

Tech-Talk: Open-Audit Classic

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

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

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.

Entstehungsgeschichte

- in den 2000er Jahren wurde Open-Audit als GPLv3 lizenzierte 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.

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

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

Agenda

- System requirements:
 - Windows Server ab 2016 (läuft aber auch unter Server 2012 R2)
 - 200 MB freier Arbeitsspeicher, 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 (HTTP-Port 888, Oberfläche auf HTTPS-Port 4443) 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 auch als XAMPP zusammengestellt, das Setup-Paket ist aber auf die benötigten Elemente reduziert.
- Im Sysko-Portal liegt ein fertiges SETUP, das alles enthält

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/>

OpenAudit Classic - XGWSPBA1

Softwareliste (1-66/66)

CSV Export XLSX Export für MS-Excel

Anzahl	Name	Version	Ver aktuell	SCX	Bemerkungen
1	64 Bit HP CIO Components Installer	22.2.1	22.2.1	SC	HP Druckertreiber-Komponente
1	7-Zip 23.01 (x64)	23.01	23.01	SC	kostenfreies Open-Source-Packprogramm (64-Bit Version, NSIS Installer mit RAR 6 Unterstützung). Mit 7zSFX Oberfläche (aus Innoset)
1	Audacity	3.4.2.0	3.4.2	C	2023.11.17-Audacity Audio Editor - kostenloser Bildbetrachter Open Source Musik-Bearbeitungssoftware zum Bearbeiten, Konvertieren und Erzeugen
1	Avidemux	2.8.2.24076	2.8.1	C	2024.04.16-Video-Bearbeitungssoftware - Open-Source, Nightlies @ https://avidemux.org/nightly/vsWin64/ Videobearbeitungs-Werkzeug (ähnlich)
1	BGinfo	4.32.0.0	4.32.0.0	SC	BGInfo Mod, RDCMAN 2.93.1431.0, Autoruns 14.10.0.0, BatteryInfoView 1.2.5.0, PuTTY 0.81.0.0, Filedate, Abmelden/Herunterfahren Links Microsoft

Navigation: STARTSEITE, Hardwareliste, Softwareliste, Sonstige Geräte, Statistiken, Offene Ports, Software Register, Administrator, CSV2XLSX, PHPMyAdmin, Wordpress-BLOG, Hilfe

Live-Demo

An meiner Maschine



- 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

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

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



Patrick Bärenfänger

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

Tel: +49 (251) 7000-3896

patrick.baerenfaenger@gws.ms



Ihr Feedback
bitte QR-Code
scannen:

