**WCG proxy resets**

Symptoms:

1. Reset alarms in the WCG Manager UI/reset emails.
2. Content\_gateway.out shows resets with stack traces.
3. Messages file (default = /var/log/messages) shows restarts. Make sure the resets are not caused by manual restarts, either via the command line/Content Gateway Manager, or via Appliance Manager of the WCG DOM.
4. Examine the extended.log entries before the reset (/opt/WCG/log/extended.log). If the same kind of urls are seen during each reset then this may be data related to the resets.
5. In some cases resets happen again and again and proxy stops processing requests. This will lead to an outage and will require a manual restart of WCG or reboot of WCG DOM.

Actions and Data to Gather:

1. Search KB articles and relevant release notes to identify a match with any existing known issues.
2. List all the key configurations: Caching, ssl decryption, Authentication, Explict/Transparent, Proxy chaining, APD and scan settings
3. WCG ConfigUploader files
4. Check if content\_gateway.out shows a stack trace for the reset. If it does not, then we may have to create an IB to let the kernel handle the crash and create a core file for further analysis.
5. Collect disk usage during the time of reset.
6. Run a script to periodically get ‘top’ output.
7. Check for system errors in messages file such as out of memory or network unreachable errors.
8. Check for DNS, DC, WISP and caching errors in messages file.
9. Analyze MRTG graphs – look for client and origin server connection spikes and memory spikes.
10. Look for memory exhaustion resets – Memory spike to over 2GB just before the reset. The content\_gateway.out shows “Could not allocate memory” errors.

Data related resets: Extended.log shows similar urls at the time of each reset.

1. If the reset seems data related, run WatchWCG.sh script. This script starts a tcpdump on the proxy on all interfaces with no filters and stops it when it detects a reset. This will give us the packet capture during the time of crash.
2. Make sure extended logging is enabled.

Memory related resets:

1. This may be caused by client connection spike. Client connection spike can be caused by DNS delays, WISP delays, DC delays.
2. If messages file shows WISP errors then we need to collect WSE configuploader, enable DStrace and WISP printself to understand the root cause of the delay.
3. Check if ‘scan all’ option is enabled and if there are several accesses to urls with large response times in the extended log.
4. Check for high number of simultaneous over 2GB file downloads during the time of reset. Sub-2GB files can also cause memory exhaustion.