



UPPSALA
UNIVERSITET



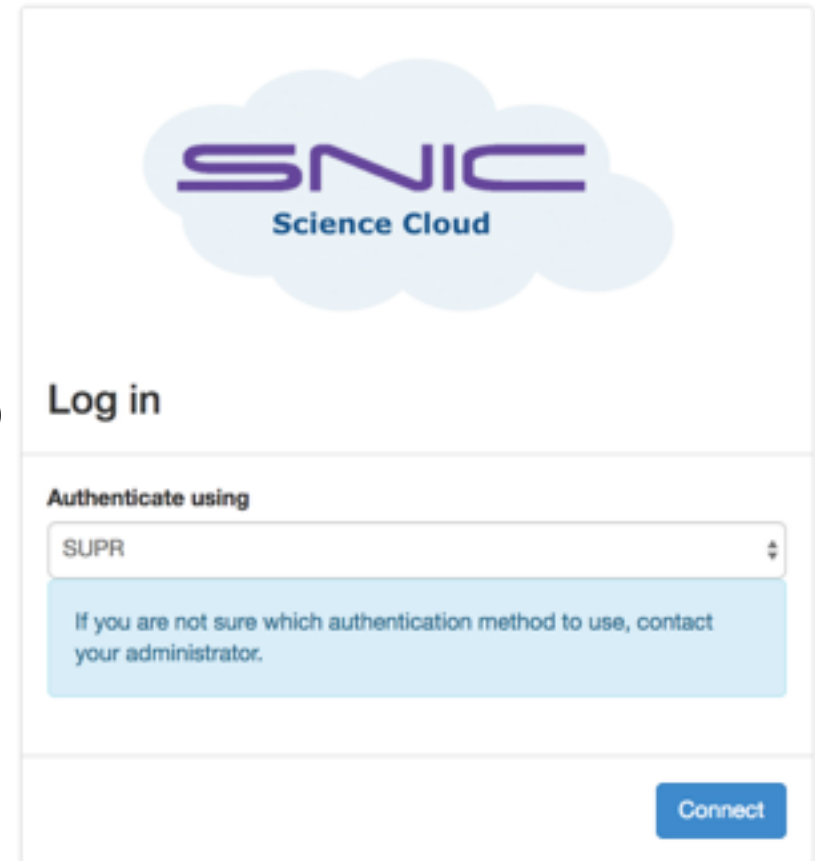
GROOT: Infrastructure_Security- as-a-Service (ISaaS)

Salman Toor

salman.toor@it.uu.se

SNIC Science Cloud (SSC)

- New Production grade setup
- Two regions are operational
 - HPC2N (Umeå)
 - C3SE (Göteborg)
 - UPPMAX (Uppsala, Soon will be operational)
- Resources
 - VCPU ,352
 - RAM 1TB
 - Storage
- OpenStack + Ceph + SAML Identity + OpenStack Ansible

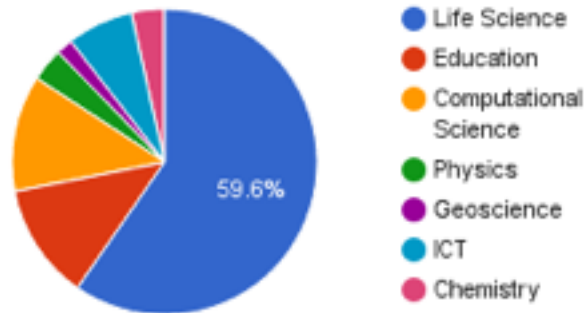


The image shows the login interface for SNIC Science Cloud. At the top, there is a logo consisting of a light blue cloud shape with the text "SNIC" in purple and "Science Cloud" in blue below it. Below the logo, the text "Log in" is displayed. Underneath, there is a section titled "Authenticate using" with a dropdown menu currently showing "SUPR". Below the dropdown, a light blue box contains the text: "If you are not sure which authentication method to use, contact your administrator." At the bottom right of the interface, there is a blue button labeled "Connect".

