Introduction

• Wigner Datacenter is part of Wigner Research Center for Physics (Wigner RCP), which belongs to the Hungarian Academy of Sciences (MTA)

• Tier-0 hosting site for CERN

• Academic Cloud for the scientific community:
  – 4000 VCPUs
  – 1.6 PB Storage
  – 1.6 PB Tape backup
Current Production State

- Legacy Cloud
- OpenStack Kilo
- Installed manually
- Instead of manual upgrade, we designed a new architecture with an automated cloud deployment
# New Architecture

<table>
<thead>
<tr>
<th>Identity Management</th>
<th>Orchestration, Service Catalog, Chargeback</th>
<th>Infrastructure as Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSO</td>
<td>Monitoring, Logging, Performance Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configuration &amp; Lifecycle Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Server Provisioning</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Storage &amp; Backup Services</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network Automation, Templates</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Freeipa Freeradius Keycloak</th>
<th>ManageIQ</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>OpsTools (Kibana, Grafana, Uchiwa, Sensu, Fluentd, Collectd)</td>
</tr>
<tr>
<td></td>
<td>Katello (Foreman Proxy, Puppet, Ansible, Pulp, Candlepin)</td>
</tr>
<tr>
<td>Openstack (Tripleo)</td>
<td>Baremetal (Cluster)</td>
</tr>
<tr>
<td>Ceph Storage / Tape Backup</td>
<td>oVirt (KVM)</td>
</tr>
<tr>
<td>Network, Firewall, IDS</td>
<td>GlusterFS</td>
</tr>
</tbody>
</table>
Toolset

- DevOPS using GitLab, Gerrit and Jenkin

- OVirt virtualized HA infrastructure
  - FreeIPA: Identity management, Kerberos, LDAP, DNS
  - Katello (+Puppet master): Configuration & life cycle management
  - Undercloud

- OpenStack deployment using TripleO

- OpsTools (integrated with TripleO)
  - Availability Monitoring: Sensu, Redis, Uchiwa
  - Log collection: Fluentd, Elasticsearch, Kibana
  - Performance monitoring: Collectd, Grafite, Grafana

- Network automation + IaC (Infrastructure as Code) with Puppet (plan)

- Infrastructure monitoring: Morpheus (plan)

- Management / user platform: ManageIQ (plan)
TripleO

- OpenStack on OpenStack
- Using a deployment cloud (Undercloud) to create and manage a workload cloud (Overcloud)
Automated way of adding servers to the Overcloud

- Katello Discovery
- IPMI Fix IP Setup
- instackenv.json
- JSON
- Baremetal node add
- Deploy & Use
- Introspect nodes
Instackenv

```json
{
    "nodes": [
        {
            "pm_password": 
            "mac": [
                "0c:c4:7a:54:42:50"
            ],
            "name": "bls4",
            "pm_type": "pxe_ipmitool",
            "pm_addr": "192.168.1.1",
            "arch": "x86_64",
            "pm_user":
            "capabilities": "node:ceph-0,profile:ceph-storage,boot_option:local"
        }
    ]
}
```
Available nodes

```
[stack@tripleo-vm ~]$ openstack baremetal node list

+----------+----------+----------------+--------------------------+--------------------------+--------------------------+--------------------------+
| UUID     | Name     | Instance UUID  | Power State | Provisioning State | Maintenance |             |
|----------+----------+----------------+--------------------------+--------------------------+--------------------------+--------------------------+
| 023ae823-bf9b-4b5d-b47b-29237e4b21fe | B2C3A | 89de5dc8-bd76-4629-bbb5-6dbfb32418ad | power on | active | False |
| 03d6c5f-6c5e-4870-9b86-a684c3dd0269 | B2C4A | 18e06411-6fdc-40b9-ba2b-1f09d8c895db | power on | active | False |
| 8ae8de3c-9213-441e-a74f-fdf1ce1f3e8 | B2C5A | c68c4b64-3dc4-4284-a705-276dd01b5778 | power on | active | False |
| 62c317ff-83ad-4ef8-bb61-4c0153bcdd8 | B2C3C | eea731d-bf67-42f2-9d59-a43702705ed8 | power on | active | False |
| c73b1b0f-86ca-4c65-89e3-d20f0ee2876 | B2C3D | 7db691e-9e05-4c6c-a270-0902207eed8a | power on | active | False |
| 0d7d23ca-2693-4660-9674-86c765648870 | B2C4C | 4d3d28ca5-9f1e-40cf-913a-93f63f21ac | power on | active | False |
| 3e926cc9-79f7-4fd4-944e-d9b4ba3d49e1 | B2C4D | None | power off | available | False |
| 7437ce1f-b1d1-4945-ba2b-59d9d3aa1f0b | B2C4C | None | power off | available | False |
| d832e1eb-7a0-450d-9b21-8e9f346750a | B2C5D | None | power off | available | False |
| dd9d2ed3-e1c-4229-9f7-6e8a9eb9621e | B2S1 | 8aab5608-2b76-491f-99db-065ba139113 | power off | active | False |
| a521d035-67c-4a51-8996-a660c1ff66c3 | B2S2 | cbd1ec69-5b74-49dd-a2df-446907b8566 | power off | active | False |
| 68dc76ee-462-4b65-8760-edd298052263 | B2S3 | 869efbaf-4c82-4fe2-9b1c-98f4b6a65c9 | power off | active | False |
```

```
[stack@tripleo-vm ~]$ openstack server list

+----------+----------+----------+--------------------------+
| ID       | Name     | Status   | Networks               |
|----------+----------+----------+--------------------------+
| c68c4b64-3dc4-4284-a705-276dd01b5778 | B2C5A-control | ACTIVE | cttplane=192.168. | overcloud-full |
| 8ae8de3c-9213-441e-a74f-fdf1ce1f3e8 | B2C3A | ACTIVE | cttplane=192.168. | overcloud-full |
| 4d3d28ca5-9f1e-40cf-913a-93f63f21ac | B2C4A | ACTIVE | cttplane=192.168. | overcloud-full |
| 62c317ff-83ad-4ef8-bb61-4c0153bcdd8 | B2C3C | ACTIVE | cttplane=192.168. | overcloud-full |
| c73b1b0f-86ca-4c65-89e3-d20f0ee2876 | B2C3D | ACTIVE | cttplane=192.168. | overcloud-full |
| 0d7d23ca-2693-4660-9674-86c765648870 | B2C4C | ACTIVE | cttplane=192.168. | overcloud-full |
| 3e926cc9-79f7-4fd4-944e-d9b4ba3d49e1 | B2C4D | ACTIVE | cttplane=192.168. | overcloud-full |
| 7437ce1f-b1d1-4945-ba2b-59d9d3aa1f0b | B2C4C | ACTIVE | cttplane=192.168. | overcloud-full |
| d832e1eb-7a0-450d-9b21-8e9f346750a | B2C5D | ACTIVE | cttplane=192.168. | overcloud-full |
| dd9d2ed3-e1c-4229-9f7-6e8a9eb9621e | B2S1 | ACTIVE | cttplane=192.168. | overcloud-full |
| a521d035-67c-4a51-8996-a660c1ff66c3 | B2S2 | ACTIVE | cttplane=192.168. | overcloud-full |
| 68dc76ee-462-4b65-8760-edd298052263 | B2S3 | ACTIVE | cttplane=192.168. | overcloud-full |
```
Yaml files describing the environment

