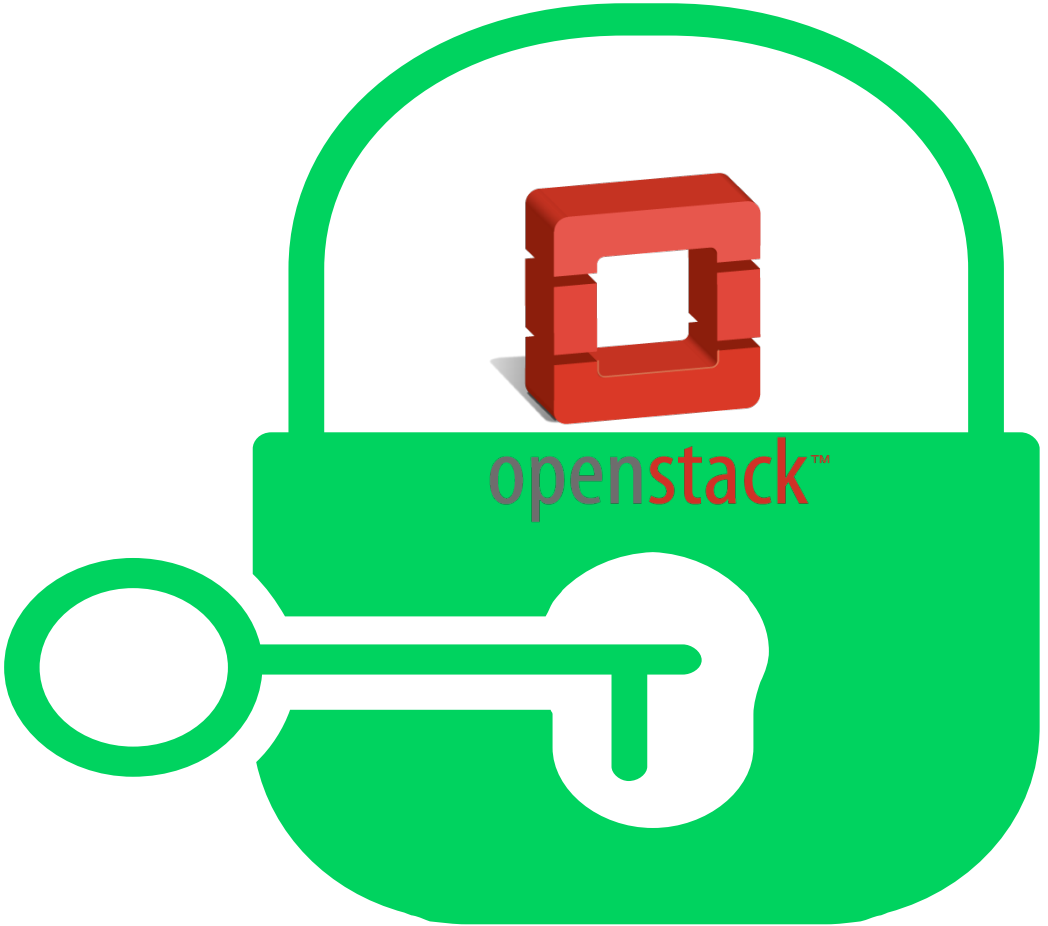
Integrating Identity with LDAP(AD/eDir) for OpenStack

SUSECON Session TUT90531

Rodolfo Bejarano
Sales Engineer
rbejarano@suse.com

Craig Liddle
Sales Engineer
Craig.liddle@suse.com

How do you enforce security on OpenStack?