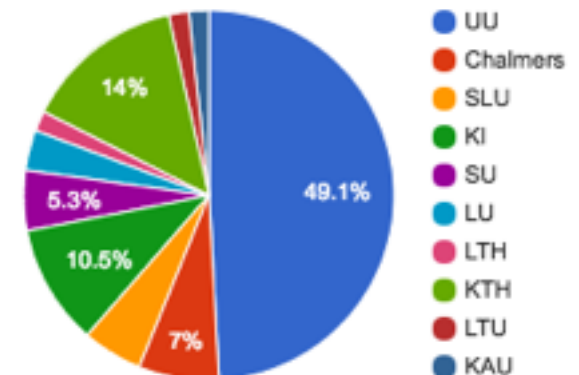
SSC previous setup

- 57 registered projects during 2015-2016
- Average 5 to 7 instances per project
- Users had complete control over allocated resources

SSC projects per area



SSC projects per institution





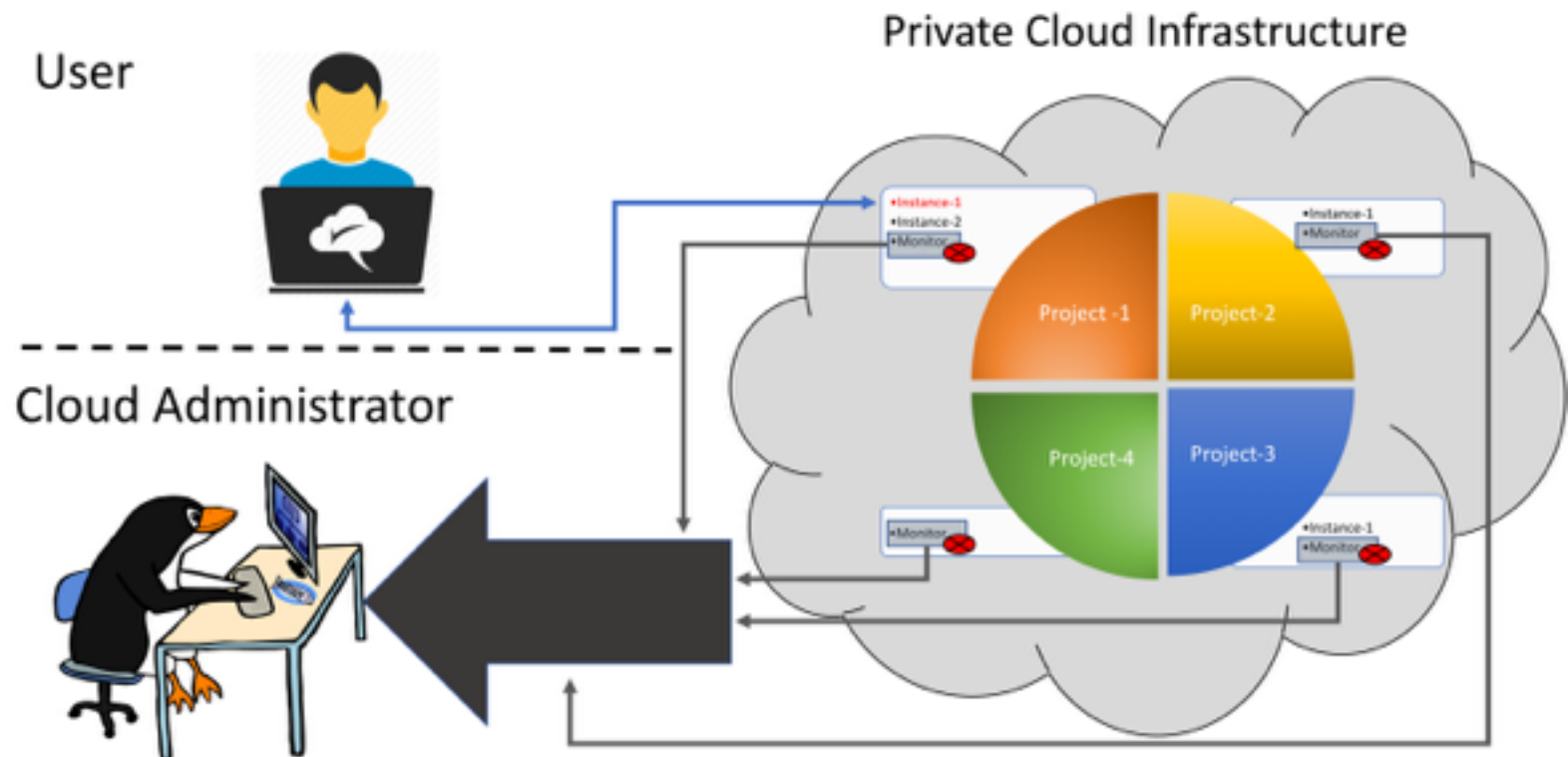
UPPSALA
UNIVERSITET

Utmost challenges