- The Overcloud is deployed using heat
- describe the environment using yaml parameters

nodes.yaml: define compute & store count

```
parameter_defaults:
  NovaRbdPoolName: ephemeral-vms
  CinderRbdPoolName: cinder-volumes
  CinderBackupRbdPoolName: cinder-backups
  GlanceRbdPoolName: glance-images
  GnocchiRbdPoolName: metrics

  CephPools:
    ephemeral-vms:
      size: 2
      pg_num: 256
      ppg_num: 256
    cinder-volumes:
      size: 2
      pg_num: 1024
      ppg_num: 1024
    cinder-backups:
      size: 2
      pg_num: 512
      ppg_num: 512
    glance-images:
      size: 2
      pg_num: 256
      ppg_num: 256
    metrics:
      size: 2
      pg_num: 256
      ppg_num: 256

ExtraConfig:
  ceph::profile::params::osd_pool_default_pg_num: 32
  ceph::profile::params::osd_pool_default_ppg_num: 32
  ceph::profile::params::osd_pool_default_size: 3

  CephStorageExtraConfig:
  ceph::profile::params::osd_journal_size: 10240
  ceph::profile::params::osds:
    '/dev/sdf':
      journal: '/dev/sdc'
    '/dev/sdi':
      journal: '/dev/sdc'
```
New features and upgrade plan

• 3 step process
  – Development environment (small, 3 node)
  – Test environment (medium, 9 nodes)
  – Production environment
Firewall

• OpnSense is a FreeBSD based open source firewall
  – Integrated Suricata
  – Integrated OpenVPN
  – Integrated Time Server

• Problems:
  – Lacks API support for automation
  – Port configuration turns off all ports
  – Pfsense code could use a rework

• We are still looking for an alternative solution that can be better automated, any suggestions?
2FA / Yubikey

- Two factor authentication to increase security
- Supports NFC
- Integrated with FreeIPA – FreeRadius
- Used for secure VPN connection
Progress so far

• Fully virtualized infrastructure
  – OVirt on 3 hosts
  – Katello
  – FreeIPA

• Working Dev and Test environment with new features added and tested continuously

• FreeIPA Integration to Overcloud nodes & to keystone
  – Tried novajoin, it didn’t register IP addresses correctly
  – Wrote custom script instead

• Still a lot of work left to do.....
Problems we currently face

• Overcloud Metadata VIP not working
• Power outage in the test environment
  – UPS failure dedicated to our test system
  – FreeIPA database corruption -> reinstall
  – FreeIPA replicas
• Overcloud cert resubmit loop
• Frequent bugs in the TripleO stable repository
Thank you!
Questions?

If you have any ideas or suggestions we would be happy to hear it.
Email: szeleczky.zoltan@wigner.mta.hu
Extra / Backup Slides

2017. 10. 19.
Availability Monitoring
Performance Monitoring

User

carbon-relay

monitor node

graphite-web

influxdb

reads data from

apache

graphana

Locks at

controller node
collectd

controller node
collectd

compute node
collectd

storage node
collectd

compute node
collectd

storage node
collectd

compute node
collectd
Logging
OVirt

OVirt is an open source virtual datacenter platform, built on the foundation of the Linux KVM hypervisor. It’s the open-source equivalent of RHEV. It provides high availability and an easy way to solve the chicken-egg problem.

We use it to virtualize our infrastructure services such as:

- Katello: Lifecycle management
- FreeIPA: SSO; Security information management solution
- TripleO undercloud
Katello / Foreman

Manage servers throughout their lifecycle, from provisioning and configuration to orchestration and monitoring. It’s the open-source equivalent of RH Satellite.

- Discover new servers, inventory
- Manage physical and virtual servers
- Supports Puppet and Ansible
- Local yum repo
- Openscap security audits

Starting point for developing automated processes, and also has GUI for convenience.
FreeIPA

- SSO for users, systems, services
- LDAP / Kerberos authentication
- Has replication functions to ensure HA
- We use it to manage our users, hosts and services securely with certificates