TYPO3.Flow - Bug # 6761

Status:	Resolved	**Priority:**	Must have
Author:	Karsten Dambekalns	**Category:**	Security
Created:	2010-03-10	**Assigned To:**	Karsten Dambekalns
Updated:	2010-10-20	**Due date:**	
PHP Version:			
Has patch:			
Complexity:			
Affected Flow version:			
Subject:	Security context in session grows with each load		

Description

Since the latest changes to security it seems something goes wrong with object serialization to the session. It grows exponentially with each page load until the memory limit is hit.

Reproducible by logging in and calling the same page again and again... Even failing login tries have that effect.

Associated revisions

Revision 6fa5c967 - 2010-03-11 16:32 - Robert Lemke

[+BUGFIX] FLOW3 (Object): Removed the obsolete SessionRegistry which was causing trouble resulting in a drastically growing session file. Fixes #6761
[+BUGFIX] FLOW3 (Security): Fixed a bug which resulted in a non working Account Repository. Fixes #6787

Revision b236c247 - 2010-03-15 13:10 - Karsten Dambekalns

[+BUGFIX] FLOW3 (Security): Fixed the token duplication in the security context, fixes #6761.

History

#1 - 2010-03-10 13:35 - Karsten Dambekalns

The effect continues even after logging out again.

#2 - 2010-03-10 13:57 - Karsten Dambekalns

Ok, it seems the session grows also when not logging in or trying to do so. Only it grows at a much lower speed, in kb rather than mb. So maybe the ObjectSerializer is the problem in general.

#3 - 2010-03-10 14:00 - Karsten Dambekalns

- File sess_j6je3itierlcpkhic6hkgle600.first.txt added

- File sess_j6je3itierlcpkhic6hkgle600.second.txt added

Attached two session files. The file doubles it's size on every page load.

#4 - 2010-03-11 10:36 - Robert Lemke

- Estimated time set to 10.00

#5 - 2010-03-11 15:21 - Robert Lemke

- Assigned To changed from Andreas Förthner to Robert Lemke

- Start date changed from 2010-03-10 to 2010-03-11

#6 - 2010-03-11 16:29 - Robert Lemke

- Estimated time changed from 10.00 to 2.00

#7 - 2010-03-11 17:00 - Robert Lemke

- Status changed from Accepted to Resolved

- % Done changed from 0 to 100

Applied in changeset r3929.

#8 - 2010-03-11 17:09 - Robert Lemke

- Status changed from Resolved to Accepted

- % Done changed from 100 to 50

- Estimated time changed from 2.00 to 4.00

Seems like I didn't fix this completely

#9 - 2010-03-15 13:03 - Karsten Dambekalns

- Assigned To changed from Robert Lemke to Karsten Dambekalns

- % Done changed from 50 to 90

The problem is caused by seperateActiveAndInactiveTokens() in combination with the way initialize() sets $this->activeTokens.

1. call
   initialize
      tokens 0
      activeTokens 1
      inactiveTokens 0
   shutdownObject
      tokens 1
      activeTokens 1
      inactiveTokens 0

2. call
   initialize
      tokens 1
      activeTokens 1
      inactiveTokens 0
   seperateActiveAndInactiveTokens
      tokens 1
      activeTokens 2 (!)
      inactiveTokens 0

shutdownObject
tokens 2
activeTokens 2
inactiveTokens 0

3. call
initialize
tokens 2
activeTokens 2
inactiveTokens 0
seperateActiveAndInactiveTokens
tokens 2
activeTokens 4 (!)
inactiveTokens 0
shutdownObject
tokens 4
activeTokens 4
inactiveTokens 0

#10 - 2010-03-15 14:00 - Karsten Dambekalns

- Status changed from Accepted to Resolved

- % Done changed from 90 to 100

Applied in changeset r3939.

#11 - 2010-10-14 13:43 - Bastian Waidelich

- Status changed from Resolved to Accepted

- Assigned To changed from Karsten Dambekalns to Bastian Waidelich

- Target version deleted (1.0 alpha 8)

It seems this issue reoccurs in the current version.. I'll dig into it

#12 - 2010-10-14 17:18 - Bastian Waidelich

- Status changed from Accepted to Resolved

- Assigned To changed from Bastian Waidelich to Karsten Dambekalns

Bastian Waidelich wrote:

> *It seems this issue reoccurs in the current version.. I'll dig into it*

Apparently the issue occurred because I had configured multiple authentication providers - so it might be just a misconfiguration. I'll check that and reopen the issue in case it is not.

Files

sess_j6je3itierlcpkhic6hkgle600.first.txt	63.7 kB	2010-03-10	Karsten Dambekalns
sess_j6je3itierlcpkhic6hkgle600.second.txt	127.1 kB	2010-03-10	Karsten Dambekalns