Hadoop HDFS / HDFS-13682

Cannot create encryption zone after KMS auth token expires

Details

Type:	Bug	Status:	RESOLVED
Priority:	Critical	Resolution:	Fixed
Affects Version/s:	3.0.0	Fix Version/s:	3.2.0, 3.1.1, 3.0.4
Component/s:	encryption, kms, namenode		
Labels:	None		
Target Version/s:	3.2.0, 3.1.1, 3.0.4		
Hadoop Flags:	Reviewed		

Description

Our internal testing reported this behavior recently.

```
[root@nightly6x-1 ~]# sudo -u hdfs /usr/bin/kinit -kt /cdep/keytabs/hdfs.keytab hdfs -l 30d -r 30d
[root@nightly6x-1 ~]# sudo -u hdfs klist
Ticket cache: FILE:/tmp/krb5cc_994
Default principal: hdfs@GCE.CLOUDERA.COM

Valid starting       Expires              Service principal
06/12/2018 03:24:09  07/12/2018 03:24:09  krbtgt/GCE.CLOUDERA.COM@GCE.CLOUDERA.COM
[root@nightly6x-1 ~]# sudo -u hdfs hdfs crypto -createZone -keyName key77 -path /user/systest/ez
RemoteException: org.apache.hadoop.security.authentication.client.AuthenticationException: GSSException: No valid credentials p
```

Upon further investigation, it's due to the KMS client (cached in HDFS NN) cannot authenticate with the server after the authentication token (which is cached by KMSCP) expires, even if the HDFS client RPC has valid kerberos credentials.

Attachments

HDFS-13682.01.patch	5 kB	15/Jun/18 16:09
HDFS-13682.02.patch	6 kB	19/Jun/18 02:50
HDFS-13682.03.patch	6 kB	20/Jun/18 18:23
HDFS-13682.dirty.repro.branch-2.patch	16 kB	15/Jun/18 03:30
HDFS-13682.dirty.repro.patch	15 kB	14/Jun/18 22:31

Issue Links

causes

HADOOP-16761 KMSClientProvider does not work with client using ticket logged in externally OPEN

Activity

Xiao Chen added a comment - 14/Jun/18 22:42

Updated a patch that reproduces this. One potential solution is to call the KMS as the login user, because all these are hdfs superuser-only ops. Uncommenting the changes in FSDirEncryptionZoneOp would pass the test. I propose in this jira, we do this one for createZone.

This a passing in CDH5, and failing in CDH6. I automatically suspected ~~HADOOP-9747~~, but cannot blame on it for anything. 🙂
One difference I noticed is that, In CDH5 we don't have these lines in KerberosAuthenticator, which is added by ~~HADOOP-11332~~. Not sure what's the correct solution here regarding that, but if we do this as the login user, the check should pass and no new subject need to be created.

daryn, may I ask for your thoughts here? Thanks for the time.

Xiao Chen added a comment - 15/Jun/18 04:08 - edited

Took an easier route and debugged branch-2. It turns out ~~HADOOP-9747~~ does have some effects here - specifically at this method. When this meets the KMSCP's morph-based-on-ugi logic, the ugi being used as actual changed from loginUgi to currentUgi. (Also has a weird HTTP 400 somehow, which is fixed if contentType is not empty).

Following this, I confirmed if we change `KMSCP#getActualUgi`'s check from `actualUgi.hasKerberosCredentials()` to `!actualUgi.isFromKeytab() && !actualUgi.isFromTicket()` (and making `UGI#isFromTicket` public of course), the test passes. This appears to be a more 'compatible' change. Patch 1 tries to do this.

