Artículo técnico sobre SiteAudit

Seguridad de SiteAudit Hosted

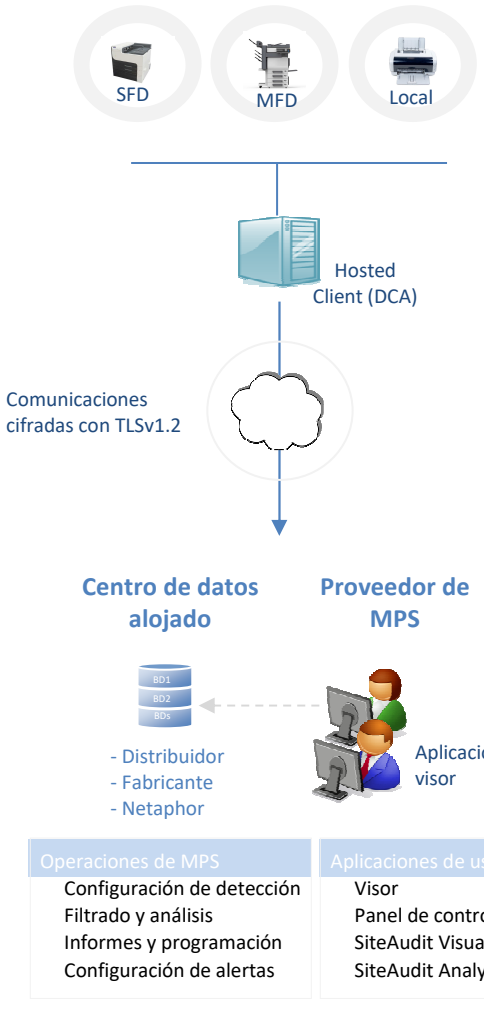
En este artículo:

Septiembre 2018

Descripción general de SiteAudit

SiteAudit Hosted es una aplicación MPS para la recopilación remota de datos de impresoras locales y en red. Emplea un Hosted Client (agente de recopilación de datos--DCA) que se ejecuta en el cliente, así como uno o varios visores que se ejecutan en el proveedor de MPS. Los datos se recopilan en el sitio del cliente y se envían a una base de datos SQL mediante transporte seguro. Ofrece una forma segura y fácil a los proveedores de MPS de recopilar y administrar la información de recuentos, suministros, errores e impresoras.

Configuración de SiteAudit Hosted



Operaciones de MPS	Aplicaciones de usuario
Configuración de detección	Visor
Filtrado y análisis	Panel de controles
Informes y programación	SiteAudit Visualizer
Configuración de alertas	SiteAudit Analyzer

Sitio del cliente - Hosted Client (DCA)

Implementación – Agente de recopilación de datos (DCA)

Edición de 32 o 64 bits de Windows 8.1/10 o Server 2012/R2 y 2016
.NET 4.5.1 o superior
SiteAudit Hosted Client (DCA)
Archivo de clave de conexión de Hosted Client (DCA)
Privilegios de administrador en Control de cuentas de usuario (CCU)

Detección y recopilación de datos

Detección: SNMP v1/v2c/SNMPv3
Recopilación de datos: SNMP, HTTP, NPAP, CPCA y WMI; cuenta de administrador local o del dominio para impresoras locales

- Puertos analizados: 161, 1650, 9100, 80, 8080, 631, 9300, 47545, 21, 23

Opciones de transporte de datos a la base de datos alojada

- Puerto TCP 443 - REST sobre HTTPS

Proveedor de MPS – Visor alojado

Implementación – Visor de MPS

Edición de 32 o 64 bits de Windows 8.1/10 o Server 2012/R2 y 2016
.NET 4.5.1 o superior
Licencia de SiteAudit Viewer o de Viewer Admin
Archivo de clave de conexión de Hosted Client (DCA)
Privilegios de administrador en Control de cuentas de usuario (CCU)

Conexión del visor a la base de datos alojada

- Puerto TCP 443 - REST sobre HTTPS
- Licencia de administrador o visor alojado de SiteAudit

Comunicación de datos

SiteAudit Hosted Client (DCA) es un recopilador de datos. Toda la comunicación se cifra antes de transmitirse a la base de datos alojada. Para todas las comunicaciones con la base de datos SQL alojada, se usa cifrado asimétrico que está certificado con un certificado SSL de como mínimo 4.096 bits emitido por una autoridad de certificados (CA) de confianza, como DigiCert™ o VeriSign® (Symantec). La transmisión de datos es a través de REST.

Tanto el Hosted Client (DCA) como los visores del proveedor de MPS solo pueden conectarse a la base de datos alojada si tienen un visor con licencia y un archivo de clave para tener acceso a la base de datos alojada.

Activación del Hosted Client (DCA)

La aplicación Netaphor Hosted Server gestiona la activación del Hosted Client. Antes de la instalación, se crea una licencia mediante un archivo de licencia de conexión que contiene una cadena de conexión cifrada y una clave compartida (longitud de 64 bits) que sirve para cifrar los datos entre el Hosted Client (DCA) y la base de datos alojada. La aplicación utiliza un transporte REST para la comunicación de datos.

Las licencias pueden tener una fecha de caducidad o se pueden revocar para desactivar el Hosted Client (DCA). Una vez que el Hosted Client (DCA) tiene el archivo de clave y se instala, almacena la clave compartida en el espacio de almacenamiento protegido de Windows de esa máquina. Los datos no se pueden recopilar ni ver sin un archivo de clave válido ni tampoco se puede tener acceso a los mismos desde otra máquina. El Hosted Client (DCA) no proporciona acceso al nombre de la base de datos, al nombre de usuario o la contraseña del cliente.

Detección y recopilación de datos

SiteAudit detecta los activos de impresora. El proceso de detección funciona como se describe a continuación. Descubrimiento sobre SNMP v1/v2c/v3:

- 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

SiteAudit busca dispositivos en los siguientes puertos:

- 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/

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.

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.

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

Lea más información sobre el tráfico de red en https://support.netaphor.com/index.php?/article/AA-00594

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
Impresiones
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)
Nombre de 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 Hosted 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/

Credenciales de inicio de sesión

SiteAudit requiere credenciales en los siguientes casos:

- Para el descubrimiento de impresoras conectadas directamente, las credenciales de administrador de Windows para los hosts con impresoras adjuntas.
- El descubrimiento directo de impresoras mediante WMI requiere una cuenta que tenga permisos completos para 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.

Common Questions about Data Collection

- 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
- SiteAudit no recopila ni almacena información de identificación personal (PII), como contraseñas de usuario, información de tarjetas de crédito, SSN, etc.
- La recopilación de datos de trabajo es opcional. La cola debe ser habilitada por el usuario para permitir esto
- Servidor SQL: el cliente controla el servidor SQL en un entorno de SiteAudit OnSite y puede cifrarse
- Comunicación externa: fuera del firewall: 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.

Resumen

La arquitectura de SiteAudit Hosted usa el mecanismo de seguridad apropiado para garantizar la protección de los datos de impresora; para ello, emplea mecanismos de transporte TLSv1.2, archivos de clave cifrados y servidores alojados seguros que están certificados por CA de confianza.

Netaphor Software Inc.

SiteAudit Hosted se lanzó en octubre de 2011 y se vende a clientes en más de 30 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 SiteAudit5.0 ha ganado el premio Winter 2012 "Pick" por ser una solución de administración del conjunto de equipos sobresaliente (Outstanding Fleet Management Solution), premio concedido por los editores de Buyers Laboratory Inc LLC (BLI).