SiteAudit Technischer Artikel

SiteAudit OnSite Sicherheit

November 2018

In diesem Dokument finden Sie:

Überblick über SiteAudit

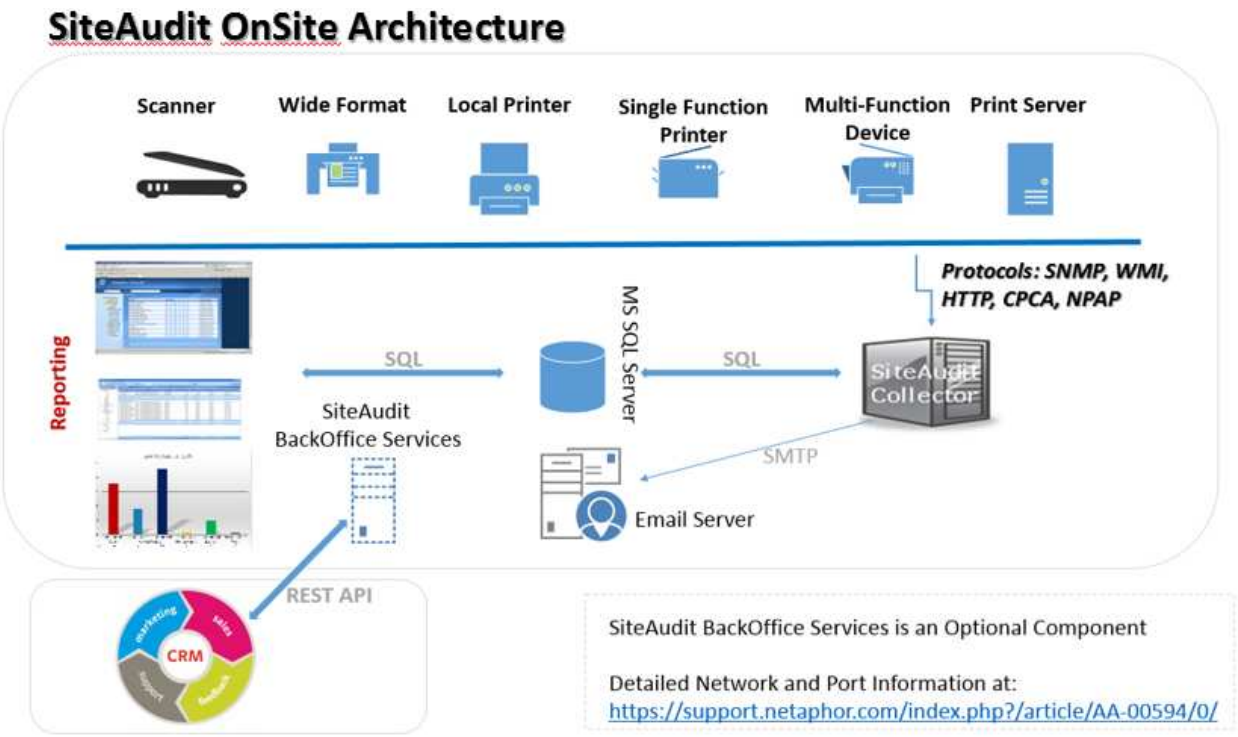
Die MPS Anwendung SiteAudit OnSite erfasst die Zustandsdaten lokaler und im Netzwerk betriebener Drucker. Sie verwendet auf Kundenseite einen Data Collection Agent und einen Viewer. Die Daten werden auf Kundenseite erfasst und zu einer Microsoft SQL-Datenbank gesendet. Sie stellt eine sichere und einfache Art für MPS-Anbieter dar, um Zähler, Verbrauchsmaterial, Fehlermeldungen und Druckerinformationen zu sammeln.

Das folgende Diagramm zeigt SiteAudit Onsite und seine verschiedenen Komponenten

Bestandteile

SiteAudit besteht aus den folgenden Hauptkomponenten:

- **SiteAudit Viewer** –Der SiteAudit Viewer wird verwendet um Berichte anzusehen, zu bearbeiten und anzupassen.
- **SiteAudit Monitor** – Der Microsoft Windows Dienst, der die Druckererkennung, das Erfassen der Daten und die Speicherung der Daten in der Datenbank durchführt.
- **SiteAudit Reporting Website** – installierte Webseite, um mittels IIS Zugang zu Berichten zu erlangen.