IMO we should still consider explicitly doing the KMS calls in the NN using the NN login ugi, this applies to both the `getMetadata` call during createEZ and the `generateEncryptedKey` call from startFile. Reason being these calls are internal to the NN, and the hdfs rpc caller isn't expected to really interact with the KMS in these cases. Can do this in a separate Jira if it sounds good to the audience.

genericqa added a comment - 15/Jun/18 06:37

☒ **-1 overall**

Vote	Subsystem	Runtime	Comment
0	reexec	0m 28s	Docker mode activated.
			Prechecks
+1	@author	0m 0s	The patch does not contain any @author tags.
+1	test4tests	0m 0s	The patch appears to include 1 new or modified test files.
			trunk Compile Tests
0	mvndep	0m 19s	Maven dependency ordering for branch
+1	mvninstall	27m 12s	trunk passed
+1	compile	29m 50s	trunk passed
+1	checkstyle	0m 23s	trunk passed
+1	mvnsite	2m 26s	trunk passed
-1	shadedclient	5m 7s	branch has errors when building and testing our client artifacts.
+1	findbugs	4m 4s	trunk passed
+1	javadoc	1m 49s	trunk passed
			Patch Compile Tests
0	mvndep	0m 19s	Maven dependency ordering for patch
-1	mvninstall	0m 56s	hadoop-hdfs in the patch failed.
-1	compile	2m 26s	root in the patch failed.
-1	javac	2m 26s	root in the patch failed.
+1	checkstyle	0m 13s	the patch passed
-1	mvnsite	1m 9s	hadoop-hdfs in the patch failed.
+1	whitespace	0m 0s	The patch has no whitespace issues.
-1	shadedclient	1m 54s	patch has errors when building and testing our client artifacts.
-1	findbugs	0m 22s	hadoop-hdfs in the patch failed.
+1	javadoc	1m 37s	the patch passed
			Other Tests
+1	unit	9m 31s	hadoop-common in the patch passed.
-1	unit	0m 57s	hadoop-hdfs in the patch failed.
+1	asflicense	0m 24s	The patch does not generate ASF License warnings.
		93m 50s	

Subsystem	Report/Notes
Docker	Client=17.05.0-ce Server=17.05.0-ce Image:yetus/hadoop:abb62dd
JIRA Issue	~~HDFS-13682~~
JIRA Patch URL	https://issues.apache.org/jira/secure/attachment/12927933/HDFS-13682.01.patch
Optional Tests	asflicense compile javac javadoc mvninstall mvnsite unit shadedclient findbugs checkstyle
uname	Linux 01cc4873cf4c 3.13.0-143-generic #192-Ubuntu SMP Tue Feb 27 10:45:36 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
Build tool	maven
Personality	/testptch/patchprocess/precommit/personality/provided.sh
git revision	trunk / 020dd61
maven	version: Apache Maven 3.3.9
Default Java	1.8.0_171
findbugs	v3.1.0-RC1
mvninstall	https://builds.apache.org/job/PreCommit-HDFS-Build/24449/artifact/out/patch-mvninstall-hadoop-hdfs-project_hadoop-hdfs.txt
compile	https://builds.apache.org/job/PreCommit-HDFS-Build/24449/artifact/out/patch-compile-root.txt
javac	https://builds.apache.org/job/PreCommit-HDFS-Build/24449/artifact/out/patch-compile-root.txt
mvnsite	https://builds.apache.org/job/PreCommit-HDFS-Build/24449/artifact/out/patch-mvnsite-hadoop-hdfs-project_hadoop-hdfs.txt
findbugs	https://builds.apache.org/job/PreCommit-HDFS-Build/24449/artifact/out/patch-findbugs-hadoop-hdfs-project_hadoop-hdfs.txt
unit	https://builds.apache.org/job/PreCommit-HDFS-Build/24449/artifact/out/patch-unit-hadoop-hdfs-project_hadoop-hdfs.txt
Test Results	https://builds.apache.org/job/PreCommit-HDFS-Build/24449/testReport/
Max. process+thread count	1348 (vs. ulimit of 10000)
modules	C: hadoop-common-project/hadoop-common hadoop-hdfs-project/hadoop-hdfs U: .
Console output	https://builds.apache.org/job/PreCommit-HDFS-Build/24449/console
Powered by	Apache Yetus 0.8.0-SNAPSHOT http://yetus.apache.org

