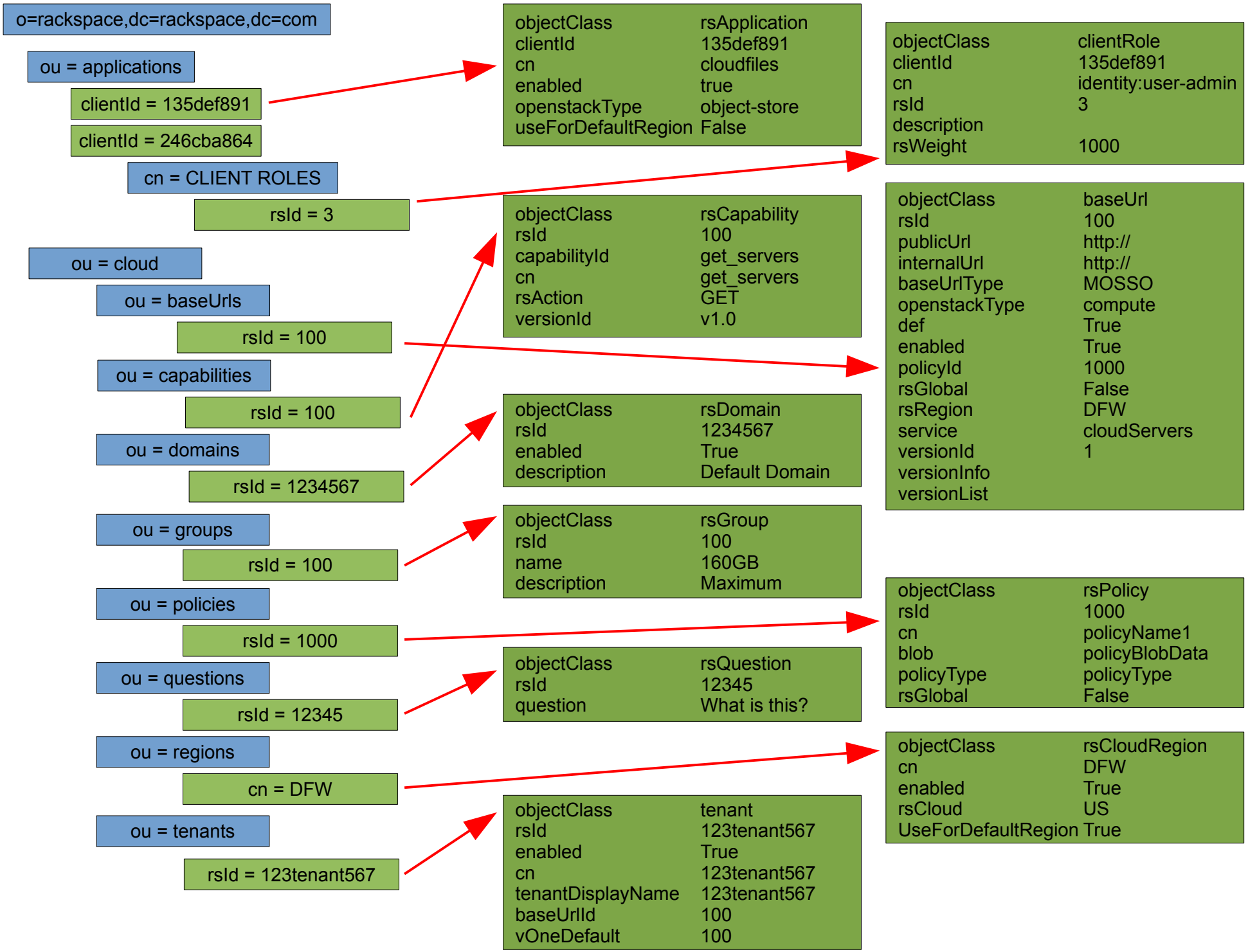
