



# Move handshake secret field from Token to BlockAccessToken

Details

Type:	Sub-task	Status:	RESOLVED
Priority:	Blocker	Resolution:	Fixed
Affects Version/s:	None	Fix Version/s:	3.3.0
Component/s:	hdfs		
Labels:	None		

Description

Currently the handshake secret is included in Token, but conceptually this should belong to Block Access Token only. More importantly, having this field in Token could potentially break compatibility. Moreover, having this field as part of Block Access Token also means we may not need to encrypt this field anymore, because block access token is already encrypted.

Attachments

<a href="#">HDFS-14611.001.patch</a>	27 kB	26/Jun/19 19:02
<a href="#">HDFS-14611.002.patch</a>	29 kB	27/Jun/19 23:42
<a href="#">HDFS-14611.003.patch</a>	32 kB	08/Jul/19 21:58

Issue Links

is broken by

<a href="#">HDFS-13617</a> Allow wrapping NN QOP into token in encrypted message	RESOLVED
--	----------

Activity

[Hadoop QA](#) added a comment - 26/Jun/19 22:36

-1 overall

Vote	Subsystem	Runtime	Comment
0	reexec	0m 15s	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 15s	Maven dependency ordering for branch
+1	mvninstall	17m 28s	trunk passed
+1	compile	17m 41s	trunk passed
+1	checkstyle	2m 23s	trunk passed
+1	mvnsite	3m 14s	trunk passed
+1	shadedclient	17m 8s	branch has no errors when building and testing our client artifacts.
+1	findbugs	5m 37s	trunk passed
+1	javadoc	2m 32s	trunk passed
			Patch Compile Tests


0	mvndep	0m 23s	Maven dependency ordering for patch
+1	mvninstall	2m 35s	the patch passed
+1	compile	16m 58s	the patch passed
+1	cc	16m 58s	the patch passed
+1	javac	16m 58s	the patch passed
-0	checkstyle	2m 8s	root: The patch generated 13 new + 249 unchanged - 0 fixed = 262 total (was 249)
+1	mvnsite	3m 11s	the patch passed
+1	whitespace	0m 0s	The patch has no whitespace issues.
+1	shadedclient	10m 34s	patch has no errors when building and testing our client artifacts.
-1	findbugs	2m 19s	hadoop-hdfs-project/hadoop-hdfs generated 1 new + 0 unchanged - 0 fixed = 1 total (was 0)
+1	javadoc	2m 33s	the patch passed
Other Tests			
+1	unit	8m 39s	hadoop-common in the patch passed.
+1	unit	1m 59s	hadoop-hdfs-client in the patch passed.
-1	unit	84m 5s	hadoop-hdfs in the patch failed.
+1	asflicense	0m 57s	The patch does not generate ASF License warnings.
		205m 11s	

Reason	Tests
FindBugs	module:hadoop-hdfs-project/hadoop-hdfs
	Found reliance on default encoding in org.apache.hadoop.hdfs.protocol.datatransfer.sasl.SaslDataTransferServer.doSaslHandshake(Peer, OutputStream, InputStream, Map, CallbackHandler):in org.apache.hadoop.hdfs.protocol.datatransfer.sasl.SaslDataTransferServer.doSaslHandshake(Peer, OutputStream, InputStream, Map, CallbackHandler): new String(byte[]) At SaslDataTransferServer.java:[line 387]
Failed junit tests	hadoop.hdfs.protocol.datatransfer.sasl.TestSaslDataTransfer
	hadoop.hdfs.web.TestWebHdfsTimeouts
	hadoop.hdfs.server.diskbalancer.TestDiskBalancer
	hadoop.hdfs.server.balancer.TestBalancerWithMultipleNameNodes
	hadoop.hdfs.server.datanode.TestDirectoryScanner