This message was automatically generated.

genericqa added a comment - 15/Jun/18 20:05

☒ **-1 overall**

Vote	Subsystem	Runtime	Comment
0	reexec	0m 22s	Docker mode activated.
			Prechecks
+1	@author	0m 0s	The patch does not contain any @author tags.
+1	test4tests	0m 0s	The patch appears to include 1 new or modified test files.
			trunk Compile Tests
0	mvndep	0m 19s	Maven dependency ordering for branch
+1	mvninstall	26m 46s	trunk passed
+1	compile	29m 39s	trunk passed
+1	checkstyle	0m 23s	trunk passed
+1	mvnsite	2m 22s	trunk passed

-1	shadedclient	5m 6s	branch has errors when building and testing our client artifacts.
+1	findbugs	3m 40s	trunk passed
+1	javadoc	1m 55s	trunk passed
			Patch Compile Tests
0	mvndep	0m 18s	Maven dependency ordering for patch
+1	mvninstall	1m 50s	the patch passed
+1	compile	28m 45s	the patch passed
+1	javac	28m 45s	the patch passed
+1	checkstyle	0m 24s	the patch passed
+1	mvnsite	2m 21s	the patch passed
+1	whitespace	0m 0s	The patch has no whitespace issues.
-1	shadedclient	2m 13s	patch has errors when building and testing our client artifacts.
+1	findbugs	3m 57s	the patch passed
+1	javadoc	1m 57s	the patch passed
			Other Tests
+1	unit	9m 19s	hadoop-common in the patch passed.
-1	unit	110m 57s	hadoop-hdfs in the patch failed.
+1	asflicense	1m 1s	The patch does not generate ASF License warnings.
		232m 52s	

Reason	Tests
Failed junit tests	hadoop.hdfs.qjournal.server.TestJournalNodeSync

Subsystem	Report/Notes
Docker	Client=17.05.0-ce Server=17.05.0-ce Image:yetus/hadoop:abb62dd
JIRA Issue	~~HDFS-13682~~
JIRA Patch URL	https://issues.apache.org/jira/secure/attachment/12928006/HDFS-13682.01.patch
Optional Tests	asflicense compile javac javadoc mvninstall mvnsite unit shadedclient findbugs checkstyle
uname	Linux 477af303e894 3.13.0-143-generic #192-Ubuntu SMP Tue Feb 27 10:45:36 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
Build tool	maven
Personality	/testptch/patchprocess/precommit/personality/provided.sh
git revision	trunk / 3e37a9a
maven	version: Apache Maven 3.3.9
Default Java	1.8.0_171
findbugs	v3.1.0-RC1
unit	https://builds.apache.org/job/PreCommit-HDFS-Build/24456/artifact/out/patch-unit-hadoop-hdfs-project_hadoop-hdfs.txt
Test Results	https://builds.apache.org/job/PreCommit-HDFS-Build/24456/testReport/
Max. process+thread count	2718 (vs. ulimit of 10000)
modules	C: hadoop-common-project/hadoop-common hadoop-hdfs-project/hadoop-hdfs U: .
Console output	https://builds.apache.org/job/PreCommit-HDFS-Build/24456/console
Powered by	Apache Yetus 0.8.0-SNAPSHOT http://yetus.apache.org

This message was automatically generated.

Xiao Chen added a comment - 15/Jun/18 20:09 - edited

Test failures doesn't look related. daryn / weichiu, do you have cycles to review?

Wei-Chiu Chuang added a comment - 18/Jun/18 18:00

Still trying to understand it –
The gist of the patch is this line

```
!actualUgi.isFromKeytab() && !actualUgi.isFromTicket()
```

If I am not mistaken, this is effectively

```
!actualUgi.shouldRelogin()
```

What the patch tries to do is use the HDFS NameNode's login UGI to access KMS, instead of the current UGI (which issues crypto -createZone command).