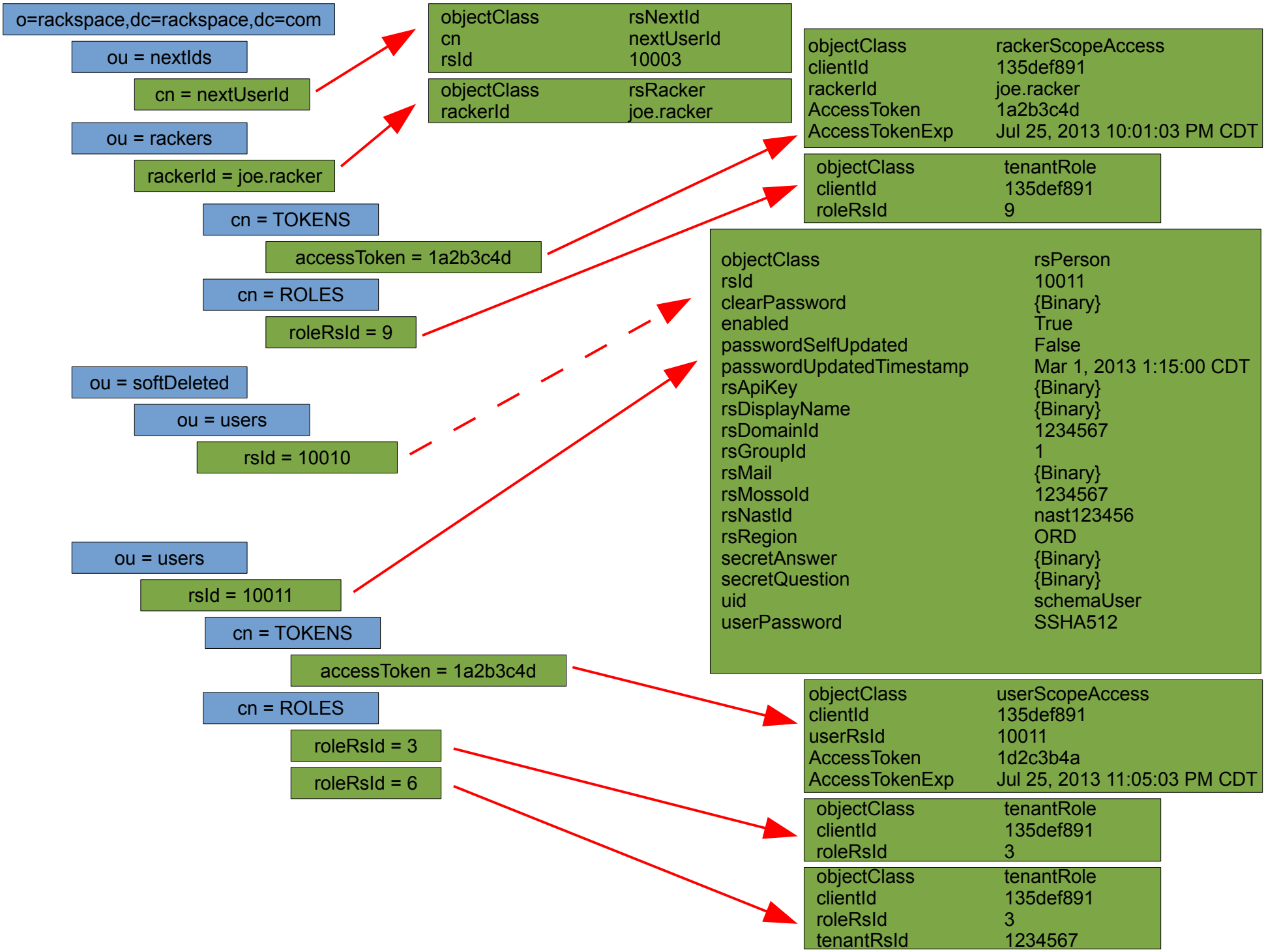
Cloud Identity

