TYPO3.Flow - Task # 46352

Status:	Resolved	**Priority:**	Should have
Author:	Christian Müller	**Category:**	Security
Created:	2013-03-16	**Assigned To:**	Christian Müller
Updated:	2013-04-29	**Due date:**	
Sprint:			
PHP Version:			
Has patch:	No		
Complexity:			
Subject:	Roles in SecurityContext should be kept until tokens change		

Description

GetRoles inside SecurityContext rebuilds the array of roles on every call which is costly and leads to a lots of created objects if roles (for example in fluid) are used a lot.

As for the building only two things are responsible, a) all available roles and b) tokens we can for now safely keep the roles until tokens change.

As soon as roles are objects that could be modified during runtime you might need to clear the array if you change the existing roles.

Associated revisions

Revision 5241493c - 2013-03-18 08:59 - Christian Müller

[TASK] Keep roles until tokens get updated

Resolves: #46352
Releases: master, 2.0
Change-Id: Id256b168ff9c6aa4cac8da8957ada237f9236c71

Revision 9f6ff081 - 2013-03-27 12:05 - Christian Müller

[TASK] Keep roles until tokens get updated

Resolves: #46352
Releases: master, 2.0
Change-Id: Id256b168ff9c6aa4cac8da8957ada237f9236c71

Revision 750ad089 - 2013-04-05 11:38 - Christian Müller

[TASK] Keep roles until tokens get updated

Resolves: #46352
Releases: master, 2.0
Change-Id: Id256b168ff9c6aa4cac8da8957ada237f9236c71

Revision e06e0f2d - 2013-05-07 17:42 - Bastian Waidelich

[BUGFIX] Authentication does not work any longer without redirects

This fixes a regression that made the authenticated roles only available
in the security context after a redirect following authentication.

Background:

This is a regression introduced with the 1st level cache added in
Id256b168ff9c6aa4cac8da8957ada237f9236c71 but the actual problem is
that the PersistenceQueryRewritingAspect initializes the security
context if it was not initialized before (since change
I44838de1503cbe49cf3fee51921b731bfaa0cfc5) when intercepting QOM
queries setting the context roles to "Anonymous" and "Everybody".

This change adds a new method Context::withoutAuthorizationChecks()
that allows you temporarily disable authorization related interceptors
e.g. PolicyEnforcement and PersistenceQueryRewriting aspects in order
to be able to circumvent authorization in low level operations (for
example to fetch the current account in an AuthenticationProvider).

Usage::

```
$this->securityContext->withoutAuthorizationChecks(
  function ($accountRepository, $username, $providerName, &$account) {
    // this will disable the PersistenceQueryRewritingAspect for this one call
    $account = $accountRepository
      ->findActiveByAccountIdentifierAndAuthenticationProviderName($username, $providerName)
  }
);
```

Change-Id: Ib31cd6bcf10504670439d4c700dda0b14e512d80
Related: #46352
Fixes: #46636
Releases: master, 2.0

Revision b964e06b - 2013-05-07 17:46 - Bastian Waidelich

[BUGFIX] Authentication does not work any longer without redirects

This fixes a regression that made the authenticated roles only available
in the security context after a redirect following authentication.

Background:

This is a regression introduced with the 1st level cache added in
Id256b168ff9c6aa4cac8da8957ada237f9236c71 but the actual problem is
that the PersistenceQueryRewritingAspect initializes the security
context if it was not initialized before (since change
I44838de1503cbe49cf3fee51921b731bfaa0cfc5) when intercepting QOM
queries setting the context roles to "Anonymous" and "Everybody".

This change adds a new method Context::withoutAuthorizationChecks()
that allows you temporarily disable authorization related interceptors

e.g. PolicyEnforcement and PersistenceQueryRewriting aspects in order
to be able to circumvent authorization in low level operations (for
example to fetch the current account in an AuthenticationProvider).

Usage::

```
$this->securityContext->withoutAuthorizationChecks(
  function ($accountRepository, $username, $providerName, &$account) {
    // this will disable the PersistenceQueryRewritingAspect for this one call
    $account = $accountRepository
      ->findActiveByAccountIdentifierAndAuthenticationProviderName($username, $providerName)
  }
);
```

Change-Id: Ib31cd6bcf10504670439d4c700dda0b14e512d80
Related: #46352
Fixes: #46636
Releases: master, 2.0

History

#1 - 2013-03-16 12:59 - Gerrit Code Review

- Status changed from Accepted to Under Review

Patch set 1 for branch **master** has been pushed to the review server.
It is available at https://review.typo3.org/18968

#2 - 2013-03-18 08:59 - Gerrit Code Review

Patch set 2 for branch **master** has been pushed to the review server.
It is available at https://review.typo3.org/18968

#3 - 2013-03-18 14:37 - Christian Müller

- Status changed from Under Review to Resolved
- % Done changed from 0 to 100

Applied in changeset commit:5241493c41d0829cb67066e1bfc0cf9d7b1ef8bc.

#4 - 2013-03-20 17:46 - Gerrit Code Review

- Status changed from Resolved to Under Review

Patch set 1 for branch **2.0** has been pushed to the review server.
It is available at https://review.typo3.org/19110

#5 - 2013-03-21 15:31 - Marco Falkenberg

After applying the patch authentication via HTTP-Basic (PersistedUsernamePasswordProvider & UsernamePasswordHttpBasic-Token) throws

#1222268609: Access denied (0 denied, 0 granted, 1 abstained)

#6 - 2013-03-27 12:08 - Gerrit Code Review

Patch set 1 for branch **composer** has been pushed to the review server.
It is available at https://review.typo3.org/19368

#7 - 2013-03-27 13:37 - Christian Müller

- Status changed from Under Review to Resolved

Applied in changeset commit:9f6ff0818cc8ace51fee4c3ab5ae2eeecd6fd59e.

#8 - 2013-04-05 11:38 - Gerrit Code Review

- Status changed from Resolved to Under Review

Patch set 2 for branch **2.0** has been pushed to the review server.
It is available at https://review.typo3.org/19110

#9 - 2013-04-05 12:37 - Christian Müller

- Status changed from Under Review to Resolved

Applied in changeset commit:750ad089bc8f8b26f362bb2e340fb3738b373076.