Would this cause confusion in enforcing KMS access control? Note that HDFS NameNode allows createEncryptionZone operation for super users (may not even be hdfs user) and after the patch, KMS would only see the request coming from hdfs user.

Additionally, UGI.shouldRelogin() depends on isHadoopLogin(). I am curious what's the effect if the subject is actually managed externally (as allowed ~~HADOOP-13805~~). (I understand that ~~HADOOP-9747~~ removed some code in ~~HADOOP-13805~~, but I have not been able to reason if it would still allow externally managed subjects)

Xiao Chen added a comment - 18/Jun/18 19:08

Thanks for taking a look Wei-Chiu.

Could you clarify the fist comment? Are you suggesting to replace the checks with `shouldRelogin`?

> Would this cause confusion in enforcing KMS access control? ... after the patch, KMS would only see the request coming from hdfs user.

loginuser is the branch-2 behavior as well. So this patch is to bring the old behavior back (the dirty.repro on branch-2 shows this)
From API perspective, it feels to me the hdfs superuser that creates the zone only needs hdfs privilege (to reach NN). The getMetadata call from NN to KMS isn't returned to the caller.

> externally managed subjects

Can we create a follow-on to ~~HADOOP-9747~~ to investigate this?

Wei-Chiu Chuang added a comment - 18/Jun/18 20:20

Sorry for not being specific.

Re: UGI.shouldRelogin().
I just feel that the if statement in KMSCP#getActualUgi() is long and confusing. it might help readability by making the if statement a separate helper method.

Regarding the user authentication & subjects, I'll follow up separately. I want to be especially careful here since it's quite easy to break existing behavior in UGI.

Xiao Chen added a comment - 19/Jun/18 02:50

Thanks for the clarification Wei-Chiu!

Patch 2 refactored a bit to improve the if statement in `KMSCP#getActualUgi` with a dedicated method.
External subject thing looks to be handled by ~~HADOOP-9747~~ ok. There are some comments on the jira, and `UGI#isHadoopLogin` is the method that handles it.

genericqa added a comment - 19/Jun/18 06:41

☒ **-1 overall**

Vote	Subsystem	Runtime	Comment
0	reexec	0m 29s	Docker mode activated.
			Prechecks
+1	@author	0m 0s	The patch does not contain any @author tags.
+1	test4tests	0m 0s	The patch appears to include 1 new or modified test files.
			trunk Compile Tests
0	mvndep	1m 56s	Maven dependency ordering for branch
+1	mvninstall	26m 54s	trunk passed
+1	compile	29m 36s	trunk passed
+1	checkstyle	0m 23s	trunk passed
+1	mvnsite	2m 25s	trunk passed
-1	shadedclient	5m 10s	branch has errors when building and testing our client artifacts.
+1	findbugs	3m 44s	trunk passed
+1	javadoc	1m 55s	trunk passed
			Patch Compile Tests
0	mvndep	0m 18s	Maven dependency ordering for patch
+1	mvninstall	1m 50s	the patch passed
+1	compile	28m 26s	the patch passed
+1	javac	28m 26s	the patch passed
+1	checkstyle	0m 24s	the patch passed
+1	mvnsite	2m 22s	the patch passed
+1	whitespace	0m 0s	The patch has no whitespace issues.
-1	shadedclient	2m 14s	patch has errors when building and testing our client artifacts.
+1	findbugs	3m 59s	the patch passed
+1	javadoc	1m 52s	the patch passed
			Other Tests
+1	unit	9m 15s	hadoop-common in the patch passed.
-1	unit	94m 33s	hadoop-hdfs in the patch failed.
+1	asflicense	0m 45s	The patch does not generate ASF License warnings.
		217m 37s	

Reason	Tests
Failed junit tests	hadoop.hdfs.server.namenode.TestReencryptionWithKMS
	hadoop.hdfs.qjournal.server.TestJournalNodeSync

