Tech-Talk: Open-Audit Classic

Quelloffenes Inventar-Werkzeug für Cloud Readiness Check, Hard- und Software-Inventar, Listen Dokumentation, von Verbandsprüfern akzeptiert

Tech-Talk: Open-Audit

Agenda

- Was ist Open-Audit Classic und wie ist es entstanden?
- Was kann man damit abbilden?
- Welche Plattform und Komponenten?
- Installation
- Live-Demo
- Eigene Auswertungen sehr einfach erstellen oder vorhandene nutzen
- Weiterentwicklung – der Open-Source Gedanke daran
- Web-Links

Tech-Talk: Open-Audit

Zweck des Projekts

- Open-Audit Classic ist eine quelloffene Software, die auf einem Windows Server betrieben, per WMI-Anfragen alle Windows PCs und Server mit ihrer Hardware und Software und Konfiguration erfasst und in einer MySQL-Datenbank speichert. Die Oberfläche ist komplett in PHP geschrieben und liegt in dieser Form vollumfänglich als Quellcode im Unterordner htdocs/openaudit.

- Die notwendigen Basiskomponenten sind ebenfalls Quelloffen und in der Form als Windows-kompilierte Dateien im XAMPP for Windows Projekt herunterladbar.

- https://sourceforge.net/projects/xampp/files/XAMPP%20Windows/
  - Aus dem Projekt werden nur Apache, Mysql (MariaDB), PHP und PHPMyadmin benötigt.

- Für das Inventarisieren von SNMP- und Netzwerkgeräten (Switches, Kameras, Webserver, IRMCs) wird das ebenfalls quelloffene NMAP mit WinPCAP benötigt Für eine auch häufig benötigte, einfache Softwareverteilung ist WPKG leicht zu implementieren. Der Ordner htdocs/ lässt sich auch optimal für eine Entwicklerinstallation von Wordpress verwenden oder für ein kleines Intranet.

Tech-Talk: Open-Audit

Entstehungsgeschichte

- in den 2000er Jahren wurde Open-Audit als GPLv3 lizensierte Open Source Software erstellt und war als Quellcode verfügbar. Seit Weggang des Haupt Entwicklers wird das Produkt unter einer AGPL-Lizenz weiterentwickelt. Weil damit Teile der Software Closed Source sind aufgrund einer grundlegenden Neuprogrammierung wurde die Weiterentwicklung eigener Vorstellungen damit komplizierter. Daher habe ich mich entschlossen, auf Basis der Open-Audit Stands, der noch unter der echten GPL-Lizenz stammt, diesen zu "forken" und weiter zu entwickeln. Das Resultat ist "Open-Audit Classic".

- Berücksichtigt wurden Anpassungen auf neue PHP-Versionen, MySQL und Apache, häufig benutzte zusätzliche Auswertungen, Erweiterungen in der WMI-Erkennung und vieles mehr Auch die Integration von NMAP und WinPCap wurde auf den aktuellen Stand gebracht.

Tech-Talk: Open-Audit

Was kann man damit machen?

- Komplettes Hardware-Inventar aller Windows PCs und Server über WMI-Script, das zeitgesteuert auf dem Server läuft, vielfach filterbar
- Liste aller freigegebenen Druckern
- Plattensizing mit Volumegrößen, Füllstand und freiem Platz
- Hardware-Inventar von Switches, Routern, Druckern IP-Kameras, USV, Linux-Systemen

- Liste aller installierten Softwareprodukte auf Windows-Systemen
- Erstellen einer Lizenzbilanz durch Filtern auf lizenzpflichtige Produkte

- Auswertungen für die IST-Analyse bei Cloud Readiness Checks in Excel übergeben und damit rechnen für die Cloud-Optimierung/Konzeption

Tech-Talk: Open-Audit

Highlights

- Doku: Open-Audit Classic wird von den Verbandsprüfern als Hard- und Softwaredokumentation in Kundenumgebungen akzeptiert
- Kann auf einem vorhandenen Server (vm) mit installiert werden. Best practice ist der s.dok Server
- Benötigt keine Clients, Zugriff erfolgt per WMI auf die Zielsysteme mit administrativen Credentials
- Offline und Push-Clients zum Inventarisieren von nicht-Netzwerk und non-domain Clients möglich
- NMAP kann SNMP-Informationen sammeln (2. zu importierende Aufgabe auf dem Server)
- Quelloffen – auch wenn man kein PHP beherrscht, lassen sich eigene Auswertungen leicht „zusammenkopieren“ und einsetzen
- Auswertungen für Lizenzbilanzen, IT-Sicherheitschecks und Cloud-Readiness Checks habe ich bereits erstellt
- Listen lassen sich nach Excel exportieren oder die MariaDB per ODBC anzapfen
- Teilweise schon in deutsch, Übersetzungen können in lang-Datei zugefügt werden

Tech-Talk: Open-Audit

Agenda

- System requirements:
  - Windows Server ab 2012 R2 (läuft aber auch unter Server 2008 R2)
  - 100 MB RAM, 10 GB Festplattenplatz, TCP und UDP Ports 3306 und 888 frei
- Microsoft Visual C++ Runtime 2015-19 (64-Bit) – im Setup Paket enthalten
- Apache Webserver (auf lokalem HTTP-Port 888) mit aktueller PHP-Version
- MariaDB aktuelle Version 10.x (Oracle hat MySQL übernommen und macht kein GPL3 mehr!)
  - Optional PHPMyAdmin zum Administrieren der Datenbank

