Whitepaper

State of 30-AUG-2017
Version 1.4

OPMONis

OPMONis

OPMONis combines in one software the monitoring of UPS and the controlling of systems. The software is running as a background Windows service. A windows client is used to set up the configuration.

The monitoring of via serial or USB cable connected UPS systems uses the WMI protocol. For network UPSs the protocol SNMPv1 is used. Independent from manufacturers any UPS that is attached to a Windows device can be used if it is shown as battery in the Device Manager or if it is providing the needed OIDs.

The controlling of the systems occurs in an agentless way by using standard protocols as WMI, vSpere API (VMware Web Services), Xen Management API, SSH, Ping and Wake on LAN (WoL). “Agentless” in this context means that there is no further software installation required on the Systems you have to control.

Availability

The OPMONis application is running in the background as a Windows service. No further maintenance is needed after first installation.

Stability

The chosen software architecture ensures a high stability. This is even increased by using stability mechanisms provided by the Windows operating system.

Correctness

All described features were ensured by performing whitebox tests during the development and by performing blackbox tests during the release cycles.

Usability

The user interface is haptic and easy to use. Even nonprofessionals can install, configure and use this application. To avoid incorrect or incomplete configuration data, all user input is validated by OPMONis. Additionally a test run can be triggered, verifying that all made configurations work properly. As well it is possibly by a commandline tool to access the basic functions of OPMONis without a GUI.

independis
information systems GmbH

www.independis.de
info@independis.de

Performance

The system resources needed by OPMONis for proper operation have been minimized. In so doing the software can be run on systems that are built for either maximal power efficiency or ideal energy-saving purposes.

Security

The communication between Windows service and client occurs over a „named pipe" connection. This ensures that access to the service from outside the device is impossible.

All sensitive data, like passwords are stored encrypted (AES) in the configuration.

For encryption is the internal Windows protection-class is used. This class is encrypting with a device-bound key. This way it`s impossible to identify out the private key from the config-file.

Specifications

- Running on Windows platform (.NET Runtime is needed)
- Windows Service for controlling and monitoring
- Windows application for configuration and monitoring (communication with Windows service by named pipe)
- All security sensitive Data is encrypted
- Controllable systems:
    - VMware ESX / ESXi / vCenter server
    - XenServer
    - Microsoft Hyper-V
    - Microsoft Windows
    - UNIX/Linux
    - MAC OS X
    - All other systems supporting SSH (Secure Shell)
- Protocols
    - vSphere API: VMware Web Services
      used to monitor and control VMware ESX / ESXi / vCenter Server
    - XenServer Management API
    - Windows Management Instrumentation (WMI)
      to control Windows Systems
    - Secure Shell (SSH)
    - Internet Control Message Protocol (ICMP, PING)
    - Wake on LAN (WoL)
    - SNMPv1

independis
information systems GmbH

www.independis.de
info@independis.de