Subsystem	Report/Notes
Docker	Client=17.05.0-ce Server=17.05.0-ce Image:yetus/hadoop:abb62dd
JIRA Issue	~~HDFS-13682~~
JIRA Patch URL	https://issues.apache.org/jira/secure/attachment/12928286/HDFS-13682.02.patch
Optional Tests	asflicense compile javac javadoc mvninstall mvnsite unit shadedclient findbugs checkstyle
uname	Linux bbd5b16ce9bf 3.13.0-143-generic #192-Ubuntu SMP Tue Feb 27 10:45:36 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
Build tool	maven
Personality	/testptch/patchprocess/precommit/personality/provided.sh
git revision	trunk / f386e78

maven	version: Apache Maven 3.3.9
Default Java	1.8.0_171
findbugs	v3.1.0-RC1
unit	https://builds.apache.org/job/PreCommit-HDFS-Build/24475/artifact/out/patch-unit-hadoop-hdfs-project_hadoop-hdfs.txt
Test Results	https://builds.apache.org/job/PreCommit-HDFS-Build/24475/testReport/
Max. process+thread count	3226 (vs. ulimit of 10000)
modules	C: hadoop-common-project/hadoop-common hadoop-hdfs-project/hadoop-hdfs U: .
Console output	https://builds.apache.org/job/PreCommit-HDFS-Build/24475/console
Powered by	Apache Yetus 0.8.0-SNAPSHOT http://yetus.apache.org

This message was automatically generated.

Wei-Chiu Chuang added a comment - 20/Jun/18 16:53

Thanks xiaochen!

Ok, I think the bug report & fix makes sense. so looks like the externally managed subjects are handled by ~~HADOOP-9747~~. the shadedclient error doesn't seem related.

Could you consider rename ugiCanRelogin as something like shouldUseLoginUser()? Somehow the name ugiCanRelogin confused me. +1 after that.

Xiao Chen added a comment - 20/Jun/18 18:24 - edited

Thanks for the review and offline discussion weichiu! Actually my memory overflowed and we can use `UGI#shouldRelogin`.

HDFS-13682.03.patch uploaded

Wei-Chiu Chuang added a comment - 20/Jun/18 19:35

+1 pending Jenkins

genericqa added a comment - 20/Jun/18 22:24

☒ **-1 overall**

Vote	Subsystem	Runtime	Comment
0	reexec	0m 33s	Docker mode activated.
			Prechecks
+1	@author	0m 0s	The patch does not contain any @author tags.
+1	test4tests	0m 0s	The patch appears to include 1 new or modified test files.
			trunk Compile Tests
0	mvndep	1m 41s	Maven dependency ordering for branch
+1	mvninstall	27m 21s	trunk passed
+1	compile	29m 36s	trunk passed
+1	checkstyle	0m 23s	trunk passed
+1	mvnsite	2m 26s	trunk passed
+1	shadedclient	14m 14s	branch has no errors when building and testing our client artifacts.
+1	findbugs	3m 42s	trunk passed
+1	javadoc	1m 54s	trunk passed
			Patch Compile Tests
0	mvndep	0m 19s	Maven dependency ordering for patch

+1	mvninstall	1m 50s	the patch passed
+1	compile	28m 29s	the patch passed
+1	javac	28m 29s	the patch passed
+1	checkstyle	0m 24s	the patch passed
+1	mvnsite	2m 22s	the patch passed
+1	whitespace	0m 1s	The patch has no whitespace issues.
+1	shadedclient	11m 19s	patch has no errors when building and testing our client artifacts.
+1	findbugs	3m 57s	the patch passed
+1	javadoc	1m 54s	the patch passed
			Other Tests
+1	unit	9m 17s	hadoop-common in the patch passed.
-1	unit	97m 46s	hadoop-hdfs in the patch failed.
+1	asflicense	0m 45s	The patch does not generate ASF License warnings.
		239m 22s	

