

## rgw - Bug #11367

### Keystone PKI token expiration is not enforced

04/10/2015 11:28 AM - Anton Aksola

<b>Status:</b> Resolved	<b>Start date:</b> 04/10/2015
<b>Priority:</b> High	<b>Due date:</b>
<b>Assignee:</b> Loic Dachary	<b>% Done:</b> 0%
<b>Category:</b>	<b>Estimated time:</b> 0.00 hour
<b>Target version:</b>	<b>Spent time:</b> 0.00 hour
<b>Source:</b> other	<b>Reviewed:</b>
<b>Tags:</b>	<b>Affected Versions:</b>
<b>Backport:</b> hammer, firefly	<b>ceph-qa-suite:</b>
<b>Regression:</b> No	<b>Pull request ID:</b>
<b>Severity:</b> 2 - major	
<b>Description</b>	
Our customer reported that their tokens do not seem to expire.	
It seems that there is no expiration check after decoding a PKI token. While there is an expiration check in the token cache class it has no effect when dealing with PKI tokens.	
I have made a small patch against firefly and it seems to correct the issue in our environment: <a href="https://github.com/aakso/ceph/tree/wip-rgw-pki-token-expire-firefly">https://github.com/aakso/ceph/tree/wip-rgw-pki-token-expire-firefly</a>	
<b>Related issues:</b>	
Copied to rgw - Backport #11721: Keystone PKI token expiration is not enforced	<b>Resolved</b> <b>04/10/2015</b>
Copied to rgw - Backport #11722: Keystone PKI token expiration is not enforced	<b>Resolved</b> <b>04/10/2015</b>

#### Associated revisions

##### Revision 2df06939 - 05/08/2015 08:50 AM - Anton Aksola

rgw: always check if token is expired

Fixes: #11367

Currently token expiration is only checked by the token cache. With PKI tokens no expiration check is done after decoding the token. This causes PKI tokens to be valid indefinitely. UUID tokens are validated by keystone after cache miss so they are not affected by this bug.

This commit adds explicit token expiration check to  
RGWSwift::validate\_keystone\_token()

Signed-off-by: Anton Aksola <[anton.aksola@nebula.fi](mailto:anton.aksola@nebula.fi)>

Reported-by: Riku Lehto <[riku.lehto@nexetic.com](mailto:riku.lehto@nexetic.com)>

##### Revision d4ef5566 - 05/26/2015 01:26 PM - Anton Aksola

rgw: always check if token is expired

Fixes: #11367

Currently token expiration is only checked by the token cache. With PKI tokens no expiration check is done after decoding the token. This causes PKI tokens to be valid indefinitely. UUID tokens are validated by keystone after cache miss so they are not affected by this bug.

This commit adds explicit token expiration check to  
RGWSwift::validate\_keystone\_token()

Signed-off-by: Anton Aksola <[anton.aksola@nebula.fi](mailto:anton.aksola@nebula.fi)>

Reported-by: Riku Lehto <[riku.lehto@nexetic.com](mailto:riku.lehto@nexetic.com)>

(cherry picked from commit 2df069390ea3bbcfbab5022750e89f51d197cc11)

#### Revision 9dfef600 - 06/07/2015 06:54 AM - Anton Aksola

rgw: always check if token is expired

Fixes: #11367

Currently token expiration is only checked by the token cache. With PKI tokens no expiration check is done after decoding the token. This causes PKI tokens to be valid indefinitely. UUID tokens are validated by keystone after cache miss so they are not affected by this bug.

This commit adds explicit token expiration check to  
RGWSwift::validate\_keystone\_token()

Signed-off-by: Anton Aksola <[anton.aksola@nebula.fi](mailto:anton.aksola@nebula.fi)>

Reported-by: Riku Lehto <[riku.lehto@nexetic.com](mailto:riku.lehto@nexetic.com)>

(cherry picked from commit 2df069390ea3bbcfbab5022750e89f51d197cc11)

## History

---

### #1 - 04/21/2015 05:50 PM - Yehuda Sadeh

The fix looks correct. Can you send a pull request against the ceph upstream repository, and add a Signed-off-by tag to the commit?

### #2 - 04/22/2015 07:47 AM - Loic Dachary

- Status changed from New to Pending Backport

- Backport set to firefly

### #3 - 04/22/2015 08:36 AM - Anton Aksola

- correct patch bug against the wrong branch, needs to be on master <https://github.com/ceph/ceph/pull/4429>

**#4 - 05/07/2015 11:53 AM - Loic Dachary**

- Status changed from *Pending Backport* to *In Progress*
- Regression set to *No*

**#5 - 05/07/2015 12:37 PM - Anton Aksola**

I tested the patch against master snapshot in our QA and it seems to work. Going to resubmit a merge request soon.

**#6 - 05/08/2015 08:59 AM - Anton Aksola**

New pull request: <https://github.com/ceph/ceph/pull/4617>

**#7 - 05/21/2015 09:08 PM - Yehuda Sadeh**

- Backport changed from *firefly* to *hammer*, *firefly*

**#8 - 05/21/2015 09:09 PM - Yehuda Sadeh**

- Status changed from *In Progress* to *Pending Backport*

**#9 - 06/30/2015 06:12 PM - Yehuda Sadeh**

- Assignee set to *Loic Dachary*

**#10 - 08/11/2015 06:28 PM - Yehuda Sadeh**

- Status changed from *Pending Backport* to *Resolved*