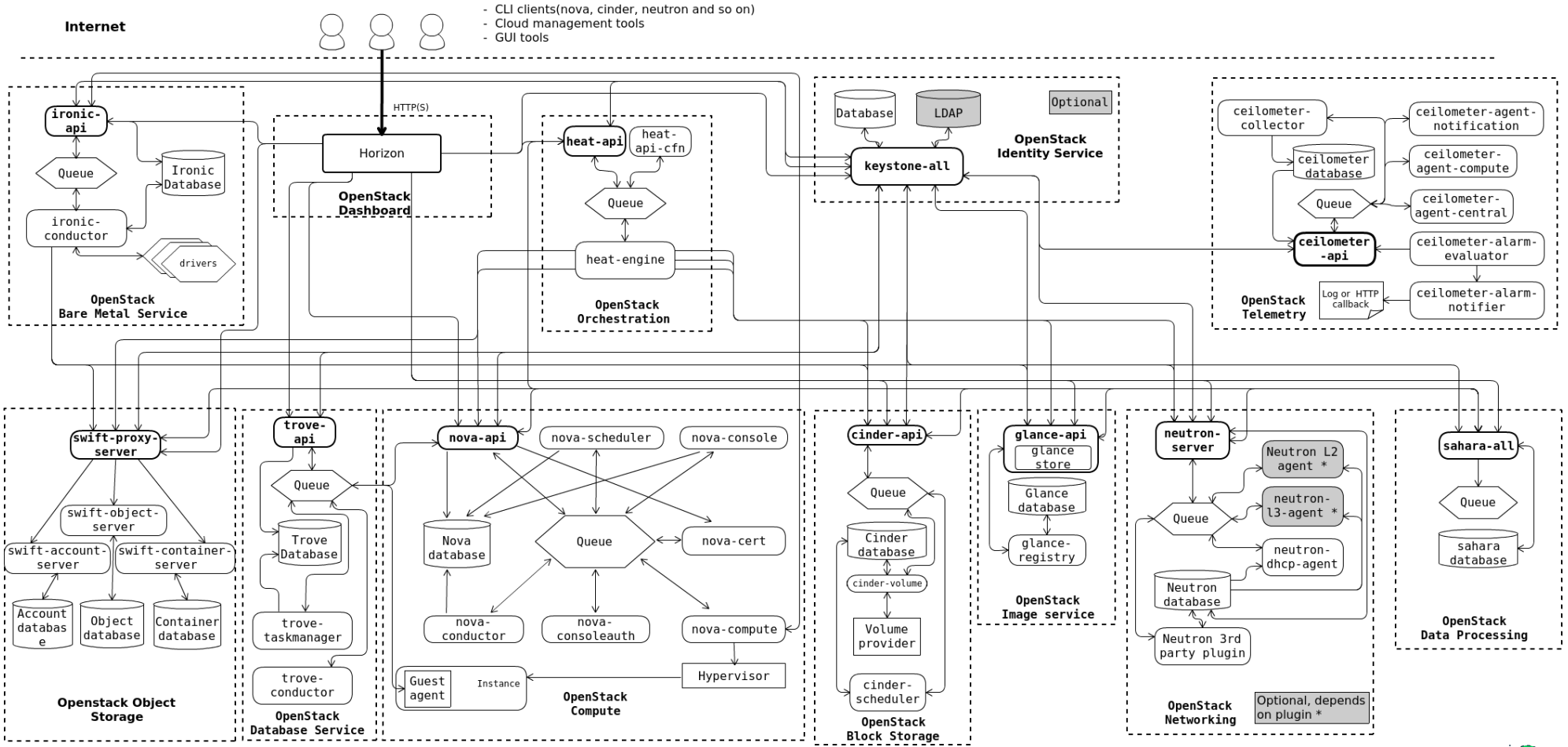


What is Keystone?

