Command monitoring

Sometimes what we want to monitor is not included in the logs. To solve that problem, Wazuh incorporates the ability to monitor the output of specific commands and treat that output just like log file content.

Contents

- How it works
  - Configure Wazuh agents to accept remote commands from the manager
  - Configure a command to monitor
  - Process the output
- Configuration
  - Basic usage
  - Monitor running Windows processes
  - Disk space utilization
  - Check if the output changed
  - Load average
  - Detect USB Storage
- FAQ
  - Can I monitor commands on Linux or Windows?
  - What are the possibilities of this capability?
  - Can I check if an application is running on an agent?