SBM fails to start after updating the kernel to patch the StackGuard Vulnerability

SBM fails to start after updating the kernel to patch the StackGuard Vulnerability

Symptom

The SBM fails to start. Log entries show the service stopping, but does not show a reason why.

```
Example monitor.log output:
STATUS | monitor  | 2017/06/21 09:00:00 | Launching a Service...
ERROR  | monitor  | 2017/06/21 09:00:00 | Service exited while loading the application.
STATUS | monitor  | 2017/06/21 09:00:00 | Service Restarts disabled.  Shutting down.
STATUS | monitor  | 2017/06/21 09:00:00 | <-- Monitor Stopped
```

Cause

Kernel-side fixes to resolve the StackGuard vulnerability, included a change to increase the stack guard gap size from one page to 1 MiB. On an SBM, this caused Java to fail to allocate memory from the same (already allocated) space, and segfault as a result.

Resolution

Our workaround is to increase the stack size to 2048k, to allow Java to allocate the appropriate amount of memory to operate the SBM.

```
-Open our server.conf file using your preferred text editor:
/usr/sbin/r1soft/conf/server.conf

-Locate the last "additional.X" line, and add a new line, incrementing the last number by 1.
For example, if your last active line is:
additional.18=-XX:ReservedCodeCacheSize=1024m
You would need to add the following:
additional.19=-Xss2048k

-Save the file

-Restart the SBM
# service cdp-server restart
```