Whitepaper

Stand 31.01.2019
Version 1.6

OPMONis

OPMONis

OPMONis kombiniert in einer Software die Überwachung von USVs und die Steuerung von Systemen. Der Betrieb erfolgt als Windows Service im Hintergrund. Die Konfiguration erfolgt über einen Windows Client der bei Bedarf gestartet wird.

Zur Überwachung seriell oder per USB angeschlossener USVs wird das WMI Protokoll verwendet, bei netzwerkfähigen USVs das SNMPv1 Protokoll Es können so herstellerunabhängig alle an einen Windows Rechner angeschlossenen USVs überwacht werden, die im Gerätemanager als Batterie angezeigt werden, oder die benötigten OIDs per SNMPv1 liefern.

Die Steuerung der Systeme erfolgt agentenlos, durch die Verwendung von Standardprotokollen wie WMI, vSphere API (VMware Web Services), Xen Management API, SSH, Ping und Wake on LAN. Agentenlos bedeutet hier, es muss auf den zu steuernden Systemen keine zusätzliche Software installiert werden.

Verfügbarkeit

Die Applikation läuft als Windows Service im Hintergrund. Es sind keine Wartungsarbeiten nötig.

Stabilität

Durch die eingesetzte Architektur der Software wird eine hohe Stabilität gewährleistet. Zusätzlich werden die vorhandenen Mechanismen des Windows Betriebssystems eingesetzt um die Stabilität des Windows Service zu optimieren.

Richtigkeit

Mit der Durchführung von White Box Tests während der Entwicklung und von Black Box Tests im Rahmen des Release-Zyklus wird sichergestellt, dass die Software die beschriebenen Anforderungen erfüllt.

Bedienbarkeit

Haptische und damit sehr leicht bedienbare Oberfläche, die es nicht nur Administratoren ermöglicht die Applikation einzurichten und zu verwenden. Benutzereingaben werden

independis
information systems GmbH

www.independis.de
info@independis.de

validiert um die Eingabe fehlerhafter Daten so weit möglich zu vermeiden. Über einen manuellen Test kann die vorgenommene Konfiguration geprüft werden. Ebenso ist es möglich über ein Kommandozeilenwerkzeug auf die Basisfunktionen von OPMONis zuzugreifen ohne eine graphische Oberfläche zu benötigen.

Performance

Die Anforderungen an die Systemressourcen zum Betrieb der Software sind möglichst gering gehalten. Dadurch lässt sich OPMONis auch auf energiesparender Hardware problemlos einsetzen.

Sicherheit

Die Kommunikation zwischen Windows Service und Client erfolgt über eine „Named Pipe“. Ein Zugriff auf den Service von außerhalb des Rechners ist somit nicht möglich.

Sicherheitsrelevante Daten wie z.B. Kennwörter werden in der Konfiguration verschlüsselt gespeichert (AES).

Für die Verschlüsselung wird die interne Windows Verschlüsselungsklasse ProtectedData verwendet. Diese verwendet einen maschinengebundenen Schlüssel, welcher nicht über die Konfigurationsdateien ausgelesen werden kann.

Technische Daten

- Betrieb auf Windows Plattform (.NET Runtime 4.7.2 oder neuer benötigt)
- Windows Service zum Überwachen und Steuern
- Verwaltungsprogramm für Konfiguration und Monitoring (Kommunikation mit dem Service über „Named Pipe“)
- Verschlüsselung sensitiver Daten (z.B. Passwörter in der Konfiguration)
- Steuerbare Systeme
    - VMware ESX / ESXi / vCenter Server
    - XenServer
    - Microsoft Hyper-V
    - Microsoft Windows
    - UNIX/Linux
    - MAC OS X
    - Alle anderen Systeme die SSH unterstützen
- Protokolle
    - vSphere API: VMware Web Services zur Überwachung und Steuerung von VMware ESX / ESXi / vCenter Server / free ESXi
    - Windows Management Instrumentation (WMI) zur Steuerung von Windows System
    - Secure Shell (SSH)
    - Internet Control Message Protocol (ICMP, PING)
    - Wake on LAN (WOL)
    - SNMPv1

independis
information systems GmbH

www.independis.de
info@independis.de