Article technique SiteAudit

Sécurité SiteAudit Hosted

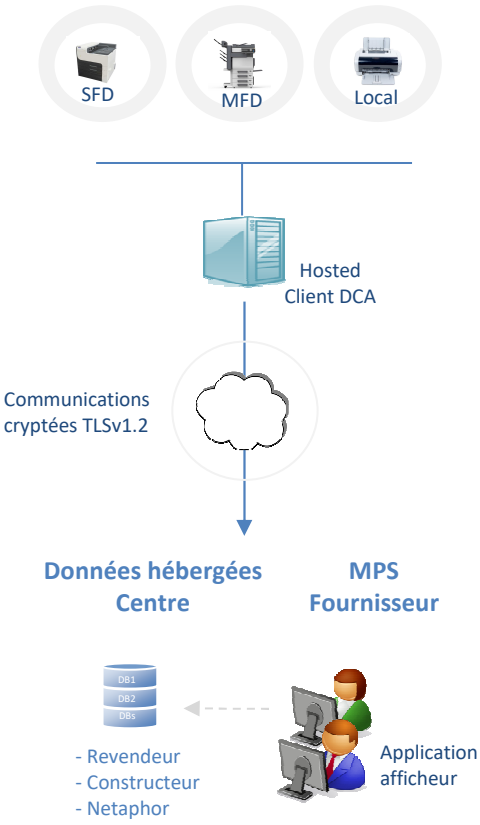
Dans cet article :

Septembre 2018

Aperçu de SiteAudit

SiteAudit Hosted est une application MPS pour la collecte à distance des données d'imprimantes locales et en réseau. Elle utilise un Hosted Client (agent de collecte de données--DCA) qui s'exécute chez le client et un ou plusieurs afficheurs qui s'exécutent chez le fournisseur MPS. Les données sont collectées sur le site du client et envoyées par transport sécurisé vers une base de données SQL. Les fournisseurs MPS obtiennent ainsi un moyen sûr et simple de collecter et de gérer les comptes, les fournitures, les erreurs et les informations sur les imprimantes.

Configuration de SiteAudit Hosted



Site du client - Hosted Client (DCA)

Déploiement – Agent de collecte de données (DCA)

- Windows 8.1/10 32 bit ou 64 bit ou Server 2012/R2 et 2016
- .NET 4.5.1 ou version ultérieure
- Client SiteAudit Hosted (DCA)
- Fichier clé de connexion Hosted Client (DCA)
- Privilèges d'administrateur pour le contrôle de compte d'utilisateur (UAC)

Découverte et collecte des données

- Découverte SNMP v1/v2/v3
- Collecte de données SNMP, HTTP, NPAP, CPCA et WMI ; compte administrateur local ou de domaine pour les imprimantes locales
- Ports analysés : 161, 1650, 9100, 8080, 80, 631, 135, 47545, 21, 23

Options de transport des données vers la base de données hébergée

- Port TCP 443 - REST sur HTTPS

Fournisseur MPS – Afficheur hébergé

Déploiement – Afficheur MPS

- Windows 8.1/10 32 bit ou 64 bit ou Server 2012/R2 et 2016
- .NET4.5.1 ou version ultérieure
- Licence SiteAudit Viewer ou licence Viewer Admin
- Fichier clé de connexion Hosted Client (DCA)
- Privilèges d'administrateur pour le contrôle de compte d'utilisateur (UAC)

Connexion de la visionneuse à la base de données hébergée

- Port TCP 443 - REST sur HTTPS
- SiteAudit Hosted Administrator ou Viewer license

Opérations MPS

- Configuration de découverte
- Filtrage et analyse
- Création de rapport et planification
- Configuration d'alerte

Applications utilisateur

- Afficheur
- Tableau de bord
- SiteAudit Visualizer
- SiteAudit Analyzer

Communication des données

Le SiteAudit Hosted Client (DCA) est un collecteur de données. Toutes les communications sont cryptées avant la transmission à la base de données hébergée. Un cryptage asymétrique est utilisé et il est certifié par un certificat SLL de 4096 bit minimum fourni par une autorité de certification (CA) de confiance comme DigiCert™ ou VeriSign® (Symantec) pour toutes les communications avec la base de données SQL hébergée. La transmission des données se fait via REST.