Erkennung und Datenerfassung

Die SiteAudit Erkennung wird über SNMP durchgeführt. Entdeckung über SNMP v1 / v2c und mit SA V6.4 oder später SNMPv3
Die Erkennung erlaubt sowohl IP-Adresskreise festzulegen als auch auszuschließen.

- jedes inbegriffene Netzwerk, der Adresskreis oder jede statische IP-Adresse entspricht den Adressen in der Auflistung
- jedes ausgeschlossene Netzwerk, der Adresskreis oder jede statische IP-Adresse ist in der Auflistung ausgeschlossen

Die Erkennung wird folgendermaßen durchgeführt:

1. SiteAudit sendet ein Signal aus, um Geräte und Router zu finden. Die Adressen müssen explizit in der Liste der zu untersuchenden Adressen enthalten sein.
2. SiteAudit führt einen Pingsuchlauf durch, um Netzwerkgeräte zu finden.

SiteAudit sucht nach den folgenden Ports, um Drucker zu finden:

- 161 SNMP um zu prüfen, ob SNMP aktiviert ist. Die Daten werden über SNMP erfasst.
- 80 HTTP um zu prüfen, ob ein integrierter Webbrowser vorhanden ist. Die Daten werden über HTML erfasst.
- 9100 Druckprotokoll für Drucker dient zur Datenerfassung.
- 1650 wie 9100
- 631 IPP Druckprotokoll dient zur Datenerfassung.
- 135 RPC, um zu prüfen, ob ein Windows Host für lokale Drucker vorhanden ist.
- 47545 (CPCA) und 9300 (NPAP) können auch verwendet werden, wenn der Drucker solche Protokolle unterstützt.
- Ports 21 (FTP) und 23 (Telnet) dienen der Identifizierung möglicher Sicherheitsrisiken

Um den Netzwerkverkehr zu minimieren, werden die Daten nach Typ und in konfigurierbaren Intervallen gesendet. Weitere Informationen zur Erkennung und Datenerfassung finden Sie unter https://support.netaphor.com/index.php?/article/AA-00594 Informationen zur DNS Erkennung finden Sie unter https://support.netaphor.com/index.php?/article/AA-00391/0/

Windows Firewall

Falls die Windows Firewall aktiviert ist, muss diese so konfiguriert werden, dass SiteAudit der Zugriff auf IP, ICMP, SNMP und SQL Server erlaubt wird. Gleiches gilt für die entfernten Hosts, an die Drucker lokal angeschlossen sind. Falls SiteAudit auf entfernte Hosts zugreift, muss die Firewall erlauben, dass die jeweiligen Pakete hinein und wieder herausgeschickt werden dürfen. Die Aktivierung von "Remoteüberwachung" aktiviert alle von SiteAudit benötigten Zugänge auf dem entfernten Host.

Der Zugang zu TCP Port 135 muss auf dem SiteAudit Monitor Host und allen Windows Zielcomputern aktiviert werden.

Direkt angeschlossene (lokale) Drucker

SiteAudit erkennt Drucker, die über USB oder parallel an einen Windows Rechner angeschlossen sind. Um Zugang zum Host zu erhalten, benötigt SiteAudit die Anmeldeinformationen des Benutzers, der an diesem PC als Administrator registriert ist. Um sicherzustellen, dass die Suche erfolgreich ist, sollten Sie:

- Alle Anmeldeinformationen sämtlicher Hosts zur Verfügung stellen
- Sicherstellen, dass die Anmeldeinformationen NICHT nach einer bestimmten Anzahl von Fehlversuchen gesperrt werden
- Den Bericht "Unauthenticated Hosts" ausführen, um einen Überblick der Hosts zu bekommen, die den Zugang verweigern, und die Anmeldeinformationen dieser Hosts hinzufügen.

Anmeldeinformationen

SiteAudit benötigt Anmeldeinformationen in vier Fällen:

- Die Installation von SiteAudit auf einem Server oder einer Workstation, der/die ein lokales Konto benötigt, um einen Dienst auszuführen.
- Installation des SQL Server oder der SQL Server Express Datenbank erfordert ein Passwort des Systemadministrators, oder falls die integrierte Sicherheit verwendet wird, die Anmeldeinformationen einer Person, die den Zugang zur Datenbank als Administrator hat.
- Für die Erkennung direkt angeschlossener Drucker werden die Windows Admin Anmeldeinformationen für die Hosts mit lokal angeschlossenen Druckern benötigt.
- Direkte Druckererkennung über WMI erfordert ein Konto mit vollen Rechten zur ROOT WMI Namespace.
- Auch zur Ermittlung von SNMPv3

SiteAudit speichert alle Passwörter in einem Windows geschützten Speicher; sie können nur auf dem Gerät entschlüsselt werden, von dem aus sie eingegeben wurden. Wird der DCA auf ein neues Gerät verschoben, müssen diese Passwörter auf diesem Gerät erneut eingegeben werden.

