Monitoring

What

Server check and Permission Check are great. This helps at installation time and to investigate issues. But what if an issue appears while you are not looking?

Let's implement interoperability with a monitoring solution to dogfood on *.tiki.org and make easily available to all other Tiki-powered sites.

Related: TRIM and System Configuration

When

- Started in Tiki12 -> https://sourceforge.net/p/tikiwiki/code/46421

Latest code:

Who

- Marc Laporte
- Changi
- Bernard Sfez
- you?

Dogfood

- We'll use for all our domains to improve uptime

Examples

- http://obm.org/wiki/obm-health-check-system
- https://sourceforge.net/projects/phpservermon/
- https://code.google.com/p/servphp/
- http://newrelic.com/
- https://cachethq.io

Wishes
Uptime/performance/content testing

Here are example of things that we want to monitor

Can be reported by Tiki

And thus, should be part of Tiki Check. If they can't be done via Tiki Check, please move to the other section.

- Basic stats about Tiki (version number, if needs upgrade, does DB need upgrade)
- How many times there has been a session collision
- How many days since index was fully rebuilt
- Number of days since last update (for sites managed via svn)
- Alert of changes in Tiki Check
  - So we know if there was a major change to a setting, which will potentially cause issues. Shared hosting companies often make changes to servers without informing anyone.
- Intrusion Detection System reported attacks
- XCache / APC: running out of memory
  - [https://github.com/wyattwalter/apc-php-monitor#readme](https://github.com/wyattwalter/apc-php-monitor#readme)
- Security DB file integrity check (but it would be better to manage this externally like TRIM does)
- Is the installer locked?
- Report of brute force login attempts
- Site closed because of too much traffic?
- Link checker
- Check missing images
- Binary files stored in DB. Ex.: if goes over 50 megs, there should be a warning to move to the filesystem.
- Check for standards compliance. See Accessibility
- Check that .htaccess is an alias of _htaccess (which should have been handled by Tiki installer)
- Check if my site has been listed on sites such as:
  - [https://developers.google.com/safe-browsing/](https://developers.google.com/safe-browsing/)
  - [https://en.wikipedia.org/wiki/McAfee_SiteAdvisor](https://en.wikipedia.org/wiki/McAfee_SiteAdvisor)

Uncertain

- Cron jobs: how do we set them up so we can have reporting and easy management?
  - How can Tiki/PHP know what cron jobs are programmed?
    - Perhaps by handling via Batch so we know what is coming up and what was done, via Logs
- Memory Consumption
- Defacement
- Spammy-looking activity

Beyond the scope of Tiki

- Crashes/errors (PHP/MySQL)
  - Email alerts of hard errors
  - "MySQL server has gone away"
- Tiki misbehaves when disk is full and often we forget to check for that: When system runs out of disk space, Tiki user will not be able to login.
- Unified search crash (ex.: the cron job to generate a new index has had an issue)
  - We would need the last date that the search was successfully re-indexed, and thus, if this is more than 10 days, there should be a warning.
• Server logs (to correlate with other reports).
• Add a check for domain name expiry
  ○ This is useful because the person hosting the Tiki may not be listed in the DNS registries and won't be informed of DNS changes (expiry, domain theft, etc)
  ○ Some Tikis can have several domain names (domain parking)
  ○ Will this be easy provided the anti-spammer protections?
  ○ Warn by email (both to TRIM manager and instance contact)
    ▪ 30 days before expiry
    ▪ Ideally, on any change to the entry (for domain theft)
  ○ See script by Jean-François Pelletier, started at Codefest
• Check response time
• Check spelling
  ○ If external tool, how does it access private content?
  ○ Check for all UTF-8 mess ups from server moves, such as: "Testing & optimization are topics of the next codeFEST PhpQuébec 2.1, which will be held in Montréal, Canada, May 16th to 18th, 2008"
• Check to see if Tiki is running properly (check presence of keyword like http://host-tracker.com/ and/or changes like http://www.changedetection.com/log/org/americana/index_log.html#changelist)
• Check for the presence of a customized 404 apache error page (we often to forget to set this up)

Other checks
It should be possible to add/create our own checks

• Check domain for presence of Google Analytics code, so as to avoid for site/design changes to lose them

Todo

• Pick a preferred tool from the options below
• Expose Tiki Check to an external monitoring tool

Website assessment services

• http://blogsuccess.com/7-free-website-evaluation-tools/
• https://www.ssllabs.com/ssltest/analyze.html?d=doc.tiki.org
• https://www.amberloom.com/

Questions

• Is realpath_cache check suitable for Tiki monitoring?
Options for local monitoring tools
logwatch

Options for external monitoring tools

Nagios

http://exchange.nagios.org/directory/Plugins/CMS-and-Blog-Software
https://www.monitoringexchange.org/inventory/Check-Plugins/Software/HTTP

Tiki-powered community members and sites related to Nagios
- http://www.ohloh.net/p/tikiwiki/contributors/167503846826
- http://www.ohloh.net/p/tikiwiki/contributors/167503732592
  - https://github.com/Tontonitch
    - http://www.ohloh.net/p/nconf/contributors/1498627906684352

Naemon

Icinga

Shinken

- Supports Nagios plugins:
Munin

Cacti

Zabbix

http://www.zabbix.com/features.php
http://www.zabbix.com/functionality.php
https://www.zabbix.com/documentation/3.0/manual/introduction/whatsnew300
http://www.zabbix.com/life_cycle_and_release_policy.php
http://www.zabbix.com/monitor_everything.php
http://www.zabbix.com/true_open_source.php
http://www.zabbix.com/consulting.php

RRDtool

Centreon

OpenNMS

Pandora FMS

http://pandorafms.com/
http://www.google-melange.com/gsoc/org/google/gsoc2012/articast

Zenoss

Observium

Check_mk

- Page project: http://mathias-kettner.de/checkmk.html
- Demo: http://mathias-kettner.de/check_mk_demo.html

Monit
Ganglia

Packetbeat
Packetbeat uses Elasticsearch and Kibana

JaM monitoring


Open Monitoring Distribution (OMD)

Prometheus
How we're building GitLab into the complete DevOps toolchain -> "We added system monitoring with Prometheus in 9.0."

Consul

PWGSC WPSS Validation Tool
"The PWGSC WPSS Validation Tool provides web developers and quality assurance testers the ability to perform a number of web site and web page validation tasks at one time. The WPSS Validation Tool crawls a site to find all of the documents, then analyses each one with a number of validation tools. The analysis includes:

- HTML validation,
- CSS validation,
- robots.txt validation,
- link violation checking,
- metadata checking,
- Technical Quality Assurance (TQA) checking,
- HTML document feature reporting, for example, forms,
- Open Data checking using a separate application tool."
https://github.com/wet-boew/wet-boew-wpss

Sensu

Related links
- https://github.com/CISecurity/Integration
- https://github.com/staabm/SysMonitor
- http://filp.github.io/whoops/
- https://github.com/jessp01/jam
- https://www.robustperception.io/monitoring-not-just-for-outages/

alias

- Nagios