誉天教育
YU TIAN EDU

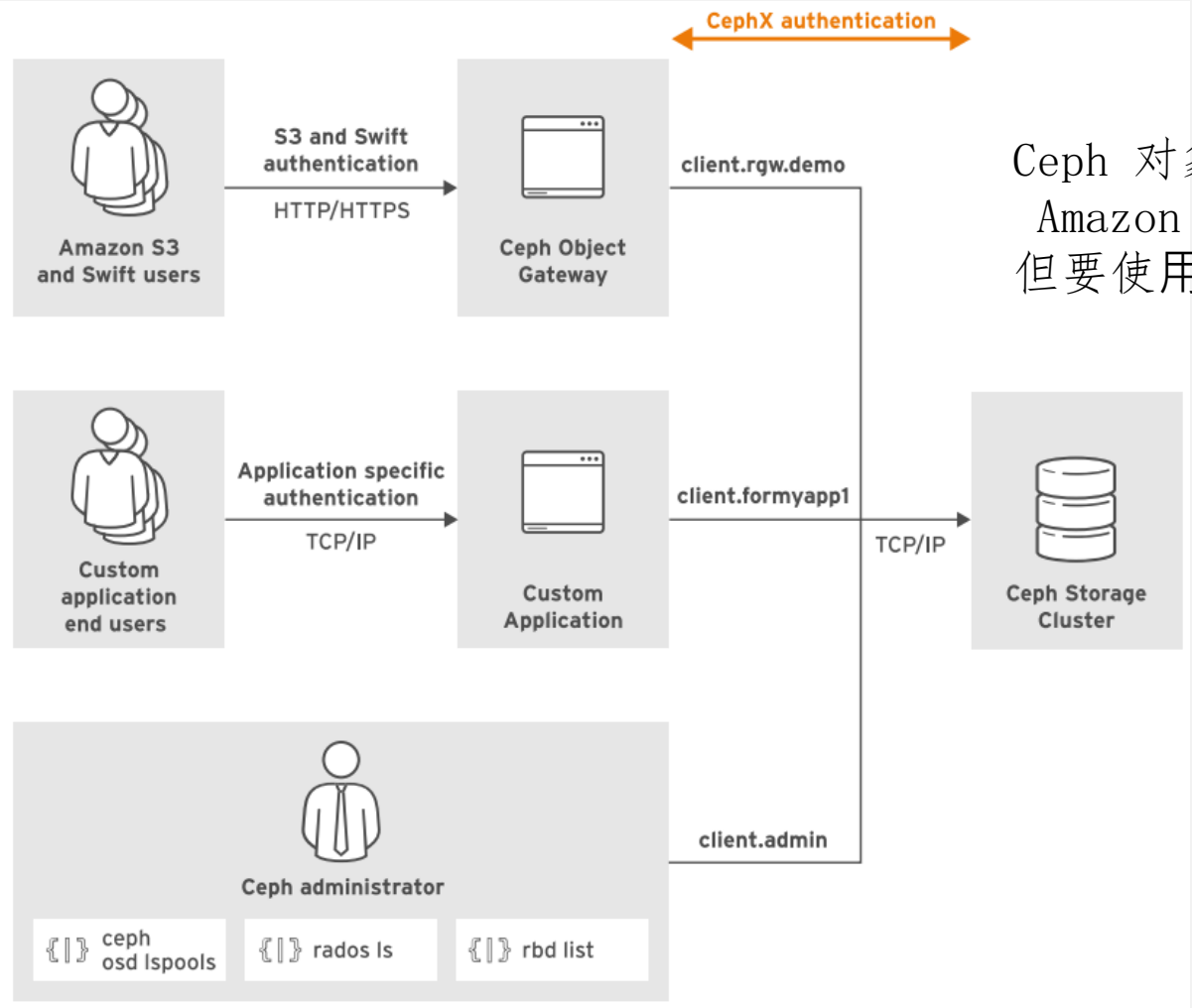
Linux云计算架构师涨薪班

Ceph用户认证与授权

学习目标

- 为什么ceph需要认证
- ceph的认证机制与原理
- 用户命名规范
- ceph命令选项
- ceph添加用户
- 用户授权及权限
- 用户权限修改
- 用户管理与备份
- 用户秘钥环

