

Über die Sicherheit von SiteAudit Hosted

September 2018

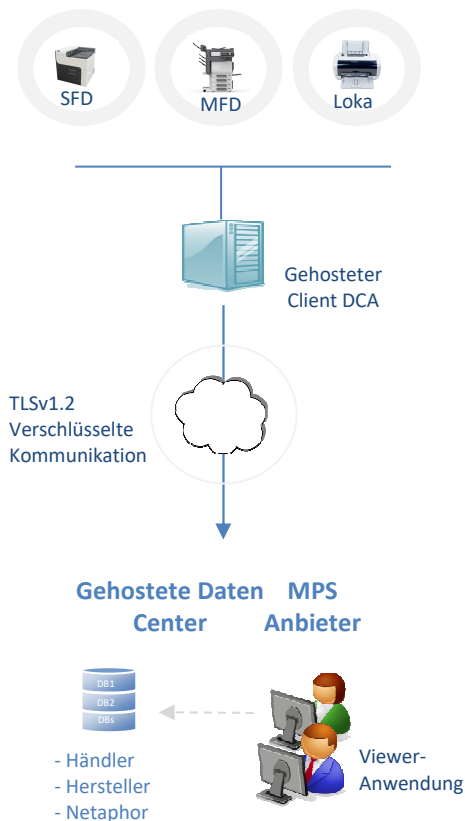
In diesem Dokument:

- Überblick Sicherheit
- Datenkommunikation und -aktivierung
- Datenerfassung und -verkehr
- Zusammenfassung

Überblick SiteAudit

SiteAudit Hosted ist eine MPS-Anwendung, um aus der Ferne Daten von lokalen und Netzwerkdruckern zu sammeln. Es verwendet einen Hosted Client (Data collection agent-DCA) auf Kundenseite und einen oder mehrere Viewer, die beim MPS-Anbieter installiert sind. Die Daten werden am Kundenstandort gesammelt und auf einem sicheren Transportweg zu einer SQL-Datenbank gesendet. Damit steht den MPS-Anbietern eine sichere und einfache Möglichkeit zur Verfügung, Zählerstände zu sammeln und zu verwalten, sowie Informationen über Verbrauchsmaterialien, Fehler und Drucker zu erhalten.

Aufbau SiteAudit Hosted



Kundenstandort - Hosted Client (DCA)

Einrichtung – Data Collection Agent (DCA)

- 32-Bit oder 64-Bit Windows 8.1/10 oder Server 2012/R2 und 2016
- .NET 4.51 oder höher
- SiteAudit Hosted Client (DCA)
- Hosted Client (DCA) Connection Key File
- Administratorprivilegien für Anwenderkontenkontrolle (User Account Control, UAC)

Erkennung und Datenerfassung

- Erkennung SNMP v1/v2c/3
- Datenerfassung SNMP, HTTP, NPAP, CPCA und WMI; Lokaler oder Domain Admin Account für lokale Drucker
- Gescannte Ports: 161, 1650, 9100, 80, 8080, 631, 9300, 47545, 21, 23

Optionen des Datentransports von gehosteten Datenbanken

- TCP port 443 – REST über HTTPS

MPS-Anbieter – Hosted Viewer

Einrichtung – MPS-Viewer

- 32-Bit oder 64-Bit Windows 8.1/10 oder Server 2012/R2 und 2016
- .NET4.5.1 oder höher
- SiteAudit Viewer Lizenz oder Viewer Admin Lizenz
- Hosted Client (DCA) Connection Key File
- Administratorprivilegien für Anwenderkontenkontrolle (User Account Control, UAC)

Viewer-Verbindung zu gehosteten Datenbanken

- TCP port 443 – REST über HTTPS
- SiteAudit Hosted Administrator- oder Viewer-Lizenz

MPS-Betrieb

- Erkennungskonfiguration
- Filtern und Analyse
- Berichtswesen und Planung
- Konfiguration der Alarmmeldungen

Benutzeranwendungen

- Viewer
- Cockpit
- SiteAudit Visualizer
- SiteAudit Analyzer

Datenkommunikation

Der SiteAudit Hosted Client (DCA) ist ein Datensammler. Die gesamte Kommunikation wird vor der Übertragung an die gehostete Datenbank verschlüsselt. Die Verschlüsselung erfolgt asymmetrisch und nach einem minimal 4096 Bit SSL-Zertifikat einer vertrauenswürdigen Zertifikatsautorität (Certificate Authority, CA) wie DigiCert™ oder VeriSign® (Symantec) für die gesamte Kommunikation mit der gehosteten SQL-Datenbank. Die Datenübertragung erfolgt über REST.

Sowohl der Hosted Client (DCA) als auch der/die Viewer des MPS-Anbieters können sich nur mit der gehosteten Datenbank verbinden, wenn sie über einen lizenzierten Viewer und eine Schlüsseldatei mit Zugang zur gehosteten Datenbank verfügen.