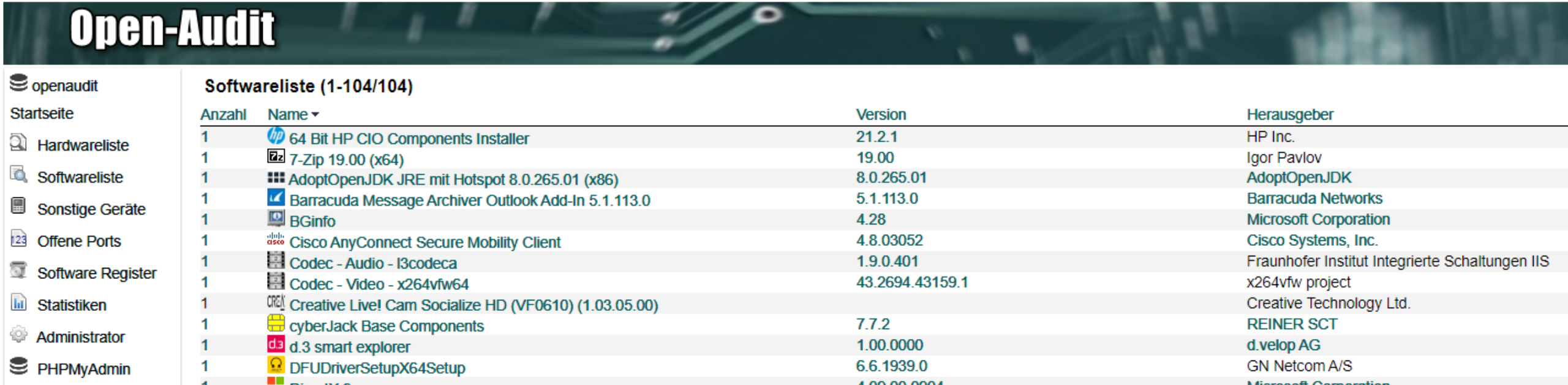
- Die grünen Elemente gibt es als XAMPP zusammengestellt

- Im Sysko-Portal liegt ein fertiges SETUP, das alles enthält

Tech-Talk: Open-Audit

Installation

- Setup Paket ~~und VC++ Runtime~~ herunterladen
- Setup auf dem geplanten Windows Server ausführen
- Liste aller IP-Adressen der Netze erstellen (Exceltabelle Spalte A je Netz 1..254 untereinander), Spalte A in Textdatei IP-Liste (Desktopverknüpfung) kopieren
- Windows Aufgabe importieren und einstellen und zum Testen 1x ausführen
- Anleitung hier: https://tech-nachrichten.de/open-audit-hard-und-software-inventar-aktualisieren/



Live-Demo

An meiner Maschine

Tech-Talk: Open-Audit

Live-Demo

- Installation
- Ggf. Registry-Schlüssel zum Zulassen von WMI-Admin-Requests als GPO verteilen für
- Windows-Aufgabe importieren
- Inventarisieren eines PCs
- Inventarisieren eines virtuellen Servers mit dem Offline-Skript
- NMAP-Scan
- Überblick Oberfläche
  - Auswertungen und Listen Hardware und Software
  - Statistik
  - Software-Register
  - Excel-Export

Tech-Talk: Open-Audit

Status → Ausblick

- Open-Audit Classic wird für Dokumentation/Inventar, IT-Sicherheitschecks, Cloud Readiness Checks und als Sysko-Werkzeug hundertfach genutzt. Die Betriebsverantwortung dafür hat jeweils der Sysko/Kunde.
- Es ist **kein Produkt** der GWS, bitte keine Supportvorgänge erstellen
- Es ist quelloffen, der Quellcode liegt auf GitHub
- Wer Ideen hat, etwas beizutragen oder Issues feststellt, kann das im Github machen und mich kontaktieren – oder es als Werkzeug für die eigene Tätigkeit beim Kunden verwenden.
  - Eigene Auswertungen
  - Informationen in einer Liste zusammenfassen

Tech-Talk: Open-Audit

Links

- Quellcode/Changelog auf Github: https://github.com/svenbolte/Open-Audit-Classic
- Technische Basis: https://sourceforge.net/projects/xampp/files/XAMPP%20Windows/
  - davon werden nur Apache, PHP, PHPMyAdmin und die MariaDB (MySQL), jeweils 64-Bit, benötigt
- Download fertiges SETUP-Paket: https://tech-nachrichten.de/?ddownload=3071

Vielen Dank für Ihre Aufmerksamkeit! Zeit für Ihre Fragen

Ihr Feedback bitte QR-Code scannen:

Patrick Bärenfänger

IT-Security-Manager und Auditor (TÜV)
Branchensoftware-Entwicklung

Tel: +49 (251) 7000-3896
Fax: +49 (251) 7000-3999
patrick.baerenfaenger@gws.ms