SiteAudit Knowledge Base

Netzwerk Traffic Guide

März 2013

In diesem Artikel:

Dieser Artikel erklärt wie SiteAudit Daten sammelt und warum die Netzwerkbelastung minimalisiert wird. Die Zielgruppe für diesen Artikel sind IT Administratoren oder sonstige Personen welche die Software implementieren.

Netzwerk Traffic

Der Netzwerk Traffic kann durch verschiedene Faktoren beeinflusst werden: Design des Netzwerks, Anzahl der Netzwerke, Subnetze und Routing. Letzteres trifft natürlich auf alle Netzwerkapplikationen zu. SiteAudit bemüht sich darum das "good citizen" Prinzip einzuhalten indem es gegenüber anderen Ressourcen im Netzwerk unauffällig und nicht beeinflussend wirkt.

- Was ist die Netzwerkbelastung?

Während des normalen Einsatzes kann der Netzwerk Traffic nicht gemessen werden, weil er dafür zu gering ist. Es besteht kein messbarer Einfluss auf die Netzwerk Bandbreite und Qualität des Dienstes. Falls „Automatisches Erfassen von Netzwerken" aktiviert ist nutzt SiteAudit Broadcasts um Netzwerke und Geräte zu finden. Broadcast kann deaktiviert und die Erfassung eingeschränkt werden um besser an Ihre Umgebung angepasst zu werden. Während des Erfassungszyklus beträgt die Messung der Netzwerkbelastung ca. 3% - 5%. Das ist der Höchstwert für SiteAudit. SiteAudit erlaubt es Informationen von IP Netzwerk Erfassungen zu importieren um ein schnelles und einfaches Setup zu ermöglichen. (Referenzieren Sie hierzu den Knowledge Base Artikel „Importieren von Daten").

Wie die Erfassung funktioniert

Wenn gewünscht ist SiteAudit dazu in der Lage alle Printer Assets zu erfassen. Broadcasts, falls aktiviert, werden nur während des Erfassungszyklus gesendet. Die Broadcast Pakete enthalten folgende Varianten:

- SNMP
- ICMP

Der Prozess der Erfassung funktioniert wie folgt:

1) Für jedes inkludierte Netzwerk auf der Liste sollte die Adresse in der Liste festgelegt werden
2) Festlegen ob Adressen ausgeschlossen werden sollen (entweder durch ein anderes Netzwerk oder eine Range)
3) Für eine inkludierte Adresse senden Sie ein ICMP Paket an diese Adresse

4) Falls die Adresse auf ICMP antwortet

5) Feststellen ob sie SNMP unterstützt, nutzen Sie die jeweils spezifizierten Community Strings um festzustellen welcher Community String genutzt werden soll

6) SiteAudit scannt die folgenden Ports um Drucker zu finden:

- 161 SNMP um zu sehen ob SNMP verfügbar ist. SNMP wird genutzt um Daten abzufragen
- 80 HTTP um zu sehen ob ein embedded Webserver vorhanden ist. HTTP wird genutzt um Daten zu sammeln
- 9100 Druckprotokoll für Drucker, wird genutzt um Daten zu sammeln
- 1650 gleich wie 9100
- 631 IPP – Druckprotokoll, wird genutzt um Daten zu sammeln. 135 RPC, wird genutzt um einen Windows Host mit direkt angeschlossenen Druckern zu entdecken

7) Wenn die Standard Printer MIB unterstützt wird handelt es sich um einen Netzwerkdrucker

8) Falls SNMP, aber nicht die Standard Printer MIB unterstützt wird, aber Port 9100 (oder äquivalent) unterstützt wird handelt es sich ebenfalls um einen Netzwerkdrucker.