Aktivierung des Hosted Client (DCA)

Die Aktivierung des Hosted Client erfolgt über die gehostete Serveranwendung von Netaphor. Vor der Installation wird eine Lizenz für die zentrale Verbindungsdatei erzeugt. Diese verwendet eine verschlüsselte Verbindungsfolge und einen Shared Key (64 Bytes lang), um Daten zwischen dem Hosted Client (DCA) und der gehosteten Datenbank zu verschlüsseln. Die Anwendung verwendet einen REST-Transport für die Datenkommunikation.

Die Lizenzen können entweder über ein Ablaufdatum oder über eine Deaktivierung des Hosted Client (DCA) entzogen werden. Sobald der Hosted Client (DCA) über das Key File verfügt und installiert ist, speichert er den Shared Key im Windows Geschützten Speicher der jeweiligen Maschine. Daten können ohne gültiges Key File weder erfasst oder angesehen, noch kann von einer beliebigen Maschine darauf zugegriffen werden. Der Hosted Client (DCA) gewährt keinen Zugang zum Namen der Kundendatenbank, zum Benutzernamen oder zum Passwort.

Erkennung und Datenerfassung

SiteAudit erkennt Druckerbestände. Der Erkennungsprozess läuft wie folgt ab. Erkennung über SNMP v1/v2c/v3

- jedes einbezogene Netzwerk, jeder Bereich, jede statische IP auf der Liste bestimmt die Adressen in dieser Liste
- jedes ausgeschlossene Netzwerk, jeder Bereich, jede statische IP bestimmt, ob eventuell Adressen dieser Liste ausgeschlossen werden sollen

SiteAudit scannt Geräte für folgende Ports:

- 161 SNMP um zu sehen, ob SNMP aktiv ist. SMP wird für die Datenerfassung verwendet
- 80 HTTP um zu sehen, ob ein Embedded Web Server vorhanden ist. HTTP wird für die Datenerfassung verwendet
- 9100 Druckerprotokoll wird für die Datenerfassung verwendet
- 1650 genauso wie 9100
- 631 IPP Druckerprotokoll für Drucker werden für die Datenerfassung verwendet.
- 135 RPC wird verwendet, um einen Windows Host für lokale Drucker zu erkennen
- 47545 (CPCA) und 9300 (NPAP) kann auch verwendet werden, wenn der Drucker diese Protokolle unterstützt
- Ports 21 (FTP) and 23 (Telnet) potenzielle Sicherheitslücke zu identifizieren

Um die Netzwerkbelastung zu minimieren, werden Daten nach Typ und in konfigurierbaren Intervallen erfasst. Weitere Informationen zur Erkennung und Datenerfassung finden Sie unter

<https://support.netaphor.com/index.php?article/AA-00594> Weitere Informationen zur DNS-Erkennung finden Sie unter <https://support.netaphor.com/index.php?article/AA-00391/0/>

Netzwerkbelastung

Die SiteAudit Datenerfassung kann als *langsamer, stetiger Empfang von Datenpaketen* bezeichnet werden. Folglich wird nur ein geringer Prozentsatz der Netzwerkbandbreite genutzt. Die Netzwerkbelastung ist abhängig von der Anzahl der Geräte, die SiteAudit überwacht. Unten sehen Sie Beispiele über die Höhe der Netzwerkbelastung in drei verschiedenen großen Flotten: 250, 1.000 und 10.000 Drucker.

Die Belastung basiert auf einer typischen Umgebung, die Ergebnisse können aber in Abhängigkeit der Zusammensetzung aus lokalen und Netzwerkdruckern, der Anzahl der Zähler, des Adressplatzes, der Anzahl der IP-Adressen und anderer Faktoren variieren.

Number of Printers	% Usage in 100 MB Network	% Usage in GB Network
250	0.003	0.000293
1000	0.001	0.000977
10000	0.103	0.010058594

Weitere Informationen zur Netzwerkbelastung finden Sie unter <https://support.netaphor.com/index.php?/article/AA-00594>

Erfasste Daten

Erfasste Daten bestehen aus Informationen über Druckerbestände, Zähler, Verbrauchsmaterial und Fehlerinformationen. Ein Beispiel erfasster Daten ist nachfolgend aufgeführt.