Subsystem	Report/Notes
Docker	Client=17.05.0-ce Server=17.05.0-ce Image:yetus/hadoop:bdbca0e
JIRA Issue	<a href="#">HDFS-14611</a>
JIRA Patch URL	<a href="https://issues.apache.org/jira/secure/attachment/12972997/HDFS-14611.001.patch">https://issues.apache.org/jira/secure/attachment/12972997/HDFS-14611.001.patch</a>
Optional Tests	dupname asflicense compile javac javadoc mvninstall mvnsite unit shadedclient findbugs checkstyle cc
uname	Linux b9d511fff440 4.4.0-139-generic #165-Ubuntu SMP Wed Oct 24 10:58:50 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
Build tool	maven
Personality	/testptch/patchprocess/precommit/personality/provided.sh
git revision	trunk / 0a37ccf
maven	version: Apache Maven 3.3.9
Default Java	1.8.0_212
findbugs	v3.1.0-RC1
checkstyle	<a href="https://builds.apache.org/job/PreCommit-HDFS-Build/27091/artifact/out/diff-checkstyle-root.txt">https://builds.apache.org/job/PreCommit-HDFS-Build/27091/artifact/out/diff-checkstyle-root.txt</a>


findbugs	<a href="https://builds.apache.org/job/PreCommit-HDFS-Build/27091/artifact/out/new-findbugs-hadoop-hdfs-project_hadoop-hdfs.html">https://builds.apache.org/job/PreCommit-HDFS-Build/27091/artifact/out/new-findbugs-hadoop-hdfs-project_hadoop-hdfs.html</a>
unit	<a href="https://builds.apache.org/job/PreCommit-HDFS-Build/27091/artifact/out/patch-unit-hadoop-hdfs-project_hadoop-hdfs.txt">https://builds.apache.org/job/PreCommit-HDFS-Build/27091/artifact/out/patch-unit-hadoop-hdfs-project_hadoop-hdfs.txt</a>
Test Results	<a href="https://builds.apache.org/job/PreCommit-HDFS-Build/27091/testReport/">https://builds.apache.org/job/PreCommit-HDFS-Build/27091/testReport/</a>
Max. process+thread count	5275 (vs. ulimit of 10000)
modules	C: hadoop-common-project/hadoop-common hadoop-hdfs-project/hadoop-hdfs-client hadoop-hdfs-project/hadoop-hdfs U: .
Console output	<a href="https://builds.apache.org/job/PreCommit-HDFS-Build/27091/console">https://builds.apache.org/job/PreCommit-HDFS-Build/27091/console</a>
Powered by	Apache Yetus 0.8.0 <a href="http://yetus.apache.org">http://yetus.apache.org</a>

This message was automatically generated.

▼  Erik Krogen added a comment - 27/Jun/19 16:04

Hi [vagarychen](#), I haven't yet taken a look at the patch, but can you start by explaining why putting the secret in `Token` is incompatible, whereas putting it within the `Block Access Token` is a compatible change?

Also, if this truly was an incompatible change to the token, this needs to be marked as a blocker for any release which includes [HDFS-13617](#).

▼  Chen Liang added a comment - 27/Jun/19 16:54


[xkrogen](#) this is a bit complicated, as explained below.

The way this could break compatibility that, in `Credentials#readFields`, the entire input stream may contain several tokens, aligned as consecutive raw bytes. And this code is not aware of the size on individual tokens, but rely on `t.readFields(in)`; to read just the right number of bytes and do the right thing. The current code adds a new field to `Token` which extends the bytes of individual token (in `Token#write` and `Token#readFields`). So if client and server run different versions, one may be sending token with extended bytes, one may not be expecting these bytes, the side that's not expecting these bytes will not read these bytes from the input in `Token#readFields`, causing subsequent read from the stream to get misaligned.


The root cause is basically that, again, this code is not aware of total number bytes it should take to construct one `Token`. But the logic is aware of the total size of underlying identifier field so putting this field in as part of identifier does not have this issue, this is why it can get resolved. Essentially, the new bytes get put into `Token#identifier`, as part of the identifier itself. When `Token#readFields` gets called, it does first read the length of the entire identifier, and create a new array (this is important) to read these bytes, and parse the identifier on those bytes. Because this part does correctly retrieve the whole identifier (which has the new bytes included), the rest of the stream stays aligned as expected.

In this case, if an old binary receives a new token identifier, it can still decode all the fields, except that the new bytes are not read, as it does not have this logic. If a new binary receives a old token, it will get a EOF at the end of parsing the identifier (the EOF in the patch `BlockTokenIdentifier`), but this is fine as all the preceding fields are parsed, and this does not affect the stream because identifier byte array is created from original stream. But either way, it is fine, in the sense that the identifier gets recreated as expected, and the rest of the stream is not affected.