Reason	Tests
Failed junit tests	hadoop.hdfs.client.impl.TestBlockReaderLocal

Subsystem	Report/Notes
Docker	Client=17.05.0-ce Server=17.05.0-ce Image:yetus/hadoop:abb62dd
JIRA Issue	~~HDFS-13682~~
JIRA Patch URL	https://issues.apache.org/jira/secure/attachment/12928520/HDFS-13682.03.patch
Optional Tests	asflicense compile javac javadoc mvninstall mvnsite unit shadedclient findbugs checkstyle
uname	Linux 38b60da8f0c5 3.13.0-143-generic #192-Ubuntu SMP Tue Feb 27 10:45:36 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
Build tool	maven
Personality	/testptch/patchprocess/precommit/personality/provided.sh
git revision	trunk / 9a9e969
maven	version: Apache Maven 3.3.9
Default Java	1.8.0_171
findbugs	v3.1.0-RC1
unit	https://builds.apache.org/job/PreCommit-HDFS-Build/24481/artifact/out/patch-unit-hadoop-hdfs-project_hadoop-hdfs.txt
Test Results	https://builds.apache.org/job/PreCommit-HDFS-Build/24481/testReport/
Max. process+thread count	3126 (vs. ulimit of 10000)
modules	C: hadoop-common-project/hadoop-common hadoop-hdfs-project/hadoop-hdfs U: .
Console output	https://builds.apache.org/job/PreCommit-HDFS-Build/24481/console
Powered by	Apache Yetus 0.8.0-SNAPSHOT http://yetus.apache.org

This message was automatically generated.

Xiao Chen added a comment - 20/Jun/18 22:56

Thanks a lot Wei-Chiu!

Test failure is ~~HDFS-13662~~, unrelated to this patch. Committing.

Hudson added a comment - 20/Jun/18 23:31

SUCCESS: Integrated in Jenkins build Hadoop-trunk-Commit #14457 (See https://builds.apache.org/job/Hadoop-trunk-Commit/14457/)
~~HDFS-13682~~. Cannot create encryption zone after KMS auth token expires. (xiao: rev 32f867a6a907c05a312657139d295a92756d98ef)

- (edit) hadoop-hdfs-project/hadoop-hdfs/src/test/java/org/apache/hadoop/hdfs/TestSecureEncryptionZoneWithKMS.java
- (edit) hadoop-common-project/hadoop-common/src/main/java/org/apache/hadoop/security/UserGroupInformation.java
- (edit) hadoop-common-project/hadoop-common/src/main/java/org/apache/hadoop/crypto/key/kms/KMSClientProvider.java

Hudson added a comment - 24/Jun/18 08:04

FAILURE: Integrated in Jenkins build Hadoop-precommit-ozone-acceptance #20 (See https://builds.apache.org/job/Hadoop-precommit-ozone-acceptance/20/)
~~HDFS-13682~~. Cannot create encryption zone after KMS auth token expires. (xiao: https://github.com/apache/hadoop/commit/32f867a6a907c05a312657139d295a92756d98ef)

- (edit) hadoop-common-project/hadoop-common/src/main/java/org/apache/hadoop/security/UserGroupInformation.java
- (edit) hadoop-hdfs-project/hadoop-hdfs/src/test/java/org/apache/hadoop/hdfs/TestSecureEncryptionZoneWithKMS.java
- (edit) hadoop-common-project/hadoop-common/src/main/java/org/apache/hadoop/crypto/key/kms/KMSClientProvider.java

Nandakumar added a comment - 12/Dec/19 16:32

This change is breaking externally managed subjects.
Even if the `currentUGI` (which is managed externally) has access, we go ahead and return `UserGroupInformation.getLoginUser()` from `KMSClientProvider#getActualUgi`.
When the `LoginUser` doesn't have access, we get "`GSSException: No valid credentials provided`."

As UGI.shouldRelogin() depends on isHadoopLogin(), it will break externally managed subjects.

People

Assignee:

Xiao Chen

Reporter:

Xiao Chen

Votes:

0 Vote for this issue

Watchers:

6 Start watching this issue

Dates

Created:

14/Jun/18 22:31

Updated:

13/Dec/19 21:23

Resolved:

20/Jun/18 22:59