Arvados - Feature #15599

[keepstore] AWS support IAM roles for authentication

08/28/2019 06:13 PM - Ward Vandewege

Status:	Resolved	**Start date:**	10/01/2019
Priority:	Normal	**Due date:**	
Assigned To:	Tom Clegg	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	2019-10-09 Sprint		

Description

AWS best practice for services running on EC2 is to use IAM roles for authentication. The AWS go sdk supports this natively, cf. https://docs.aws.amazon.com/sdk-for-go/v1/developer-guide/configuring-sdk.html

It would be nice if Keepstore supported IAM roles, perhaps falling back to that authentication method when SecretKeyFile and AccessKeyFile are not supplied in the configuration file. Maybe using the metadata to detect that it's running on EC2 first so we don't provide confusing information when no credentials are present and Keepstore is running elsewhere.

Getting credentials from instance metadata:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html#instance-metadata-security-credentials

Subtasks:

Task # 15619: Review 15599-keepstore-iam-role	**Resolved**

Associated revisions

Revision 3911cd83 - 10/02/2019 03:48 PM - Tom Clegg

Merge branch '15599-keepstore-iam-role'

closes #15599

Arvados-DCO-1.1-Signed-off-by: Tom Clegg <tclegg@veritasgenetics.com>

History

#1 - 08/28/2019 06:21 PM - Ward Vandewege

- Target version set to To Be Groomed

#2 - 09/04/2019 01:54 PM - Tom Clegg

- Description updated

#3 - 09/04/2019 02:05 PM - Tom Morris

- Target version changed from To Be Groomed to Arvados Future Sprints

- Story points set to 2.0

#4 - 09/11/2019 02:57 PM - Tom Morris

- Target version changed from Arvados Future Sprints to 2019-09-25 Sprint

#5 - 09/11/2019 03:05 PM - Tom Clegg

- Assigned To set to Tom Clegg

#9 - 09/12/2019 02:35 PM - Tom Clegg

- Status changed from New to In Progress

#10 - 09/12/2019 02:56 PM - Tom Clegg

15599-keepstore-iam-role @ 47afcd7595b49cf8a1756cb8f00139cd6269f544 -- https://ci.curoverse.com/view/Developer/job/developer-run-tests/1521/

(hasn't been tested on a real cluster yet)

#12 - 09/25/2019 03:15 PM - Tom Clegg

- Target version changed from 2019-09-25 Sprint to 2019-10-09 Sprint

#13 - 09/27/2019 09:32 PM - Tom Clegg

Tested on 4xphq with explicit role name in config file:


```
{"PID":18718,"level":"info","msg":"keepstore dev starting, pid 18718","time":"2019-09-27T21:00:49.465594064Z"}
{"PID":18718,"URL":"http://169.254.169.254/latest/meta-data/iam/security-credentials/keepstore-s3","level":"de
bug","msg":"getting credentials","time":"2019-09-27T21:00:49.465725839Z"}
{"AccessKeyID":"ASIA3EZBYHRBBUPFAKFB","Expiration":"2019-09-28T02:57:38Z","LastUpdated":"2019-09-27T20:43:26Z"
,"PID":18718,"TTL":"5h51m48.533271563s","level":"debug","msg":"updated credentials","time":"2019-09-27T21:00:4
9.466734253Z"}
{"PID":18718,"level":"info","msg":"started volume 4xphq-nyw5e-dk9mjspdg2v8mhq
 (s3-bucket:\"4xphq-keep\"), ReadOnly=false","time":"2019-09-27T21:00:49.466829958Z"}
{"Listen":"10.20.65.1:22222","PID":18718,"Service":"keepstore","URL":"http://keep0.4xphq.arvadosapi.com:22222"
,"level":"info","msg":"listening","time":"2019-09-27T21:00:49.483401771Z"}
{"PID":18718,"RequestID":"req-1r4cxk9sf6cua1xnv358","level":"info","msg":"request","remoteAddr":"10.20.65.1:27
940","reqBytes":3,"reqForwardedFor":"","reqHost":"keep0:22222","reqMethod":"PUT","reqPath":"acbd18db4cc2f85ced
ef654fccc4a4d8","reqQuery":"","time":"2019-09-27T21:00:55.469119263Z"}
{"PID":18718,"RequestID":"req-1r4cxk9sf6cua1xnv358","level":"info","msg":"response","remoteAddr":"10.20.65.1:2
7940","reqBytes":3,"reqForwardedFor":"","reqHost":"keep0:22222","reqMethod":"PUT","reqPath":"acbd18db4cc2f85ce
def654fccc4a4d8","reqQuery":"","respBytes":86,"respStatus":"OK","respStatusCode":200,"time":"2019-09-27T21:00:
55.600618560Z","timeToStatus":0.131478,"timeTotal":0.131497,"timeWriteBody":0.000019}
```