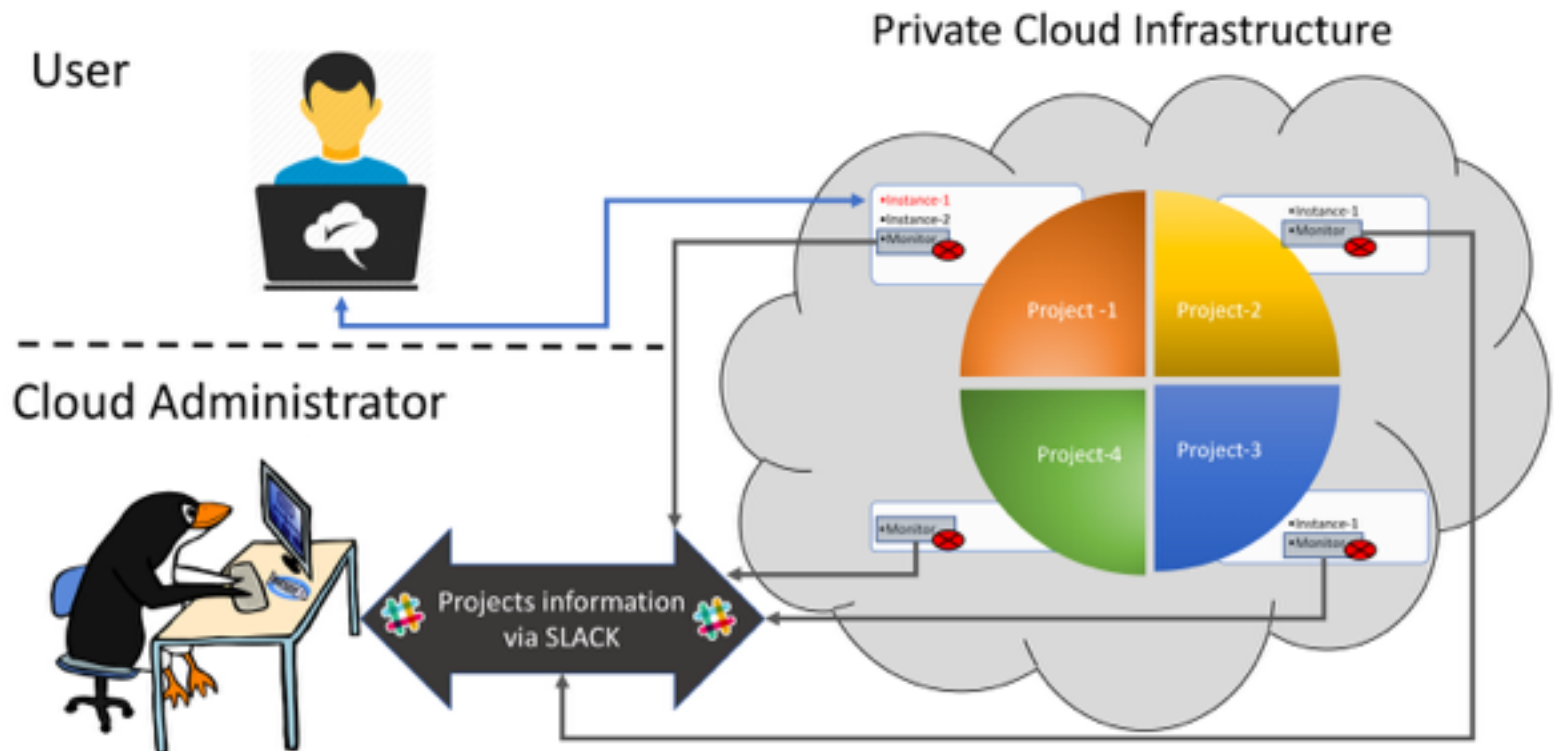
- Stable deployment of OpenStack setup
- Working model based on different regions
- System monitoring
- Projects and users management
- Overall system security

Infrastructure_Security-as-a-Service(ISaaS)

- Masters Thesis Project
- Student: Aleksander Okonski




Infrastructure_Security-as-a-Service(ISaaS)