Le Hosted Client (DCA) et le ou les afficheurs du fournisseur MPS peuvent uniquement se connecter à la base de données hébergée s'ils disposent d'un afficheur avec licence et d'un fichier clé avec accès à la base de données hébergée.

Activation de Hosted Client (DCA)

L'activation de Hosted Client est gérée par l'application Netaphor Hosted Server. Avant l'installation, une licence de fichier clé de connexion est créée et contient une chaîne de connexion cryptée ainsi qu'une clé partagée (d'une longueur de 64 octets) utilisée pour crypter les données entre le Hosted Client (DCA) et la base de données hébergée. L'application utilise un transport REST pour la communication de données.

Les licences peuvent avoir une date d'expiration ou peuvent être retirées pour désactiver le Hosted Client (DCA). Lorsque le Hosted Client (DCA) possède le fichier clé et qu'il est installé, il stocke la clé partagée dans le stockage protégé de Windows sur cette machine. Les données ne peuvent pas être collectées ni consultées dans un fichier clé valide et ne sont accessibles sur aucune autre machine. Le Hosted Client (DCA) ne fournit pas l'accès au nom de la base de données du client, au nom d'utilisateur ou au mot de passe.

Découverte et collecte des données

SiteAudit découvre les ressources d'imprimante. Le processus de découverte fonctionne comme suit :

- chaque réseau, plage, IP fixe inclus dans la liste détermine les adresses dans cette liste
- chaque réseau, plage, IP fixe exclu détermine si l'une de ces adresses est exclue

SiteAudit analyse des machines sur les ports suivants :

- 161 SNMP pour vérifier si SNMP est activé. SNMP est utilisé pour collecter les données
- 80 HTTP pour vérifier si un serveur web intégré est présent. HTTP est utilisé pour collecter les données
- Protocole d'impression 9100 pour les imprimantes, utilisé pour collecter les données
- 1650, identique à 9100
- Protocole d'impression 631 IPP, utilisé pour collecter les données.
- 135 RPC, utilisé pour détecter un hôte Windows pour les imprimantes locales
- En outre, les ports pour CPCA et NPAP peuvent aussi être utilisés si l'imprimante prend en charge ces protocoles
- 47545 (CPCA) et 9300 (NPAP) peuvent également être utilisés si l'imprimante prend en charge ces protocoles.
- Ports 21 (FTP) et 23 (Telnet) pour identifier une faille de sécurité potentielle

Pour réduire le trafic sur le réseau, les données sont collectées par type et selon des intervalles configurables. Pour en savoir plus sur la découverte et la collecte de données, consultez https://support.netaphor.com/index.php?/article/AA-00594 Pour en savoir plus sur la découverte DNS, consultez https://support.netaphor.com/index.php?/article/AA-00391/0/

Trafic réseau

La collecte de données par SiteAudit peut être caractérisée comme une *réception lente et régulière de paquets*. Cela permet de consommer un plus petit pourcentage de la bande passante du réseau. Le trafic réseau dépend du nombre de machines que SiteAudit surveille. Voici quelques exemples de quantité de trafic réseau employés par trois tailles de parc différentes : 250, 1000 et 10 000 imprimantes.

Les estimations du trafic se basent sur un environnement type, mais les résultats peuvent varier selon le mélange d'imprimantes locales et en réseau, du nombre de compteurs, de l'espace d'adresse, du nombre d'adresses IP et d'autres facteurs.

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

Pour en savoir plus sur le trafic réseau, consultez https://support.netaphor.com/index.php?/article/AA-00594

Données collectées

Les données collectées se composent d'informations sur les ressources d'imprimante, d'informations sur les compteurs, les fournitures et les erreurs. Voici un exemple des données collectées.