LDAP Directory Structure

April 2, 2013


o=rackspace,dc=rackspace,dc=com
ou = applications
clientId = 135def891
clientId = 246cba864
cn = CLIENT ROLES
rsId = 3
ou = cloud
ou = baseUrls
rsId = 100
ou = capabilities
rsId = 100
ou = domains
rsId = 1234567
ou = groups
rsId = 100
ou = policies
rsId = 1000
ou = questions
rsId = 12345
ou = regions
cn = DFW
ou = tenants
rsId = 123tenant567
objectClass rsApplication
clientId 135def891
cn cloudfiles
enabled true
openstackType object-store
useForDefaultRegion False
objectClass clientRole
clientId 135def891
cn identity:user-admin
rsId 3
description
rsWeight 1000
objectClass rsCapability
rsId 100
capabilityId get_servers
cn get_servers
rsAction GET
versionId v1.0
objectClass baseUrl
rsId 100
publicUrl http://
internalUrl http://
baseUrlType MOSSO
openstackType compute
def True
enabled True
policyId 1000
rsGlobal False
rsRegion DFW
service cloudServers
versionId 1
versionInfo
versionList
objectClass rsDomain
rsId 1234567
enabled True
description Default Domain
objectClass rsGroup
rsId 100
name 160GB
description Maximum
objectClass rsPolicy
rsId 1000
cn policyName1
blob policyBlobData
policyType policyType
rsGlobal False
objectClass rsQuestion
rsId 12345
question What is this?
objectClass rsCloudRegion
cn DFW
enabled True
rsCloud US
UseForDefaultRegion True
objectClass tenant
rsId 123tenant567
enabled True
cn 123tenant567
tenantDisplayName 123tenant567
baseUrlId 100
vOneDefault 100


o=rackspace,dc=rackspace,dc=com
ou = nextIds
cn = nextUserId
ou = rackers
rackerId = joe.racker
cn = TOKENS
accessToken = 1a2b3c4d
cn = ROLES
roleRsId = 9
ou = softDeleted
ou = users
rsId = 10010
ou = users
rsId = 10011
cn = TOKENS
accessToken = 1a2b3c4d
cn = ROLES
roleRsId = 3
roleRsId = 6
objectClass rsNextId
cn nextUserId
rsId 10003
objectClass rsRacker
rackerId joe.racker
objectClass rackerScopeAccess
clientId 135def891
rackerId joe.racker
AccessToken 1a2b3c4d
AccessTokenExp Jul 25, 2013 10:01:03 PM CDT
objectClass tenantRole
clientId 135def891
roleRsId 9
objectClass rsPerson
rsId 10011
clearPassword {Binary}
enabled True
passwordSelfUpdated False
passwordUpdatedTimestamp Mar 1, 2013 1:15:00 CDT
rsApiKey {Binary}
rsDisplayName {Binary}
rsDomainId 1234567
rsGroupId 1
rsMail {Binary}
rsMossoId 1234567
rsNastId nast123456
rsRegion ORD
secretAnswer {Binary}
secretQuestion {Binary}
uid schemaUser
userPassword SSHA512
objectClass userScopeAccess
clientId 135def891
userRsId 10011
AccessToken 1d2c3b4a
AccessTokenExp Jul 25, 2013 11:05:03 PM CDT
objectClass tenantRole
clientId 135def891
roleRsId 3
objectClass tenantRole
clientId 135def891
roleRsId 3
tenantRsId 1234567

Applications

- An application defines an available Service.
- An application can contain Roles for a Service.
- The openStackType attribute defines the type of Service
- The “identity” application holds all Global Roles as well as identity roles. (To change in near future to separate identity roles)

Domains

- A Domain can have many Tenants. These become accessible endpoints to users when a user is a member of the Domain.

Groups

- A group defines limits used by other systems.
- A group can be related to a User.

Regions

- A Region defines the region within a deployed Cloud. (Current clouds are US and UK)
- A Cloud must only have one Default Region assigned at a time.
- A region maps to the region for EndpointTemplates.

Tenants

- A Service Catalog consists of a list of EndpointTemplates with Tenants. EndpointTemplates are assigned to a Tenant, which then
- exposes services that the Tenant can be interacted with.

Users

- A user can only be a member of a single Domain.
- A user can have a single default region.
- A user only has a single ApiKey.
- A user can have multiple Groups
- A UID is unique at the “Users” level.
- A user can be assigned multiple Roles.
- A users Service Catalog is managed by Roles containing a Tenant.
- A user can have multiple tokens at any given time.
- An impersonated token lives under the individual doing impersonation. (To change after migration)
- A user has accessible endpoints when the Domain has additional Tenants even though the user doesn't have a role on the Tenant.