Ceph认证说明



Ceph 对象网关有自己的用户数据库来验证
Amazon S3 或 Swift 用户的身份
但要使用 client.rgw.demo 帐户来访问集群

Ceph认证机制

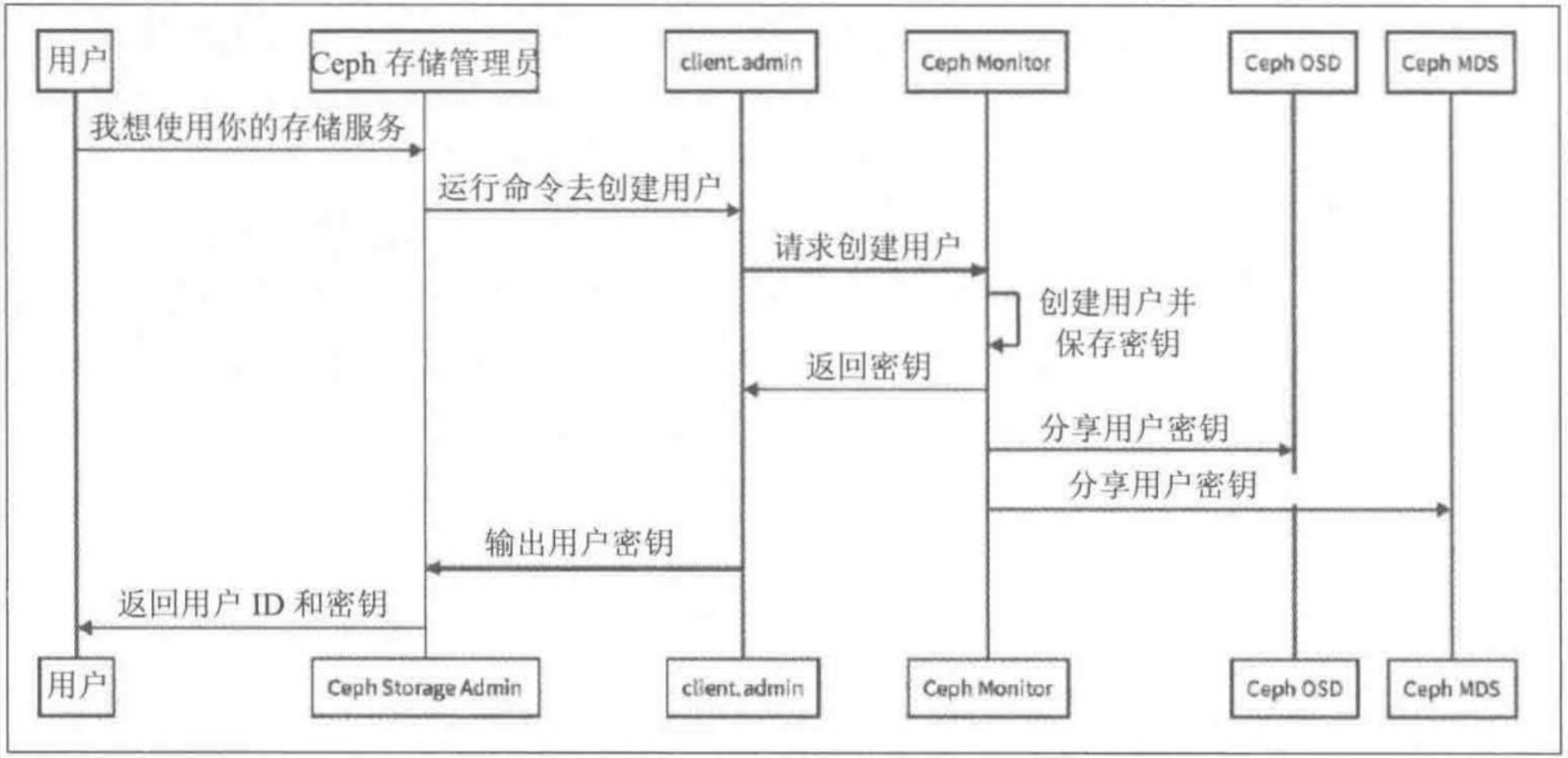
- None：这种模式下，任何用户可以在不经过身份验证时就访问Ceph集群

```
auth_cluster_required = none
auth_service_required = none
auth_client_required = none
```