9) Falls das Gerät auf ICMP antwortet, es sich aber nicht um einen Netzwerkdrucker handelt, prüfen Sie bitte ob es über Port 135 läuft

10) Falls es Port 135 unterstützt versuchen Sie bitte eine Verbindung mit Hilfe von WMI und den bereitgestellten Zugangsdaten

11) Wenn die Zugangsdaten funktionieren prüfen Sie bitte ob lokale Drucker oder Print Queues auf diesem Host vorhanden sind

12) Der Erfassungsprozess skaliert außerdem durch das Nutzen von verschiedenen Verbindungen, abhängig von dem Host der läuft und den Ressourcen

Erfassungsscan Timing

Die Länge der Dauer die ein Erfassungsscan in Anspruch nimmt hängt von verschiedenen Faktoren ab. Diese Faktoren sind:

1) Der Host auf welchem SiteAudit läuft und die Ressourcen dieses Hosts (Bsp.: Prozessor, Memory, Netzwerkbandbreite)

2) Anzahl der zu scannenden Netzwerkadressen

3) Netzwerkbandbreite inklusive der Bandbreite aller Netzwerke die zu scannen sind

4) Dichte der Netzwerke und Ranges die gescannt werden sollen. Bei spärlich besiedelten Netzwerken wird bedeutend mehr Zeit für den Scan in Anspruch genommen. Das liegt daran, dass hier viele Adressen nicht auf ICMP antworten was wiederum bedeutet, dass nach der Timeout Periode neue Anfragen gesendet werden, was den Scan dieser Netzwerke bedeutend verlängert.

Der Erfassungsscan ist so eingestellt, dass er in Intervallen von 7 Tagen läuft. Als Beispiel, wenn der Erfassungsscan 2 Tage benötigt um vollständig beendet zu sein wird der nächste Scan in 5

Tagen beginnen. Falls ein Erfassungscan länger als 7 Tage dauert wird der nächste Scan nach Abschluss des letzten Scans erfolgen.

Warum der Traffic minimal ist

Die SiteAudit Datensammlung kann als ein langsames, stetiges Erhalten von Paketen bezeichnet werden. Das resultiert in einer geringeren prozentualen Belastung der Bandbreite. Im Gegensatz hierzu stehen Applikationen wie Web JetAdmin die große Pakete über das Netzwerk verschicken. Als Konsequenz benötigen diese Applikationen zeitlich gesteuerte Datensammlungen, in der Regel während Zeiten der niedrigen Nutzung. Dies ist ein Unterschied im Produkt Design die zeigt was die Verfügbarkeit von Daten und die Netzwerkbelastung angeht.

Sammeln nach Daten-Typ

SiteAudit Druckerdaten beinhalten zwei Typen, unbeständige und beständige Daten. Die Standard Werte werden unten aufgelistet:

- Unbeständige Daten (Daten die sich ständig ändern können):

Zählerstände – werden jede Stunde gesammelt
Druckjobs – werden alle 4 Stunden gesammelt
Informationen zu Verbrauchsmaterial – werden alle 40 Minuten gesammelt
Alarme – es wird alle 10 Minuten nach Veränderungen nachgesehen
Schwellwerte – werden alle 30 Minuten gecheckt
Device Status – wird alle 10 Minuten gecheckt
Move Add Change – wird alle 10 Minuten gecheckt

- Beständige Daten (Daten die sich nicht ständig verändern):

Netzwerk- und Identifikationsinformationen – werden alle 7 Tage gecheckt
Konfigurationsinformationen (Input/Output Optionen) – werden alle 12 Stunden gecheckt
SiteAudit speichert auch Daten über Adressen die entdeckt werden aber keine Drucker sind.

Diese Daten beinhalten:

- SNMP Informationen, Port Informationen
- Für Windows Hosts, Hersteller/Modell//Letzter Neustart und eingeloggter User, falls konfiguriert.
- Für Windows Hosts die Printserver sind und auf welchen Queues gefunden werden sammelt SiteAudit ebenfalls Jobdaten, falls konfiguriert.

Netzwerk Traffic Volumen

Der Netzwerk Traffic hängt davon ab wieviele Devices SiteAudit überwacht. Die folgenden Faktoren sind involviert was die Kalkulation der Anzahl der Pakete angeht:

Erfassungs Traffic:

- ICMP: Zur Erfassung wird ein ICMP Paket an jede IP Adresse jedes Netzwerks welches auf der Liste steht geschickt. Falls eine Broadcast Adresse für das Netzwerk vorhanden ist wird ein ICMP Broadcast an dieses Netzwerk gesendet. Das Paket startet drei neue Versuche für Devices die nicht antworten.