Tested on 4xphq with no role/keys at all in config file:


```
{"PID":22175,"level":"info","msg":"keepstore dev starting, pid 22175","time":"2019-09-27T21:17:04.277819697Z"}
{"PID":22175,"URL":"http://169.254.169.254/latest/meta-data/iam/security-credentials/","level":"debug","msg":"
looking up IAM role name","time":"2019-09-27T21:17:04.277925380Z"}
{"PID":22175,"Role":"keepstore-s3","level":"debug","msg":"looked up IAM role name","time":"2019-09-27T21:17:04
.278761723Z"}
{"PID":22175,"URL":"http://169.254.169.254/latest/meta-data/iam/security-credentials/keepstore-s3","level":"de
bug","msg":"getting credentials","time":"2019-09-27T21:17:04.278789657Z"}
{"AccessKeyID":"ASIA3EZBYHRBBUPFAKFB","Expiration":"2019-09-28T02:57:38Z","LastUpdated":"2019-09-27T20:43:26Z"
,"PID":22175,"TTL":"5h35m33.720482749s","level":"debug","msg":"updated credentials","time":"2019-09-27T21:17:0
4.279522613Z"}
{"PID":22175,"level":"info","msg":"started volume 4xphq-nyw5e-dk9mjspdg2v8mhq
 (s3-bucket:\"4xphq-keep\"), ReadOnly=false","time":"2019-09-27T21:17:04.279577157Z"}
{"Listen":"10.20.65.1:22222","PID":22175,"Service":"keepstore","URL":"http://keep0.4xphq.arvadosapi.com:22222"
,"level":"info","msg":"listening","time":"2019-09-27T21:17:04.290799872Z"}
{"PID":22175,"RequestID":"req-1ozvvwrenud7l1kn6t7i","level":"info","msg":"request","remoteAddr":"10.20.65.1:28
180","reqBytes":3,"reqForwardedFor":"","reqHost":"keep0:22222","reqMethod":"PUT","reqPath":"acbd18db4cc2f85ced
ef654fccc4a4d8","reqQuery":"","time":"2019-09-27T21:18:01.033740317Z"}
{"PID":22175,"RequestID":"req-1ozvvwrenud7l1kn6t7i","level":"info","msg":"response","remoteAddr":"10.20.65.1:2
8180","reqBytes":3,"reqForwardedFor":"","reqHost":"keep0:22222","reqMethod":"PUT","reqPath":"acbd18db4cc2f85ce
def654fccc4a4d8","reqQuery":"","respBytes":86,"respStatus":"OK","respStatusCode":200,"time":"2019-09-27T21:18:
01.172539408Z","timeToStatus":0.138775,"timeTotal":0.138793,"timeWriteBody":0.000019}
```


15599-keepstore-iam-role @ 0b4def357b45cec17ee45673aa14d64ec99c56c3 --
https://ci.curoverse.com/view/Developer/job/developer-run-tests/1558/

#14 - 09/30/2019 11:24 PM - Tom Clegg

15599-keepstore-iam-role @ 5612cb8542511ea96108604499b8b7e37e3804c2 --
https://ci.curoverse.com/view/Developer/job/developer-run-tests/1568/

#15 - 10/01/2019 01:55 PM - Tom Clegg

15599-keepstore-iam-role @ 5612cb8542511ea96108604499b8b7e37e3804c2 --
https://ci.curoverse.com/view/Developer/job/developer-run-tests/1569/

#16 - 10/01/2019 06:36 PM - Peter Amstutz

Documentation nit, the example in configure-s3-object-storage.html has values for both "IAMRole" and "AccessKey"/"SecretKey", which are mutually exclusive. (Is there are error if they are both configured?) Would be better to leave all the fields blank and explain the *default* behavior and then how to override it.

#17 - 10/01/2019 07:05 PM - Tom Clegg

15599-keepstore-iam-role @ fbbba2116c046a3c20a71ea0268501a1a5b802e5 --
https://ci.curoverse.com/view/Developer/job/developer-run-tests/1573/

- config example has blanks, and presents blank/automatic as the normal case
- startup error if config is ambiguous (IAMRole and Secret/AccessKey are both non-empty)

#18 - 10/01/2019 08:20 PM - Peter Amstutz

Tom Clegg wrote:

> 15599-keepstore-iam-role @ fbbba2116c046a3c20a71ea0268501a1a5b802e5 -- https://ci.curoverse.com/view/Developer/job/developer-run-tests/1573/
>
> - config example has blanks, and presents blank/automatic as the normal case
> - startup error if config is ambiguous (IAMRole and Secret/AccessKey are both non-empty)

LGTM

#19 - 10/02/2019 05:10 PM - Tom Clegg

- Status changed from In Progress to Resolved

Applied in changeset arvados|3911cd836c4e937262d48f9b0af703a9d7d68cdd.

#20 - 10/03/2019 02:49 PM - Tom Clegg

- Release set to 22