fpath]}/#{resource[:key]}")
79: 79: 79: 79:   else
80: 80: 80: 80:     uri = URI("#{resource[:url].to_s}/#{resource[:fpath]}/#{resource[:key]}#{url_args}")
81: 81: 81: 81:   end
82: 82: 82: 82:   return uri
83: 83: 83: 83: end
84: 84: 84: 84:
85: 85: 85: 85: @@ Puppet::Type.type(:teigisecret).provider(:ruby) do
86: 86: 86: 86:   if defined? @teigisecret_cache and @teigisecret_cache.has_key?(resource[:key])
87: 87: 87: 87:     return @teigisecret_cache[resource[:key]]
88: 88: 88: 88:   end
89: 89: 89: 89:
90: 90: 90: 90:   uri = self.make_uri()
91: 91: 91: 91:   req = Net::HTTP.new(uri.host, uri.port)
92: 92: 92: 92:   res = Net::HTTP.get(uri.host, uri.path)
93: 93: 93: 93:
94: 94: 94: 94:   res = Net::HTTP.get(uri.host, uri.path)
95: 95: 95: 95:
96: 96: 96: 96:   res = conn.start { |conn| conn.request(req) }
97: 97: 97: 97:   false
98: 98: 98: 98:   fail "teigi:modified, 'teigisecret'[:resource[:key]] not modified" if res.code == "304"
99: 99: 99: 99:   "Returned #{res.code}" unless res.code == "200"
100: 100: 100: 100:
101: 101: 101: 101:   payload = JSON.parse(res.body)
102: 102: 102: 102:   fail "Bad data getting 'teigisecret'[:resource[:key]]" +
103: 103: 103: 103:     " from uri[#{uri.to_s}]" unless payload.has_key?("secret")
104: 104: 104: 104:   if payload.has_key?("encoding") and payload["encoding"] == "base64"
105: 105: 105: 105:     payload["secret"] = Base64.decode4(payload["secret"])
106: 106: 106: 106:   end
107: 107: 107: 107:   if !is_create
108: 108: 108: 108:     if payload.has_key?("scope") and payload.has_key?("entity")
109: 109: 109: 109:       self.write_meta(payload["update_time"], payload["scope"], payload["entity"])
110: 110: 110: 110:     end
111: 111: 111: 111:     if payload.has_key?("data")
112: 112: 112: 112:       mydata = payload["data"]
113: 113: 113: 113:       if mydata.has_key?(resource[:key])
114: 114: 114: 114:         payload["secret"] = mydata[resource[:key]] + Base64.decode4(payload["secret"])
115: 115: 115: 115:       end
116: 116: 116: 116:     end
117: 117: 117: 117:   end
118: 118: 118: 118:   unless defined? @teigisecret_cache
119: 119: 119: 119:   end
120: 120: 120: 120: end
...

code/manifest/secret/sub_file.pp
...
77: 77: 77: 77: @@ define teigisecret::sub_file {
78: 78: 78: 78:   source => $mysource,
79: 79: 79: 79: }
80: 80: 80: 80:
81: 81: 81: 81: ensure_resource('teigisecret', $teigi_keys, {'path' => $teigi::thg::path, 'url' => $teigi::thg::url, 'urlargs' => $teigi::thg::urlargs,
82: 82: 82: 82:   'secretpath' => $teigi::thg::secretpath, 'require' => "file[${teigi::thg::path}]}")
83: 83: 83: 83: ensure_resource('teigisecret', $teigi_keys, {'path' => $teigi::thg::path, 'url' => $teigi::thg::url, 'urlargs' => $teigi::thg::urlargs,
84: 84: 84: 84:   'secretpath' => $teigi::thg::secretpath, 'require' => "file[${teigi::thg::path}]}")
85: 85: 85: 85:
86: 86: 86: 86: file[$path]
87: 87: 87: 87: ensure => present,
88: 88: 88: 88: }
```

10

```
[root@ika ~]# puppet agent -tv
Info: Using configured environment 'playground_ika'
Info: Retrieving pluginfacts
Info: Retrieving plugin
Info: Loading facts
Info: Caching catalog for ika.cern.ch
Info: Applying configuration version '1505469422'
Notice: Hello mitkooooooooo
Notice: /Stage[main]/Hg_playground::Toteva/Notify[Hello mitkooooooooo]/message: defined 'message' as 'Hello mitkooooooooo'
Notice: /Stage[main]/Hg_playground::Toteva/Teigi::Secret::Sub_file[/tmp/testpass]/Teigisecret[zhechkaplay]/ensure: created
Notice: /Stage[main]/Hg_playground::Toteva/Teigi::Secret::Sub_file[/tmp/testpass]/Teigi_sub_file[/tmp/testpass]/ensure: created
Notice: Applied catalog in 9.03 seconds
[root@ika ~]# cat /tmp/testpass
passFIka=passFirst
passFromZhechka=passSecondPrim
```



# FUTURE PLANS

ORGANISED SECRETS IN AN HIERARCHICAL ORDER



**Thanks for Watching**