- SNMP: Zur Erfassung wird ein SNMP Paket an jede IP Adresse jedes Netzwerks welches auf der Liste steht geschickt. Falls eine Broadcast Adresse für das Netzwerk vorhanden ist wird ein ICMP Broadcast an dieses Netzwerk gesendet. Das Paket startet drei neue Versuche für Devices die nicht antworten. Das Paket startet die neuen Versuche für jeden Community String in der Liste der bereitgestellten Community Strings. Dieser spezifische Paket Typ kann reduziert werden indem man von der Liste der bereitgestellten und bereits gesetzten Community Strings gewisse unnötige Community Strings entfernt.

- Port Scan: Jeder Device der auf ICMP antwortet wird Port Scan Pakete erhalten. Die Portnummern die für jeden Device gescannt werden sind: 161, 80, 8080, 9100, 1650, 631 und 135. Mit Ausnahme von Port 161, welcher ein UDP Port ist, sind alles TCP Ports. Jeder Scan startet bis zu drei neue Versuche.

Überwachung von Traffic:

- Unbeständige Daten: Hängt vom Typ des Devices sowie der Anzahl der Zähler und verfügbaren Informationen des Verbrauchsmaterials jedes Devices ab. Fortgeschrittene Devices unterstützen ca. 20 Zähler. Jeder Zähler benötigt ein Paket. In der Regel unterstützen Devices 3 – 4 Zähler. Jedes Paket besteht aus 512 Bytes. Hier gibt es keine neuen Versuche. Die Daten der Verbrauchsmaterialien ähneln denen der Zähler. Fortgeschrittene Devices unterstützen 3 – 4 Typen von Verbrauchsmaterialien und jedes Verbrauchsmaterial besitzt 6 verschiedene Informationen die dafür benötigt werden. Das heißt, es können, für fortgeschrittene Devices, 18 – 24 Pakete benötigt werden. Alarme werden in Bezug auf die Alarmtabelle abgerufen. Wenn in der Alarmtabelle keine Veränderungen erkennbar sind wird auch nichts empfangen. Die Alarmtabelle besteht aus 7 individuellen Teilen von Daten die abgerufen werden.

- Beständige Daten: In der Regel werden ca. 100 Pakete von Daten am Tag empfangen.

Lokale Drucker und Queue Daten:

- Alle diese Daten werden mit Hilfe von WMI abgefragt. WMI nutzt RPC und Windows Authentifizierung. Es werden 5 separate Anfragen vom abzufragenden Host erstellt. Die Pakete sind TCP wobei die Größe und Anzahl der Pakete abhängt von Größe der Netzwerkpakete, Art der Authentifizierung und der Anfrage die gestellt wird.

SQL Traffic:

SQL Traffic wird zum Aktualisieren der DB genutzt wenn sich Daten ändern. Dies ist TCP Traffic zum Server. SQL Traffic entsteht ebenfalls für Anfragen zwischen SiteAudit Viewer Applikationen und der Datenbank. Die Größe des Traffics hängt ab von Anzahl präsenter Devices, der maximalen Größe der Netzwerkpakete und der Art der Authentifizierung. Der Traffic findet nur zwischen Hosts, auf welchen SiteAudit läuft, und dem SQL Server statt.

Sonstiger Traffic:

Sonstiger Traffic entsteht wenn Email Benachrichtigungen generiert werden müssen. Hinzu kommen die Emails die für zeitlich gesteuerte Berichte versendet werden müssen, sofern diese genutzt werden. Email Traffic ist zum SMTP Server.

