Artículo técnico sobre SiteAudit

Seguridad de SiteAudit OnSite

En este artículo:

octubre 2018

Descripción general de SiteAudit

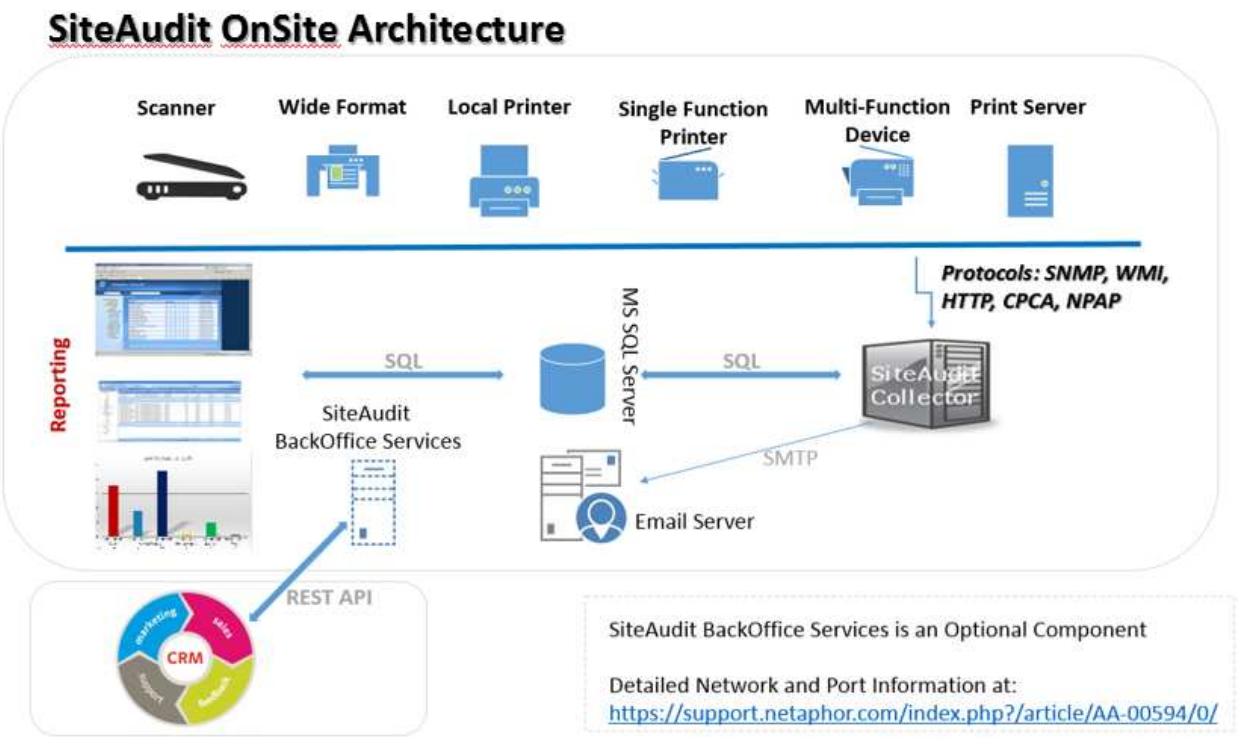
SiteAudit OnSite es una aplicación MPS para la recopilación de datos de impresoras locales y en red. Emplea un agente de recopilación de datos que se ejecuta en el cliente, así como uno o varios visores. Los datos se recopilan en el sitio del cliente y se envían a una base de datos Microsoft SQL. Ofrece una forma segura y fácil a los proveedores de MPS de recopilar y administrar la información de recuentos, suministros, errores e impresoras.

En el diagrama más abajo se representa SiteAudit OnSite y los distintos componentes.

Componentes

SiteAudit consta de los siguientes componentes principales:

- **SiteAudit Viewer**: SiteAudit Viewer se utiliza para ver, editar y personalizar informes.
- **SiteAudit Monitor:** servicio de Microsoft Windows que realiza detección de impresoras, recopilación de datos de uso y almacenamiento de los datos en una base de datos.
- **SiteAudit Reporting Website:** sitio Web instalado que utiliza IIS para proporcionar acceso a los informes.