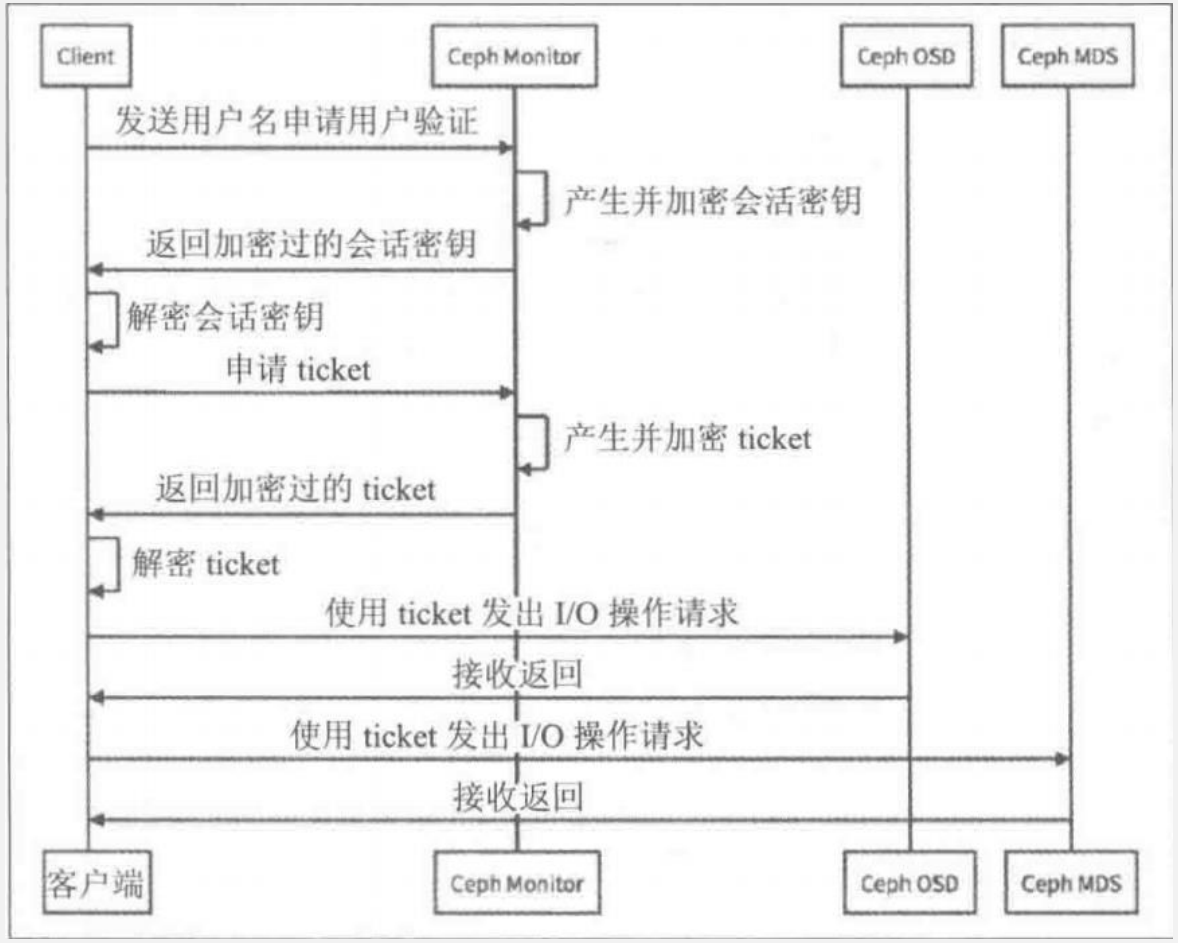
- Cephx：Cephx协议类似于Kerberos协议，它允许经过验证的客户端访问ceph集群

```
auth_cluster_required = cephx
auth_service_required = cephx
auth_client_required = cephx
```

Ceph密钥创建机制



Ceph身份验证过程



Ceph用户命名规范

- Ceph守护进程使用的帐户名与相关守护进程名称匹配：osd.1 或 mon.node1，这些用户默认会在安装时被创建

- librados的客户端应用，帐户名以client.开头。例如，将OpenStack与Ceph集成时，常常会创建专用的client.openstack用户。另外，当部署 Ceph Object Gateway时，会创建client.rgw.帐户。如果要在librados基础上部署自定义软件，也应当创建特定帐户

- Ceph客户端所使用的帐户名以client.开头，运行ceph和rados等命令时使用。安装程序会创建超级管理员client.admin，它具有访问所有内容及修改集群配置的功能。如果运行命令时不通过 --name 或 --id 明确指定用户名，Ceph默认使用client.admin

Ceph命令的选项

- ceph -s
  - --id 用户名
  - --name $type.$id client.admin
  - --keyring 用户秘钥 /etc/ceph/ceph.client.admin.keyring
  - --conf 指定ceph的配置文件
- rados -p pool-name ls
  - --id 用户名
  - --name $type.$id client.admin