Zugriffssicherheit

- Benutzer haben gesicherten Zugang zu SiteAudit-Daten, die in einer MS SQL Server-Datenbank gespeichert sind und auf die sie über ihr Windows-Konto oder alternativ über ein MS SQL Server-Konto zugreifen können. Der Zugang, um die SiteAudit-Anwendung zu starten, wird über die Active Directory-Anmeldung bereitgestellt.
- Die Funktionssicherheit von Netaphor SiteAudit ist optional und dazu entwickelt, den Zugang zu verschiedenen SiteAudit Funktionen zu kontrollieren. Die Kontrolle wird aufrechterhalten, indem den Benutzern Rollen zugewiesen werden, so wie ein Windows Administrator Benutzern Rollen zuweist, um die Nutzung von Funktionen auf einem Windows-Computer zu erlauben oder zu verweigern. SiteAudit Rollen werden innerhalb der von SiteAudit verwendeten SQL Serverdatenbank definiert und verwaltet. Der Zugang erfolgt über den System-/Datenbankadministrator.
- Um sich zu authentifizieren, können Benutzer jede Anmeldemethode verwenden, die sie gewohnt sind (wenn es sich um ein Active Directory Konto handelt); bei einem SQL-Konto erfolgt die Authentifizierung über einen Benutzernamen/ein Passwort.
- Separate Zugangskontrolle wird über die Anwendung nicht verwaltet. Zugang besteht entweder über Active Directory oder ein SQL Konto.
- Benutzeridentifizierungen werden nicht außerhalb des Kundenetzwerks verwendet.

Netzwerkbelastung

Die SiteAudit Datenerfassung kann als *ein langsamer kontinuierlicher Empfang von Paketen* beschrieben werden. Daher ist nur ein Bruchteil der zur Verfügung stehenden Bandbreite belastet. Der Netzwerkverkehr steht im Zusammenhang mit der Anzahl der Geräte, die SiteAudit überwacht. Die folgenden Beispiele beschreiben den Netzwerkverkehr für drei unterschiedlich große Geräteflotten: 250, 1.000 und 10.000 Drucker.

Die Abschätzung des Netzwerkverkehrs basiert auf einer typischen Umgebung, jedoch kann das Ergebnis vom Verhältnis der lokalen und Netzwerkdrucker, Anzahl der Zähler, Adressumfang, Anzahl der IP-Adressen und anderen Faktoren abhängen.

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

Lesen Sie mehr zum Thema Netzwerkverkehr https://support.netaphor.com/index.php?/article/AA-00594

SNMP Zugang

Das SNMP-Protokoll beinhaltet eine Regelung zur Zugangskontrolle über die "Community" Zeichenfolgen. Es wird eine Community Zeichenfolge benötigt, um Zugang zum Gerät zu erlangen. SiteAudit pflegt eine Liste mit Community Zeichenfolgen, die verwendet wird, um Zugang zu den SNMP-Daten des Geräts zu bekommen.

Diese Liste besitzt eine Reihenfolge, in der SiteAudit Zugangsversuche unternimmt, bis die Liste komplett abgearbeitet ist. Diese Liste enthält bereits Einträge (einen Satz normalerweise gebräuchlicher Zeichenfolgen), aber der Benutzer kann Zeichenfolgen löschen oder hinzufügen und auch deren Reihenfolge für die Verwendung ändern.

Einige SNMP Agenten innerhalb des Geräts können so konfiguriert sein, dass sie "Authentifizierungsfehler" Traps erzeugen, wenn eine Zeichenfolge nicht für das Gerät gültig ist. Um diese Traps zu verhindern sollten Sie:

- Sicherstellen, dass die Liste der Community Zeichenfolgen nur benötigte Begriffe enthält.
- Authentifizierungsfehler Traps ignorieren, wenn sie als Quelle der Anfrage, also SiteAudit, identifiziert werden (die Anwendung, die die Mitteilung der ungültigen Community Zeichenfolge sendet).
- Deaktivieren der Authentifizierungsfehler Traps am Gerät.

