Metacat - Bug #6994

Bad call to MNStorage.update() via REST API can result in bad state and StackOverflowErrors

03/23/2016 01:27 PM - Bryce Mecum

Status:	New	**Start date:**	03/23/2016
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:		**Spent time:**	0.00 hour
Bugzilla-Id:			

Description

This all happened on arcticdata.io production over the last couple of days.

I was attempting to update an object and forgot the {PID} part of the REST API URL: PUT /object/{pid}. This resulted in unexpected behavior and an unexpected state.

- The request returned a ServiceError (HTTP Status 500) of "StackOverflowError", this was unexpected.
- The sysmeta for the PID I was updating changed: The PID became obsoleted and obseletedBy the new PID I chose. This was expected.
- Calls to /meta and /object for the new PID failed, this was unexpected.

It appears that the new PID was reserved but never assigned sysmeta or object bytes, resulting in an unexpected system state.

I then set about a path of archiving the PID by first removing public read access, which resulted in another StackOverflowError but public read access was revoked as expected. In the end, I had Chris Jones do an administrative delete on the object.

I see two things here:

1. The requests returned StackOverflowErrors. It seems like a stack overflow shouldn't be possible. The requests returning this error took ~10+ seconds to return which would imply this is a great attack vector.
2. An invalid REST API call was not rejected immediately (the call where I was missing the {PID} part of the URL