Detección y recopilación de datos

SiteAudit realiza la detección mediante SNMP. Descubrimiento a través de SNMP v1 / v2c y con SA V6.4 o posterior SNMPv3
La detección permite tanto incluir como excluir direcciones IP:

- cada red, intervalo e IP estática incluidos en la lista determinan las direcciones en esa lista
- cada red, intervalo e IP estática excluidos determinan si se excluyen algunas de estas direcciones

El proceso de detección funciona como se describe a continuación:
1. SiteAudit realiza difusiones para buscar dispositivos y enrutadores si una dirección de difusión se incluye de forma explícita como una de las direcciones de detección.
2. SiteAudit realiza barridos de ping para buscar dispositivos de red.

SiteAudit explora los siguientes puertos para buscar impresoras:

- SNMP 161 para ver si SNMP está activado. SNMP se usa para recopilar datos
- HTTP 80 para ver si hay un servidor web incrustado. HTTP se usa para recopilar datos
- Protocolo de impresión 9100 de impresoras, que se usa para recopilar datos
- 1650 igual que 9100
- Protocolo de impresión IPP 631, que se usa para recopilar datos
- RPC 135, que se usa para detectar un host Windows para impresoras locales
- Además, también se pueden usar los puertos para CPCA y NPAP si la impresora admite estos protocolos
- 47545 (CPCA) y 9300 (NPAP) también se pueden usar si la impresora admite esos protocolos
- Puertos 21 (FTP) y 23 (Telnet) para identificar una vulnerabilidad de seguridad potencial

Para reducir al mínimo el tráfico de red, los datos se recopilan por tipo y en intervalos configurables. Lea más información sobre la detección y recopilación de datos en https://support.netaphor.com/index.php?/article/AA-00594. Lea más información sobre la detección DNS en https://support.netaphor.com/index.php?/article/AA-00391/0/.

Windows Firewall

Si Windows Firewall está activado, se debe configurar de modo que permita el acceso de SiteAudit a RIP, ICMP, SNMP, SQL Server y los hosts remotos de las impresoras conectadas directamente. En los hosts remotos a los que SiteAudit tiene acceso, Windows Firewall debe permitir la entrada de los paquetes correspondientes y la salida de respuestas. Al activar "Supervisión remota" se permiten todos los accesos de firewall que SiteAudit necesita en un host remoto.

El acceso al puerto TCP 135 se debe activar en el host de SiteAudit Monitor y en todos los PC Windows de destino.

Impresoras de conexión directa (locales)

SiteAudit busca las impresoras conectadas directamente (con conexiones USB o en paralelo) a un host Windows. Para tener acceso al host, SiteAudit necesita las credenciales de un usuario que sea administrador en ese host. Para asegurarse de que la detección se realiza correctamente, debe:

- Proporcionar una credencial que funcione en todos los hosts
- Asegurarse de que estas credenciales NO se bloquean después de una serie de intentos fallidos
- Ejecutar los informes "Unauthenticated Hosts" para ver los hosts que no permitieron el acceso y agregar las credenciales para esos hosts

Credenciales

SiteAudit necesita credenciales en cuatro instancias:

- La instalación de SiteAudit en un servidor o en una estación de trabajo requiere una cuenta local que se ejecute como un servicio.
- La instalación de la base de datos SQL Server o SQL Server Express requiere una contraseña SA (administrador del sistema) o, en caso de utilizarse seguridad integrada, las credenciales de inicio de sesión de un usuario que tenga acceso de administrador a la base de datos.
- Para la detección de las impresoras conectadas directamente, credenciales del administrador de Windows en los hosts con impresoras conectadas.
- La detección de impresoras directas con WMI requiere una cuenta que disponga de permisos completos en el espacio de nombres ROOT WMI.
- Para el descubrimiento de SNMPv3

SiteAudit almacena todas las contraseñas en Windows Protected Storage y solo se puede descifrar en la máquina donde se ingresaron. Si el DCA se mueve a una nueva máquina, estas contraseñas deben reingresarse en esta máquina.

Datos recopilados

Los datos recopilados consisten en información de activos de impresora, contadores, suministros e información de errores. Abajo se muestra un ejemplo de los datos recopilados.