Informations sur les ressources
Constructeur
Modèle
Adresse IP
Nom imprimante
Numéro produit
Numéro de série
Étiquette ressource
Emplacement
Adresse MAC imprimante
Adresse MAC hôte

Fournitures
Niveau de fournitures restant %
Niveau fourniture original
Pourcentage de fournitures utilisées
Date détection toner
Date de remplacement
Description fournitures
Type fournitures
Référence fournitures
Numéro de série fournitures
Date d'installation fournitures

Compteurs
Total pages
N/B tout
Impression N/B
Copie N/B
N/B grand
Couleur tout
Impression couleur
Copie couleur
Couleur grand
Grand
Petit
Copies
Impressions
Fax
Numérisations

Erreurs
Code alerte
Niveau gravité
Niveau formation
État
État résolution
Description incident
Durée incident
Début et fin incident

Erreurs (suite)
Nom accord de niveau de service
Contact
Total erreurs
Temps de fonctionnement %
Dernière communication réussie
Dernière notification
État machine (prête/erreur/avertissement)
Temps de réponse

Aucune donnée de carte de crédit ou personnelle n'est stockée. Les données de travaux peuvent être collectées si SiteAudit Hosted est configuré pour collecter ces informations. Cette fonctionnalité est désactivée par défaut. Des identifiants d'administrateur local avec accès aux postes de travail cibles sont nécessaires pour configurer cette fonctionnalité. Pour une liste complète de données, voir https://support.netaphor.com/index.php?/article/AA-00779/104/

Connectez-vous sur les informations d'identification

SiteAudit requiert des informations d'identification dans les cas suivants:

- Pour la découverte d'imprimantes directement connectées, identifiants de l'administrateur Windows pour les hôtes avec imprimantes connectées.
- La découverte directe d'imprimantes à l'aide de WMI nécessite un compte disposant de toutes les autorisations pour l'espace de noms ROOT WMI.
- Pour la découverte SNMPv3

SiteAudit stocke tous les mots de passe dans Windows Protected Storage et ne peut être déchiffré que sur la machine sur laquelle ils ont été entrés. Si le DCA est déplacé vers une nouvelle machine, ces mots de passe doivent être ressaisis sur cette machine.

Common Questions about Data Collection

- Collecte des données de périphérique: seules les données de périphérique sont collectées. Les informations utilisateur ne sont pas collectées à partir d'un périphérique. Les informations, telles que les comptes d'utilisateur sur le périphérique pour l'impression Follow Me ou l'impression sécurisée ou la liste des tâches sur les périphériques, ne sont pas collectées
- Aucune information d'identification personnelle (PII), telle que les mots de passe des utilisateurs, les informations de carte de crédit, le SSN, etc., n'est collectée ou stockée par SiteAudit.
- La collecte des données de travail est facultative. Le spouleur doit être activé par l'utilisateur pour permettre cette
- SQL Server: le client contrôle le serveur SQL dans un environnement SiteAudit OnSite et peut être chiffré.
- Communication externe - en dehors du pare-feu: elle est sous le contrôle du client. La seule communication externe se fait par courrier électronique de notification ou par rapports programmés. Le client peut contrôler quelles notifications sont envoyées et à qui. Il en va de même pour les rapports planifiés

Récapitulatif
En utilisant des mécanismes de transport TLSv1.2, des fichiers clés cryptés et des serveurs hébergés sécurisés certifiés par des CA de confiance, les mécanismes de sécurité appropriés sont utilisés par l'architecture de SiteAudit Hosted pour garantir la protection des données de l'imprimante.

Netaphor Software Inc.

SiteAudit Hosted a été lancé en octobre 2011 et ses ventes couvrent plus de 30 pays.

Fondée en 1997 et implantée à Irvine, Californie, Netaphor Software, Inc. (www.netaphor.com) développe et commercialise des outils de gestion de ressources qui aident les sociétés à contrôler les coûts d'impression et à améliorer le service. SiteAudit, produit phare de la société, est la solution logicielle leader sur le segment du marché intermédiaire et entreprise pour identifier et gérer les coûts et les services, permettant aux organisations d'économiser jusqu'à 30 % durant le cycle de vie des ressources d'imprimante. Netaphor SiteAudit 5.0 est le gagnant du prix Winter 2012 Pick en qualité de solution de gestion de parc exceptionnelle décerné par les rédacteurs de Buyers Laboratory Inc LLC (BLI).