

Kepler - Bug #3071

KAR files should be sent along with workflow to slaves

01/16/2008 02:55 PM - Chad Berkley

Status:	Resolved	Start date:	01/16/2008
Priority:	Normal	Due date:	
Assignee:	jianwu jianwu	% Done:	0%
Category:	distributed execution	Estimated time:	0.00 hour
Target version:	2.X.Y	Spent time:	0.00 hour
Bugzilla-Id:	3071		
<b>Description</b> When a master sends the workflow out to the slaves, it should also send any kar files that are needed for execution of the workflow. This comes with security risks since you are allowing arbitrary code to execute on the slave. The workflow itself is arbitrary code, especially since the workflow can use the command line actor to execute system commands. This needs to be looked into and the security policies need to be adjusted accordingly.			

History

#1 - 01/16/2008 02:56 PM - Chad Berkley

kar files should be signed so that the recipient at least can know that they are coming from who they should be.

#2 - 03/29/2010 12:43 PM - jianwu jianwu

In the new KAR specification of the coming Kepler 2.0, KAR files can not include actor classes and jars. So parsing KAR files won't enable slave execute them if the actors are not in the suite of slave.

The current assumption of master-slave execution is that all actors in DistributedCompositeActor should also in the slave sides. Usually master and slave need to be in the same suite.

Using module mechanism of Kepler 2.0, published modules could be dynamically gotten by slave. Yet it is heavy requirement that the modules have to be published.

The current decision is to postpone this bug and ask master and slave nodes have the same suite (including master-slave module) before using DistributedCompositeActor.

#3 - 03/27/2013 02:22 PM - Redmine Admin

Original Bugzilla ID was 3071