Marked as blocker as suggested.

▼  Erik Krogen added a comment - 27/Jun/19 17:16

Makes sense, thank you for the detailed explanation!

▼  Chen Liang added a comment - 27/Jun/19 23:43

The failed test `TestSaslDataTransfer` is related, fix in v002 patch, also address the findbug warning.

▼  Hadoop QA added a comment - 28/Jun/19 03:14

 -1 overall

Vote	Subsystem	Runtime	Comment
------	-----------	---------	---------

0	reexec	0m 17s	Docker mode activated.
			<b>Prechecks</b>
+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.
			<b>trunk Compile Tests</b>
0	mvndep	7m 50s	Maven dependency ordering for branch
+1	mvninstall	17m 6s	trunk passed
+1	compile	16m 9s	trunk passed
+1	checkstyle	2m 16s	trunk passed
+1	mvnsite	3m 23s	trunk passed
+1	shadedclient	16m 37s	branch has no errors when building and testing our client artifacts.
+1	findbugs	5m 40s	trunk passed
+1	javadoc	2m 21s	trunk passed
			<b>Patch Compile Tests</b>
0	mvndep	0m 25s	Maven dependency ordering for patch
+1	mvninstall	2m 17s	the patch passed
+1	compile	15m 42s	the patch passed
+1	cc	15m 42s	the patch passed
+1	javac	15m 42s	the patch passed
-0	checkstyle	2m 4s	root: The patch generated 15 new + 249 unchanged - 0 fixed = 264 total (was 249)
+1	mvnsite	3m 4s	the patch passed
+1	whitespace	0m 0s	The patch has no whitespace issues.
+1	shadedclient	10m 22s	patch has no errors when building and testing our client artifacts.
+1	findbugs	6m 4s	the patch passed
+1	javadoc	2m 22s	the patch passed
			<b>Other Tests</b>
+1	unit	8m 42s	hadoop-common in the patch passed.
+1	unit	2m 0s	hadoop-hdfs-client in the patch passed.
-1	unit	80m 32s	hadoop-hdfs in the patch failed.
+1	asflicense	0m 54s	The patch does not generate ASF License warnings.
		203m 26s	

Reason	Tests
Failed junit tests	hadoop.hdfs.web.TestWebHdfsTimeouts
	hadoop.hdfs.server.datanode.TestDirectoryScanner

Subsystem	Report/Notes
Docker	Client=17.05.0-ce Server=17.05.0-ce Image:yetus/hadoop:bdbca0e
JIRA Issue	<a href="#">HDFS-14611</a>
JIRA Patch URL	<a href="https://issues.apache.org/jira/secure/attachment/12973127/HDFS-14611.002.patch">https://issues.apache.org/jira/secure/attachment/12973127/HDFS-14611.002.patch</a>
Optional Tests	dupname asflicense compile javac javadoc mvninstall mvnsite unit shadedclient findbugs checkstyle cc
uname	Linux ee757e0d4c47 4.4.0-139-generic #165-Ubuntu SMP Wed Oct 24 10:58:50 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
Build tool	maven
Personality	/testptch/patchprocess/precommit/personality/provided.sh


git revision	trunk / 4a21224
maven	version: Apache Maven 3.3.9
Default Java	1.8.0_212
findbugs	v3.1.0-RC1
checkstyle	<a href="https://builds.apache.org/job/PreCommit-HDFS-Build/27100/artifact/out/diff-checkstyle-root.txt">https://builds.apache.org/job/PreCommit-HDFS-Build/27100/artifact/out/diff-checkstyle-root.txt</a>
unit	<a href="https://builds.apache.org/job/PreCommit-HDFS-Build/27100/artifact/out/patch-unit-hadoop-hdfs-project_hadoop-hdfs.txt">https://builds.apache.org/job/PreCommit-HDFS-Build/27100/artifact/out/patch-unit-hadoop-hdfs-project_hadoop-hdfs.txt</a>
Test Results	<a href="https://builds.apache.org/job/PreCommit-HDFS-Build/27100/testReport/">https://builds.apache.org/job/PreCommit-HDFS-Build/27100/testReport/</a>
Max. process+thread count	4746 (vs. ulimit of 10000)
modules	C: hadoop-common-project/hadoop-common hadoop-hdfs-project/hadoop-hdfs-client hadoop-hdfs-project/hadoop-hdfs U: .
Console output	<a href="https://builds.apache.org/job/PreCommit-HDFS-Build/27100/console">https://builds.apache.org/job/PreCommit-HDFS-Build/27100/console</a>
Powered by	Apache Yetus 0.8.0 <a href="http://yetus.apache.org">http://yetus.apache.org</a>

This message was automatically generated.