Wie Netzwerk Traffic gemessen wird

Natürlich ist es schwierig den Netzwerk Traffic zu pauschalisieren oder vorherzusehen da es immer von der jeweiligen Umgebung abhängt. Zu den variablen gehören Netzwerkkonfiguration, Device Typen, z.B. High-End MFP`s mit allen möglichen Optionen generieren mehr Meldungen als ein kleiner monochromer Arbeitsplatzdrucker. Während SiteAudit bisher keine Probleme bzgl. exzessivem Netzwerk Traffic hatte ist es wichtig dies in der Kundenumgebung zu testen. Ein einfacher Weg dies zu tun ist eine Netzwerk Analyse Applikation in einer Testumgebung laufen zu lassen um zu sehen welcher Netzwerk Traffic generiert wird.
Netaphor empfiehlt eine kostenfreie Applikation namens Wireshark zum Testen. Diese ist verfügbar unter: www.wireshark.com/

Netzwerk Traffic Beispiele

Unten finden Sie Beispiele für die Beanspruchung bzgl. Netzwerk Traffic anhand vier verschiedener Größen der Druckerflotten: 250, 1,000, 10,000 und 25,000 Drucker.

- *Geschätzter Netzwerk Traffic für 250 Drucker*

Art des Pakets	Anzahl	Bemerkung
· Erfassungspakete	40500	Anzahl Erfassungspakete/Zyklus
· Überwachungspakete	19016	Geschätzte Erfassungspakete/Stunde
· Bandbreite	9	Durchschnittl. Nutzung Bandbreite Nutzung/Stunde in MB
· Bandbreite/Sekunde	0.003	Durchschnittl. Bandbreite Nutzung/Sekunde in MB
· % Nutzung in GB Netzwerk	**0.000293**	% der Bandbreite genutzt in einem GB Netzwerk
· % Nutzung in 100MB Netzwerk	**0.003**	% der Bandbreite genutzt in einem 100MB Netzwerk

- *Geschätzter Netzwerk Traffic für 1.000 Drucker*

Art des Pakets	Anzahl	Bemerkung
· Erfassungspakete	1159200	Anzahl Erfassungspakete/Zyklus
· Überwachungspakete	75920	Geschätzte Erfassungspakete/Stunde
· Bandbreite	37	Durchschnittl. Nutzung Bandbreite Nutzung/Stunde in MB
· Bandbreite/Sekunde	0.01	Durchschnittl. Bandbreite Nutzung/Sekunde in MB
· % Nutzung in GB Netzwerk	**0.000977**	% der Bandbreite genutzt in einem GB Netzwerk
· % Nutzung in 100MB Netzwerk	**0.001**	% der Bandbreite genutzt in einem 100MB Netzwerk

- *Geschätzter Netzwerk Traffic für 10.000Drucker*

Art des Pakets	Anzahl	Bemerkung
· Erfassungspakete	5025000	Anzahl Erfassungspakete/Zyklus
· Überwachungspakete	762038	Geschätzte Erfassungspakete/Stunde
· Bandbreite	372	Durchschnittl. Nutzung Bandbreite Nutzung/Stunde in MB
· Bandbreite/Sekunde	0.103	Durchschnittl. Bandbreite Nutzung/Sekunde in MB
· % Nutzung in GB Netzwerk	**.010058594**	% der Bandbreite genutzt in einem GB Netzwerk
· % Nutzung in 100MB Netzwerk	**0.103**	% der Bandbreite genutzt in einem 100MB Netzwerk

- *Geschätzter Netzwerk Traffic für 25.000 Drucker*

Art des Pakets	Anzahl	Bemerkung
· Erfassungspakete	5025000	Anzahl Erfassungspakete/Zyklus
· Überwachungspakete	1901550	Geschätzte Erfassungspakete/Stunde
· Bandbreite	928	Durchschnittl. Nutzung Bandbreite Nutzung/Stunde in MB
· Bandbreite/Sekunde	0.258	Durchschnittl. Bandbreite Nutzung/Sekunde in MB
· % Nutzung in GB Netzwerk	**0.025195313**	% der Bandbreite genutzt in einem GB Netzwerk
· % Nutzung in 100MB Netzwerk	**0.258**	% der Bandbreite genutzt in einem 100MB Netzwerk

Anmerkung: Traffic Schätzungen basieren auf typischen Umgebungen während die Ergebnisse sich verändern können abhängend von Mix lokaler- und Netzwerkdrucker, Anzahl der Zähler, Adressen Range, Anzahl der IP Adressen und anderen Faktoren.