Infrastructure_Security-as-a-Service(ISaaS)


- Two phases
 - Phase-1: Inform cloud administrator regarding abnormal activities using Slack (almost completed)
 - Slack API uses OAuth 2.0
 - communicate via BOT-user
 - One Slack BOT per project
 - Each project has its own channel
 - Ansible based deployment of monitoring instance
 - Phase-2: A forensic tool for compromised instances (Work in progress)

Infrastructure_Security-as-a-Service(ISaaS)


SecGroup ▾ 

😊 New! Set your status

🔍 All Threads

CHANNELS (5) 

- # general
- # random
- # c2015003


DIRECT MESSAGES 


- ♥ slackbot
- 👤 salmantoor (you)
- 🗉 groot

+ Invite people

 **salmantoor** 2:38 PM
@isaas help

 **isaas** APP 2:38 PM
The following are excepted:"openstackinfo ("serverlist", routerlist", " networklist", "securitygroups")", "vmproblems ID", "vmdatabase ID ", "vmstatus key value" , "fullreport"

 **salmantoor** 1:15 PM
@isaas fullreport

 **isaas** APP 1:15 PM
Tenant name: SNIC 2017/13-8
Tenant ID: SNIC 2017/13-8

```
--Server With ID: 9041c535-8e2b-4f99-b2b1-1f99fae251f9
--Server With ID: 146b0502-b45b-4034-8645-919444035401
--Server With ID: 3546e222-a511-49db-a027-1f1995298065
Server ID: 3546e222-a511-49db-a027-1f1995298065 | 4567 has been found closed
and is not in the config
--Server With ID: d814d0ca-6f58-4a33-9033-a946e2f126ee
--Server With ID: a62a8841-1a20-4e15-ac15-eeffe17b5361
--Server With ID: 54d6fdf7-dea3-4b4a-ace3-fae557252abf
--Server With ID: 9d21538b-dd6a-4674-a304-408f73073b38
--Server With ID: b07c416c-0751-4c83-8715-7b7ce6b87fbb
Server ID: b07c416c-0751-4c83-8715-7b7ce6b87fbb | 4567 has been found closed and
is not in the config
--Server With ID: db52beaf-ab6c-4307-a82a-f65989cc0989
--Server With ID: ef72334f-d3a6-42fe-a689-2a50bfadefa7
--Server With ID: 05767451-90ca-4e36-bc58-ad9d688dbb10
--Server With ID: a448f3b8-306f-40d7-bbf7-19acfa9b35b
--Server With ID: ef0d48ce-6c36-44c1-884c-19983d7261e5
Server ID: ef0d48ce-6c36-44c1-884c-19983d7261e5 | OpenSSH on port 22 is version:
6.6.1p1 Ubuntu 2ubuntu2.8 -- Should be = 7.2p2 Ubuntu 4ubuntu2.1
```


Infrastructure_Security-as-a-Service(ISaaS)

Server ID: ef0d48ce-6c36-44c1-884c-19983d7261e5 | OpenSSH on port 22 is version: 6.6.1p1 Ubuntu 2ubuntu2.8 -- Should be = 7.2p2 Ubuntu 4ubuntu2.1

Server ID: 51ed7b1c-75cb-4175-8c81-304f6f7604e2 | 1175 has been found filtered and is not in the config

Server ID: f57b9369-4e15-4151-9b0b-7d405cbdb5e4 | ip_external_auth: publickey password keyboard-interactive -- Should be = publickey

Infrastructure_Security-as-a-Service(ISaaS)



groot 1:53 PM

@isaas database 1463c1b7-6f73-411a-85ab-46ae95e2c537



isaas APP 1:53 PM ☆

Tenant name: c2015003

Tenant ID: c2015003

```
[
  {
    "ID": "1463c1b7-6f73-411a-85ab-46ae95e2c537",
    "IP": {
      "ip_external": "130.238.29.103",
      "ip_external_auth": "publickey",
      "ip_internal": "192.168.1.184",
      "ip_internal_auth": "publickey"
    },
    "_id": {
      "$oid": "58c965e709cad70b5ba1a1bb"
    },
    "ports": {
      "22": "open",
      "443": "closed",
      "5000": "closed",
      "6000": "closed",
      "80": "closed"
    },
    "services": {
      "OpenSSH on port 22 is version": "7.2p2 Ubuntu 4ubuntu2.1"
    }
  }
]
```