▼  [Konstantin Shvachko](#) added a comment - 28/Jun/19 23:02

Looks reasonable overall, simpler than the previous approach, and preserves compatibility, which is the key point. Minor comments:


- 1. `SaslDataTransferServer` - some unused imports still need to be reverted
- 2. `public byte[] createPassword(BlockTokenIdentifier identifier)` - may not need to be public
- 3. Update JavaDoc for the new parameter in constructor `BlockTokenSecretManager()`
- 4. Also check the checkstyle warnings.

▼  [Chen Liang](#) added a comment - 08/Jul/19 21:58

Thanks for the review [shv](#), post v003 patch.

▼  [Konstantin Shvachko](#) added a comment - 08/Jul/19 23:19

+1 on my side for v3 patch.

▼  [Hadoop QA](#) added a comment - 09/Jul/19 02:20

 **-1 overall**

Vote	Subsystem	Runtime	Comment
0	reexec	0m 41s	<a href="#">Docker mode activated.</a>
			<b>Prechecks</b>
+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.
			<b>trunk Compile Tests</b>
0	mvndep	1m 11s	<a href="#">Maven dependency ordering for branch</a>
+1	mvninstall	18m 44s	trunk passed
+1	compile	19m 0s	trunk passed
+1	checkstyle	2m 15s	trunk passed
+1	mvnsite	3m 30s	trunk passed
+1	shadedclient	17m 35s	branch has no errors when building and testing our client artifacts.
+1	findbugs	5m 49s	trunk passed
+1	javadoc	2m 41s	trunk passed
			<b>Patch Compile Tests</b>


0	mvndep	0m 24s	Maven dependency ordering for patch
+1	mvninstall	2m 30s	the patch passed
+1	compile	18m 12s	the patch passed
+1	cc	18m 12s	the patch passed
+1	javac	18m 12s	the patch passed
-0	checkstyle	2m 15s	root: The patch generated 1 new + 250 unchanged - 0 fixed = 251 total (was 250)
+1	mvnsite	3m 23s	the patch passed
+1	whitespace	0m 0s	The patch has no whitespace issues.
+1	shadedclient	10m 43s	patch has no errors when building and testing our client artifacts.
+1	findbugs	6m 12s	the patch passed
+1	javadoc	2m 33s	the patch passed
Other Tests			
+1	unit	8m 29s	hadoop-common in the patch passed.
+1	unit	1m 58s	hadoop-hdfs-client in the patch passed.
-1	unit	116m 48s	hadoop-hdfs in the patch failed.
+1	asflicense	0m 42s	The patch does not generate ASF License warnings.
		242m 54s	

Reason	Tests
Failed junit tests	hadoop.hdfs.server.namenode.TestFSImage
	hadoop.hdfs.server.datanode.TestDirectoryScanner
	hadoop.hdfs.web.TestWebHdfsTimeouts


