rgw - Bug #35988

RGW Ldap Authorization fails

09/14/2018 06:33 PM - Warren Usui

Status:	In Progress	**% Done:**	100%
Priority:	Normal	**Spent time:**	0.00 hour
Assignee:	Matt Benjamin		
Category:			
Target version:			
Source:		**Affected Versions:**	
Tags:		**ceph-qa-suite:**	
Backport:		**Pull request ID:**	
Regression:	No	**Crash signature (v1):**	
Severity:	3 - minor	**Crash signature (v2):**	
Reviewed:			

Description

I believe that this is the same problem as 23091.

Trying to authenticate an ldap RGW user fails.

```
python /tmp/bucket.py
EU
Traceback (most recent call last):
  File "/tmp/bucket.py", line 20, in <module>
    bucket = conn.create_bucket('testuser-new-bucket')
  File "/usr/local/lib/python2.7/dist-packages/boto/s3/connection.py", line 628, in create_bucket
    response.status, response.reason, body)
boto.exception.S3ResponseError: S3ResponseError: 403 Forbidden
<?xml version="1.0" encoding="UTF-8"?><Error><Code>AccessDenied</Code><RequestId>tx000000000000000000
00b-005b9bfd8c-11b8-default</RequestId><HostId>11b8-default-default</HostId></Error>
```

/var/log/ceph/ceph-client.rgw.vpm019.log

```
2018-09-14 18:14:46.797 7efdea2e2700 10 moving default.rgw.meta+users.keys+ewogICAgIlJHV19UT0tFTiI
6IHsKICAgICAgICAidmVyc2lvbiI6IDEsCiAgICAgICAgInR5cGUiOiAibGRhcCIsCiAgICAgICAgImlkIjogInRlc3R1c2VyI
iwKICAgICAgICAia2V5IjogIi9ldGMvYmluZHBhc3MiCiAgICB9Cn0K to cache LRU end
2018-09-14 18:14:46.797 7efdea2e2700  5 error reading user info, uid=ewogICAgIlJHV19UT0tFTiI6IHsKI
CAgICAgICAidmVyc2lvbiI6IDEsCiAgICAgICAgInR5cGUiOiAibGRhcCIsCiAgICAgICAgImlkIjogInRlc3R1c2VyIiwKICA
gICAgICAia2V5IjogIi9ldGMvYmluZHBhc3MiCiAgICB9Cn0K can't authenticate
2018-09-14 18:14:46.797 7efdea2e2700 20 rgw::auth::s3::LocalEngine denied with reason=-2028
2018-09-14 18:14:46.797 7efdea2e2700 20 rgw::auth::s3::AWSAuthStrategy denied with reason=-13
2018-09-14 18:14:46.797 7efdea2e2700  5 Failed the auth strategy, reason=-13
2018-09-14 18:14:46.797 7efdea2e2700 10 failed to authorize request
2018-09-14 18:14:46.797 7efdea2e2700 20 handler->ERRORHANDLER: err_no=-13 new_err_no=-13
2018-09-14 18:14:46.801 7efdea2e2700  2 req 10:1.019706:s3:PUT /testuser-new-bucket/:create_bucket
:op status=0
2018-09-14 18:14:46.801 7efdea2e2700  2 req 10:1.019745:s3:PUT /testuser-new-bucket/:create_bucket
:http status=403
2018-09-14 18:14:46.801 7efdea2e2700  1 ====== req done req=0x7efdea2d9830 op status=0 http_status
=403 ======
2018-09-14 18:14:46.801 7efdea2e2700 20 process_request() returned -13
2018-09-14 18:14:46.801 7efdea2e2700  1 civetweb: 0x55bdfea0c000: 172.21.2.19 - - [14/Sep/2018:18:
14:45 +0000] "PUT /testuser-new-bucket/ HTTP/1.1" 403 389 - Boto/2.49.0 Python/2.7.12 Linux/4.4.0-
24-generic
```

```
2018-09-14 18:14:52.165 7efe03efa700  2 RGWDataChangesLog::ChangesRenewThread: start
```

/etc/ceph/ceph.conf

```
[global]
public network = 172.21.2.0/21
fsid = f3b87010-5fc0-4721-8d54-d351a1a89e1e
mon_initial_members = vpm019, vpm125, vpm153
mon_host = 172.21.2.19,172.21.2.125,172.21.2.153
auth_cluster_required = cephx
auth_service_required = cephx
auth_client_required = cephx
rgw_ldap_secret = "/etc/bindpass"
rgw_ldap_uri = "ldap://vpm169.front.sepia.ceph.com"
rgw_ldap_binddn = "uid=ceph,cn=users,cn=accounts,dc=front,dc=sepia,dc=ceph,dc=com"
rgw_ldap_searchdn = "cn=users,cn=accounts,dc=front,dc=sepia,dc=ceph,dc=com"
rgw_ldap_dnattr = "uid"
rgw_s3_auth_use_ldap = "true"
debug rgw = 20

[client.rgw.vpm019]
rgw_frontends = "civetweb port=7480"
```