Erfasste Daten

Die erfassten Daten hängen vom jeweiligen Drucker, Zählern, Verbrauchsmaterial und Fehlerinformationen ab. Die folgende Liste ist lediglich ein Beispiel.

Bestandsinfo
Hersteller
Modell
IP-Adresse
Druckername
Produktnummer
Seriennr.
Bestands-Tag
Standort
Drucker MAC-Adresse
Host MAC-Adresse

Verbrauchsmaterial
Verbleibendes VB in %
Original Befüllmenge
% der verwendeten VB
Datum Tonererkennung
Gewechselt am
VB-Beschreibung
VB-Typ
VB-Teilenr.
VB-Seriennr.
VB-Inst.-Datum

Zähler
Gesamtseiten
S/W Alle
S/W Druck
S/W Kopie
S/W Groß
Farbe Alle
Farbdruck
Farbe Kopie
Farbe Groß
Groß
Klein
Kopie
Druck
Fax
Scans

Fehler
Alarmcode
Sicherheitsstufe
Trainingsstufe
Status
Aufllösungsstatus
Problembeschreibung
Problemdauer
Problem Start/Ende

Fehler (Fortsetzung)
Leistungsvertrag Name
Kontakt
Gesamtfehler
Verfügbarkeit%
Letzte erfolgreiche Kommunikation
Zuletzt gemeldet
Gerätestatus (Bereit/Fehler/Warnung)
Reaktionszeit

*VB=Verbrauchsmaterial

Es werden keine Kredit- oder persönliche Daten gespeichert. Auftragsdaten werden nur dann gespeichert, wenn die Konfiguration von SiteAudit vorsieht, diese zu sammeln. Als Standard ist diese Funktion deaktiviert. Es wird ein lokaler Admin mit Anmeldeinformationen der gewünschten Arbeitsplatzrechner benötigt, um diese Funktion zu aktivieren. Eine komplette Liste der Daten finden Sie unterhttps://support.netaphor.com/index.php?/article/AA-00779/104/

Häufige Fragen zur Datensammlung

- Datensammlung vom Gerät Die Datensammlung bezieht sich nur auf das gesamte Gerät. Es werden keine Benutzerinformationen über die Geräte erfasst. Folglich werden Informationen wie Benutzerkonten auf dem Gerät für Follow Me Printing oder sicheren Druck oder die Liste der Aufträge auf diesem Gerät nicht erfasst.
- Keine personenbezogenen Daten (Personally Identifiable Information oder PII) wie Benutzerpasswort, Kreditkarteninformationen, SSN oder ähnliches werden von SiteAudit weder erfasst noch gespeichert.
- Die Sammlung von Auftragsdaten ist eine Option. Diese Daten werden über den Windows Spooler gesammelt, müssen aber vom Benutzer aktiviert werden, um dies zuzulassen.
- Die Daten werden auf einem SQL Server gespeichert. Da es sich hierbei um SiteAudit OnSite handelt, kontrolliert der Kunde den SQL Server und kann optional entscheiden, ob die Daten auf dem Server verschlüsselt werden sollen.
- Externe Kommunikation – außerhalb der Firewall: All das liegt in der Kontrolle des Kunden. Die einzige externe Kommunikation erfolgt über Benachrichtigungen oder geplante Berichte. Der Kunde hat die Kontrolle, welche Benachrichtigungen versendet werden und an wen. Ähnliches gilt für geplante Berichte.

Netaphor Software Inc.

SiteAudit OnSite wurde im Oktober 2006 im Markt eingeführt und wird von Kunden in mehr als 50 Ländern genutzt.

Gegründet 1997 mit seinem Sitz in Irvine, Kalifornien, entwickelt und verkauft Netaphor Software, Inc. (www.netaphor.com) Werkzeuge zur Bestandsverwaltung, die Kunden dabei unterstützen, Druckerkosten zu optimieren und den Service zu verbessern. Das Hauptprodukt der Firma, SiteAudit, ist eine der führenden Lösungen in mittleren und größeren Unternehmen, um Kosten zu identifizieren, den Bestand zu verwalten, den Service zu verbessern und Firmen über die Nutzungszeit eine Bestandskostenersparnis bis zu 30 % zu ermöglichen. Netaphor SiteAudit 5.0 und 6.0 gewann im Winter 2012 und 2015 die "Pick" Auszeichnung als herausragendes Produkt zur Flottenverwaltung beim Buyers Laboratory Inc LLC (BLI).