添加用户

- ceph auth add
  - 当用户存在，当权限不变，则不进行任何输出
  - 当用户存在，不支持修改权限
  - 示例：ceph auth add client.user1 mon 'allow r' osd 'allow rw pool=pool01’
- ceph auth get-or-create 当用户不存在，则创建用户并授权并返回用户和key
  - 当用户存在，权限不变，返回用户和key
  - 当用户存在，权限修改，则返回报错
  - 示例：ceph auth get-or-create client.user1 mon 'allow r' osd 'allow rw pool=pool01'
- ceph auth get-or-create-key
  - 当用户不存在，则创建用户并授权只返回key
  - 当用户存在，权限不变，只返回key
  - 当用户存在，权限修改，则返回报错
  - 示例：ceph auth get-or-create client.user1 mon 'allow r' osd 'allow rw pool=pool01'

Ceph授权

- Ceph把数据以对象的形式存于各存储池中，Ceph用户必须具有访问存储池的权限才能够读写数据
- Ceph用caps来描述给用户的授权，这样才能使用Mon、OSD和MDS的功能
- caps也用于限制对某一存储池内的数据或某个命名空间的访问
- Ceph管理员用户可在创建或更新普通用户时赋予其相应的caps

CAPS权限说明

权限	描述
allow	在守护进程的访问权限设置之前
r	为用户提供读取权限，需要通过mon来检索集群crush映射
w	授予用户对对象的写入权限
x	授予用户调用对象方法的权限，包括读和写，以及在monitor上执行用户身份验证的权限
*	将一个指定存储池的完整权限（r、w和x）以及执行管理命令的权限授予用户
profile osd	授权一个用户以OSD身份连接其它OSD或者Monitor，用于OSD心跳和状态报告
profile bootstrap-osd	允许用户引导OSD。比如cephadm和ceph-volume工具都使用
profile rbd	授予用戶对 Ceph 块设备的读写权限
profile rbd-read-only	授予用戶对 Ceph 块设备的只读权限

Ceph授权对象

- 授权语法：
  - {daemon-type} allow {capability}' [{daemon-type} 'allow {capability}']
- 授权对象：
  - monitor caps,包括r、w、x参数以及allow profiles {cap}
    - mon 'allow rwx'
    - mon 'allow profile osd'
  - osd caps,包括r、w、x以及profile osd
    - osd 'allow rw'
    - osd 'allow rw pool=rbd ‘ namespace=
  - mds
    - mds 'allow'

授权操作

- 普通授权
  - mon 'allow r' osd 'allow rw'
- 基于存储池的授权
  - mon 'allow r' osd 'allow rw pool=myfirstpool'
- 基于对象前缀授权
  - mon 'allow r' osd 'allow rw object_prefix pref'
- 基于命名空间授权
  - mon 'allow r' osd 'allow rw pool=myfirstpool namespace=photos'
- 基于路径授权
  - 只适用于CephFS，CephFS通过这种方式来限制对特定目录的访问
  - mon 'allow r' osd 'allow rw pool=cephfs_data' mds 'allow rw path=/webcontent'
- 限制用户只能使用特定的管理员指令
  - mon 'allow r, allow command "auth get-or-create", allow command "auth list"'

修改用户权限

- ceph auth caps 用户修改用户授权。如果给定的用户不存在，直接返回报错。如果用户存在，则使用新指定的权限覆盖现有权限。所以，如果只是给用户新增权限，则原来的权限需要原封不动的带上。如果需要删除原来的权限，只需要将该权限设定为空即可。
- ceph auth get client.bob
- ceph auth caps client.bob mon 'allow r' osd 'allow rw pool=liverpool'
- ceph auth caps client.bob mon ' ' osd ' '

用户管理

- 查看系统所有用户
  - ceph auth list
- 获取某个用户的详细信息
  - ceph auth get client.admin
- 获取用户的key
  - ceph auth print-key client.admin
- 删除指定用户
  - ceph auth del client.bob

用户备份

- 导出用户
  - ceph auth get client.bob -o /etc/cephceph.client.bob.keyring
- 导入用户(导入的用户需要有caps权限)
  - ceph auth import -i /etc/ceph/ceph.client.bob.keyring

用户密钥管理

客户端访问ceph集群时，会使用本地的keyring文件，默认依次查找下列路径和名称的keyring文件：

/etc/ceph/$cluster.$name.keyring

/etc/ceph/$cluster.keyring

/etc/ceph/keyring

/etc/ceph/keyring.bin

PS:无论用户的秘钥放在哪个文件都要确保本机上的ceph用户对该文件有读取的权限

誉天教育
YU TIAN EDU

Thank you