/tmp/bucket.py

```
import boto
import boto.s3.connection

access_key = "ewogICAgIlJHV19UT0tFTiI6IHsKICAgICAgICAidmVyc2lvbiI6IDEsCiAgICAgICAgInR5cGUiOiAibGRh
cCIsCiAgICAgICAgImlkIjogInRlc3R1c2VyIiwKICAgICAgICAia2V5IjogIi9ldGMvYmluZHBhc3MiCiAgICB9Cn0K"

secret_key = ""

boto.config.add_section('s3')
boto.config.set('s3', 'use-sigv2', 'True')
conn = boto.connect_s3(
    aws_access_key_id = access_key,
    aws_secret_access_key = secret_key,
    host = "vpm019.front.sepia.ceph.com",
    port = 7480,
    is_secure=False,
    calling_format = boto.s3.connection.OrdinaryCallingFormat(),
    )

print boto.s3.connection.Location.EU
bucket = conn.create_bucket('testuser-new-bucket')
for bucket in conn.get_all_buckets():
    print "{name}\t{created}".format(
        name = bucket.name,
        created = bucket.creation_date,
)
```

ldapsearch using the uri, binddn and searchdn used in /etc/ceph/ceph.conf works.

```
ldapsearch -x -D 'uid=ceph,cn=users,cn=accounts,dc=front,dc=sepia,dc=ceph,dc=com' -H ldap://vpm169
.front.sepia.ceph.com -b 'cn=users,cn=accounts,dc=front,dc=sepia,dc=ceph,dc=com' -s sub 'uid=testu
```

```
ser' -w t0pSecret
# extended LDIF
#
# LDAPv3
# base <cn=users,cn=accounts,dc=front,dc=sepia,dc=ceph,dc=com> with scope subtree
# filter: uid=testuser
# requesting: ALL
#

# testuser, users, accounts, front.sepia.ceph.com
dn: uid=testuser,cn=users,cn=accounts,dc=front,dc=sepia,dc=ceph,dc=com
displayName: test user
uid: testuser
objectClass: ipaobject
objectClass: person
objectClass: top
objectClass: ipasshuser
objectClass: inetorgperson
objectClass: organizationalperson
objectClass: krbticketpolicyaux
objectClass: krbprincipalaux
objectClass: inetuser
objectClass: posixaccount
objectClass: ipaSshGroupOfPubKeys
objectClass: mepOriginEntry
loginShell: /bin/sh
initials: tu
gecos: test user
sn: user
homeDirectory: /home/testuser
mail: testuser@front.sepia.ceph.com
krbPrincipalName: testuser@FRONT.SEPIA.CEPH.COM
givenName: test
cn: test user
ipaUniqueID: 630cc0ba-b7af-11e8-8bed-525400ae0e7b
uidNumber: 1463400003
gidNumber: 1463400003
memberOf: cn=ipausers,cn=groups,cn=accounts,dc=front,dc=sepia,dc=ceph,dc=com
krbPasswordExpiration: 20180913234827Z
krbLastPwdChange: 20180913234827Z

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

Subtasks:

Bug # 23091: rgw + OpenLDAP = Failed the auth strategy, reason=-13	**Duplicate**

History

#1 - 09/20/2018 06:11 PM - Matt Benjamin

- Status changed from New to In Progress

- Assignee set to Matt Benjamin

Hi Warren,

Ok, actually this looks like RGW isn't attempting to use the ExternalAuthStrategy. It does look like you proved the ldap search creds are good, the bind creds might not be, but I would not assume that.

Matt

#2 - 02/06/2019 03:08 PM - Bernhard Krieger

Matt Benjamin wrote:

> Hi Warren,
>
> Ok, actually this looks like RGW isn't attempting to use the ExternalAuthStrategy. It does look like you proved the ldap search creds are good, the bind creds might not be, but I would not assume that.
>
> Matt

Running into same issue (13.2.4 CentOS7)
Cred and filter are correct. Bind to ldap is working when rgw starts.

I did a tcpdump.
Rgw didnt make a user lookup to the ldap server when a s3client is connecting to rgw instance.

#3 - 02/06/2019 03:22 PM - Matt Benjamin

Warren's issue turned out to be internal iiuc, but perhaps Warren, you can comment?

In my experience w/Centos, RHEL, this would most likely be related to TLS cert verification, and I'd suggest experimentally disabling it to find out.

regards,

Matt