Información de activos
Fabricante
Modelo
Dirección IP
Nombre de impresora
N.º de producto
N.º de serie
Etiqueta de activo
Ubicación
Dirección MAC de impresora
Dirección MAC de host

Suministros
Nivel restante de suministros (%)
Nivel de suministro original
% de suministros usados
Fecha detección de tóner
Fecha de sustitución
Descripción de suministros
Tipo de suministros
N.º de pieza de suministros
N.º de serie de suministros
Fecha instalación de suministros

Contadores
Total de páginas
Total en B/N
Impresión en B/N
Copia en B/N
B/N grande
Total en color
Impresión en color
Copia en color
Color grande
Grande
Pequeño
Copias
Impresione
Fax
Escaneado

Errores
Código de alerta
Nivel de gravedad
Nivel de formación
Estado
Estado de resolución
Descripción del incidente
Duración del incidente
Inicio y fin del incidente

Errores (continuación)
Acuerdo de nivel de servicio
Contacto
Total de errores
Tiempo de actividad (%)
Última comunicación correcta
Última notificación
Estado del dispositivo (Listo/Error/Advertencia)
Tiempo de respuesta

No se almacenan datos de tarjetas de crédito ni datos personales. Es posible recopilar datos de los trabajos si SiteAudit se configura para recopilar esta información. De forma predeterminada, esta función está desactivada. Para configurar esta función, se necesita una credencial de administrador local con acceso a las estaciones de trabajo de destino. Para ver una lista completa de los datos, consulte https://support.netaphor.com/index.php?/article/AA-00779/104/

Tráfico de red

La recopilación de datos de SiteAudit puede caracterizarse por ser una *recepción de paquetes constante y lenta*, lo que conlleva un porcentaje inferior de uso del ancho de banda de red. El tráfico de red depende del número de dispositivos que SiteAudit supervisa. Abajo se incluyen ejemplos de la cantidad de tráfico de red usada por tres diferentes tamaños de conjuntos de equipos: 250, 1.000 y 10.000 impresoras.

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

Las estimaciones del tráfico se basan en un entorno típico, pero los resultados pueden variar según la combinación de impresoras locales y en red, el número de contadores, el espacio de dirección, el número de direcciones IP y otros factores.
Lea más información sobre el tráfico de red en https://support.netaphor.com/index.php?/article/AA-00594

Preguntas comunes sobre la recopilación de datos

Recopilación de datos del dispositivo: solo se recopilan los datos del dispositivo. La información del usuario no se recopila desde un dispositivo. La información, como las cuentas de usuario en el dispositivo para Follow Me Printing o la impresión segura o la lista de trabajos en dispositivos, no se recopila

1. SiteAudit no recopila ni almacena información de identificación personal (PII), como contraseñas de usuario, información de tarjetas de crédito, SSN, etc.

2. La recopilación de datos de trabajo es opcional. Estos datos se recopilan desde la Cola de Windows, pero el usuario debe habilitarlos para permitir esto.

3. Los datos se almacenan en un servidor SQL: el cliente controla el servidor SQL en un entorno SiteAudit OnSite y, opcionalmente, puede decidir que los datos en el servidor estén encriptados.

4. Comunicación externa: fuera del firewall: esto está bajo el control del cliente. La única comunicación externa es a través de correo electrónico de notificación o informes programados. El cliente puede controlar qué notificaciones se envían y a quién. Lo mismo es cierto para los informes programados.

Netaphor Software Inc.

SiteAudit Onsite se lanzó en octubre de 2006 y se vende a clientes en más de 50 países.

Fundada en 1997 y con sede central en Irvine, California (EE.UU.), Netaphor Software, Inc. (www.netaphor.com) desarrolla y vende herramientas de administración de activos que ayudan a las empresas a controlar los costes de las impresoras y mejorar el servicio. El producto estrella de la empresa, SiteAudit, es una solución de software, líder en el segmento de empresas y mercado medio, para identificar y administrar los costes y el servicio; con el uso de esta solución, las empresas consiguen un ahorro de hasta el 30 por ciento durante la vida útil de los activos de impresora. Netaphor SiteAudit 5.0 y 6.0 han ganado los premios Winter 2012 y Winter 2015 "Pick" por ser unas soluciones de administración del conjunto de equipos sobresalientes (Outstanding Fleet Management Solution), premio concedido por los editores de Buyers Laboratory Inc LLC (BLI).