Subsystem	Report/Notes
Docker	Client=17.05.0-ce Server=17.05.0-ce Image:yetus/hadoop:bdbca0e
JIRA Issue	<a href="#">HDFS-14611</a>
JIRA Patch URL	<a href="https://issues.apache.org/jira/secure/attachment/12973983/HDFS-14611.003.patch">https://issues.apache.org/jira/secure/attachment/12973983/HDFS-14611.003.patch</a>
Optional Tests	dupname asflicense compile javac javadoc mvninstall mvnsite unit shadedclient findbugs checkstyle cc
uname	Linux 5c3f90eb4f78 4.4.0-138-generic #164-Ubuntu SMP Tue Oct 2 17:16:02 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
Build tool	maven
Personality	/testptch/patchprocess/precommit/personality/provided.sh
git revision	trunk / 4632708
maven	version: Apache Maven 3.3.9
Default Java	1.8.0_212
findbugs	v3.1.0-RC1
checkstyle	<a href="https://builds.apache.org/job/PreCommit-HDFS-Build/27172/artifact/out/diff-checkstyle-root.txt">https://builds.apache.org/job/PreCommit-HDFS-Build/27172/artifact/out/diff-checkstyle-root.txt</a>
unit	<a href="https://builds.apache.org/job/PreCommit-HDFS-Build/27172/artifact/out/patch-unit-hadoop-hdfs-project_hadoop-hdfs.txt">https://builds.apache.org/job/PreCommit-HDFS-Build/27172/artifact/out/patch-unit-hadoop-hdfs-project_hadoop-hdfs.txt</a>
Test Results	<a href="https://builds.apache.org/job/PreCommit-HDFS-Build/27172/testReport/">https://builds.apache.org/job/PreCommit-HDFS-Build/27172/testReport/</a>
Max. process+thread count	3501 (vs. ulimit of 10000)
modules	C: hadoop-common-project/hadoop-common hadoop-hdfs-project/hadoop-hdfs-client hadoop-hdfs-project/hadoop-hdfs U: .
Console output	<a href="https://builds.apache.org/job/PreCommit-HDFS-Build/27172/console">https://builds.apache.org/job/PreCommit-HDFS-Build/27172/console</a>

Powered by	Apache Yetus 0.8.0 <a href="http://yetus.apache.org">http://yetus.apache.org</a>
------------	--

This message was automatically generated.

▼  **Chen Liang** added a comment - 11/Jul/19 20:25

The failed tests are unrelated. I've committed v003 patch to trunk, thanks [shv](#) for the review!

▼  **Hudson** added a comment - 11/Jul/19 20:27


FAILURE: Integrated in Jenkins build Hadoop-trunk-Commit #16894 (See <https://builds.apache.org/job/Hadoop-trunk-Commit/16894/>)

[HDFS-14611](#). Move handshake secret field from Token to BlockAccessToken. (cliang: rev 8fb5ca3f405550828a17e689b9c60ddf7fb95ec1)

- (edit) hadoop-hdfs-project/hadoop-hdfs-client/src/main/java/org/apache/hadoop/hdfs/protocolPB/PBHelperClient.java
- (edit) hadoop-hdfs-project/hadoop-hdfs/src/main/java/org/apache/hadoop/hdfs/server/namenode/NameNodeRpcServer.java
- (edit) hadoop-common-project/hadoop-common/src/main/proto/Security.proto
- (edit) hadoop-hdfs-project/hadoop-hdfs/src/main/java/org/apache/hadoop/hdfs/security/token/block/BlockTokenSecretManager.java
- (edit) hadoop-common-project/hadoop-common/src/main/java/org/apache/hadoop/security/token/Token.java
- (edit) hadoop-hdfs-project/hadoop-hdfs/src/test/java/org/apache/hadoop/hdfs/TestBlockTokenWrappingQOP.java
- (edit) hadoop-hdfs-project/hadoop-hdfs/src/main/java/org/apache/hadoop/hdfs/protocol/datantransfer/sasl/SaslDataTransferServer.java
- (edit) hadoop-hdfs-project/hadoop-hdfs/src/main/java/org/apache/hadoop/hdfs/server/blockmanagement/BlockManager.java
- (edit) hadoop-hdfs-project/hadoop-hdfs-client/src/main/java/org/apache/hadoop/hdfs/security/token/block/BlockTokenIdentifier.java
- (edit) hadoop-hdfs-project/hadoop-hdfs-client/src/main/java/org/apache/hadoop/hdfs/protocol/datantransfer/sasl/SaslDataTransferClient.java
- (edit) hadoop-hdfs-project/hadoop-hdfs-client/src/main/proto/hdfs.proto

#### ▼ People

Assignee:

 **Chen Liang**

Reporter:

 **Chen Liang**

Votes:

 0 Vote for this issue

Watchers:

 7 Start watching this issue

#### ▼ Dates

Created:

26/Jun/19 18:59

Updated:

11/Jul/19 20:27

Resolved:

11/Jul/19 20:26