Bestandsinformation

Hersteller
Modell
IP-Adresse
Druckername
Produktnummer
Seriennummer
Bestandskennzeichnung
Ort
Drucker MAC-Adresse
Host MAC-Adresse

Verbrauchsmaterial

Restbestand Verbrauchsmaterial %
Original Bestand Verbrauchsmaterial
Benutztes Verbrauchsmaterial in %
Datum des erkannten Toners
Ersetzt am
Art des Verbrauchsmaterials
Verbrauchsmaterialtyp
Artikelnummer Verbrauchsmaterial
Seriennummer Verbrauchsmaterial
Installationsdatum Verbrauchsmaterial

Zähler

Gesamtseiten
S/W Alle
S/W Druck
S/W Kopie
S/W Groß
Farbe Alle
Farbe Druck
Farbe Kopie
Farbe Groß
Groß
Klein
Kopie
Druck
Fax
Scan

Fehler

Alarm Code
Schweregrad
Trainingsstand
Zustand
Lösungsstatus
Ereignisbeschreibung
Ereignisdauer
Ereignis Start und Ende

Fehler (Fortsetzung)

Name Service Level Agreement
Kontakt
Gesamtfehler
Betriebszeit %
Letzte erfolgreiche Kommunikation
Zuletzt erkannt
Gerätstatus (Bereit/Fehler/Warnung)
Antwortzeit

Kreditkarten oder persönliche Daten werden nicht gespeichert. Auftragsdaten können erfasst werden, wenn die Konfiguration von SiteAudit die Erfassung dieser Informationen vorsieht. Standardmäßig ist diese Einstellung deaktiviert. Eine lokale Admin-Berechtigung mit Zugang zu den Zielrechnern ist erforderlich, um diese Funktion zu konfigurieren. Eine vollständige Liste der Daten finden Sie unter <https://support.netaphor.com/index.php?/article/AA-00779/104/>

Anmeldeinformationen

SiteAudit erfordert in den folgenden Fällen Anmeldeinformationen:

- Für die Erkennung direkt verbundener Drucker die Windows-Administratoranmeldeinformationen für die Hosts mit angeschlossenen Druckern.
- Für die direkte Druckererkennung mit WMI ist ein Konto erforderlich, das über die vollständigen Berechtigungen für den ROOT WMI-Namespace verfügt.
- Für die SNMPv3-Erkennung

SiteAudit speichert alle Kennwörter in Windows Protected Storage und kann nur auf dem Computer entschlüsselt werden, auf dem sie eingegeben wurden. Wenn der DCA auf einen neuen Computer verschoben wird, müssen diese Kennwörter auf diesem Computer erneut eingegeben werden.

Common Questions about Data Collection

- **Gerätedatenerfassung:** Es werden nur Gerätedaten erfasst. Benutzerinformationen werden nicht von einem Gerät erfasst. Informationen, wie z. B. Benutzerkonten auf dem Gerät für Follow-Me-Druck oder sicheres Drucken oder die Liste der Aufträge auf Geräten, werden nicht erfasst
- Keine personenbezogenen Daten (PII) wie Benutzerkennwörter, Kreditkarteninformationen, SSN usw. werden von SiteAudit gesammelt oder gespeichert
- Die Auftragsdatenerfassung ist optional. Diese Daten werden vom Windows-Spooler gesammelt, müssen jedoch vom Benutzer aktiviert werden, um dies zuzulassen
- Daten werden in einem SQL Server gespeichert: Der Kunde steuert den SQL Server in einer SiteAudit OnSite-Umgebung und kann optional entscheiden, dass die Daten auf dem Server verschlüsselt werden

Externe Kommunikation - außerhalb der Firewall: Dies wird vom Kunden gesteuert. Die einzige externe Kommunikation erfolgt über Benachrichtigungs-E-Mail oder geplante Berichte. Der Kunde kann steuern, welche Benachrichtigungen an wen gesendet werden. Gleiches gilt für geplante Berichte

Zusammenfassung

Durch die Verwendung des TLS v1.2 Transportmechanismus, verschlüsselter Key Files und sicherer gehosteter Server, die nach vertrauenswürdigen CA zertifiziert sind, werden von SiteAudit Hosted angemessene Sicherheitsmechanismen genutzt, die den Schutz der Druckdaten gewährleisten.

Netaphor Software Inc.

SiteAudit Hosted wurde im Oktober 2011 in den Markt eingeführt und wird an Kunden in über 30 Länder verkauft.

Netaphor Software, Inc. (www.netaphor.com) wurde 1997 in Irvine, Kalifornien, gegründet; Entwicklung und Vertrieb von Lösungen zur Druckkostenkontrolle sowie eine Weiterentwicklung von Dienstleistungen sollen Unternehmen beim Bestandsmanagement helfen. Das tragende Produkt unserer Firma, SiteAudit, ist die führende Softwarelösung für mittelständische Unternehmen und Betriebe, um Kosten und Service zu identifizieren und zu managen, so dass diese Unternehmen bis zu 30 Prozent der Kosten im Lebenszyklus des Druckerbestands einsparen können. Netaphor SiteAudit 5.0 ist der Gewinner des Winter 2012 "Pick" Preises als Herausragende Flottenmanagementlösung durch die Herausgeber im Buyers Laboratory Inc LLC (BLI).