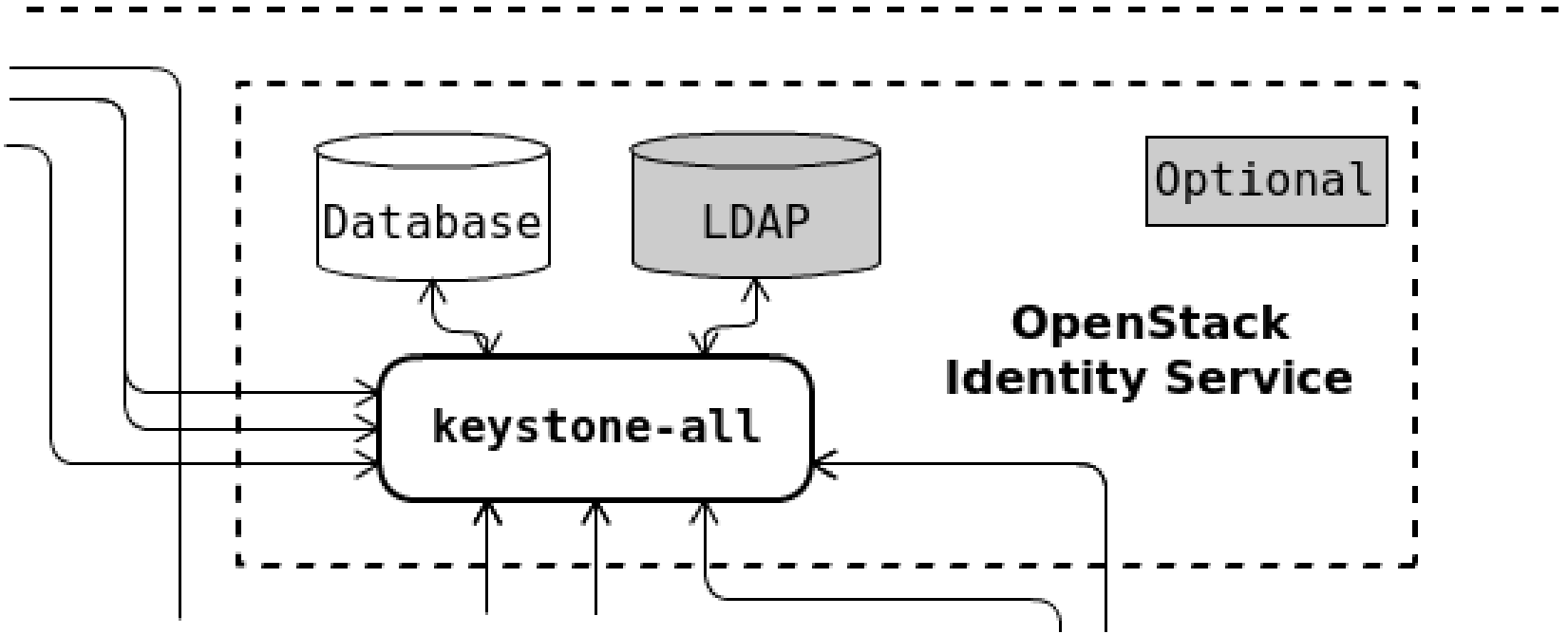
- Keystone is a core component that is used by all other OpenStack services. It provides authentication and authorization services. Keystone needs to be installed on a Control Node. Keystone can be made highly available by deploying it on a cluster.

- By default Keystone uses an SQL database back-end store for authentication. LDAP can be used in addition to the default or as an alternative. Using LDAP requires the Control Node on which Keystone is installed to be able to contact the LDAP server.

Keystone Workflow



Keystone Workflow



Configuring Keystone for LDAP identity

1. In the [identity] section of keystone.conf, replace
driver=keystone.identity.backends.sql.Identity
with driver = keystone.identity.backends.ldap.Identity.

2.Change LDAP settings in the keystone.conf file

[ldap]
url = ldap://localhost
user = dc=Manager,dc=openstack,dc=org
password = yourpassword
suffix = dc=openstack,dc=org
user_tree_dn = ou=Users,dc=openstack,dc=org
user_objectclass = inetOrgPerson
user_id_attribute = cn
…

But….There is also a hybrid configuration

The Hybrid LDAP back-end allows to create a mixed LDAP/SQL setup. This is especially useful when an existing LDAP server should be used to authenticate cloud users. The system and service users (administrators and operators) needed to set up and manage SUSE Cloud will be managed in the local SQL database. Assignments of users to projects and roles will also be stored in the local database.
How to set the identity and assignment drivers to the hybrid back-end:

```
 "identity": {
    "driver": "keystone.identity.backends.hybrid.Identity"
  },
  "assignment": {
    "driver": "keystone.assignment.backends.hybrid.Assignment"
  }
```

In conclusion..

Keystone provides identity services for all OpenStack projects. In addition to the default SQL back end, Keystone supports LDAP and pluggable authentication modules. During this session we showed how to enable LDAP as a Keystone back end by either installing a new LDAP server or configuring Keystone to use an existing one. Finally you have the option to have a hybrid configuration will allows you to seamlessly integrate your authentication without the need of any schema modifications to Suse OpenStack Cloud.

Reference Material

https://www.suse.com/documentation/suse-cloud-5/book_cloud_deploy/data/sec_depl_ostack_keystone.html

https://ask.openstack.org/en/question/8404/how-do-i-combine-active-directory-and-sql-authentication-for-keystone/

https://wiki.openstack.org/wiki/HowtoIntegrateKeystonewithAD

https://wiki.openstack.org/wiki/Keystone

http://docs.openstack.org/developer/keystone/

Ready to see it in action!!

Questions


SUSE®
We adapt. You succeed.