Article technique SiteAudit

Sécurité SiteAudit OnSite

Dans cet article :

Novembre 2018

Aperçu de SiteAudit

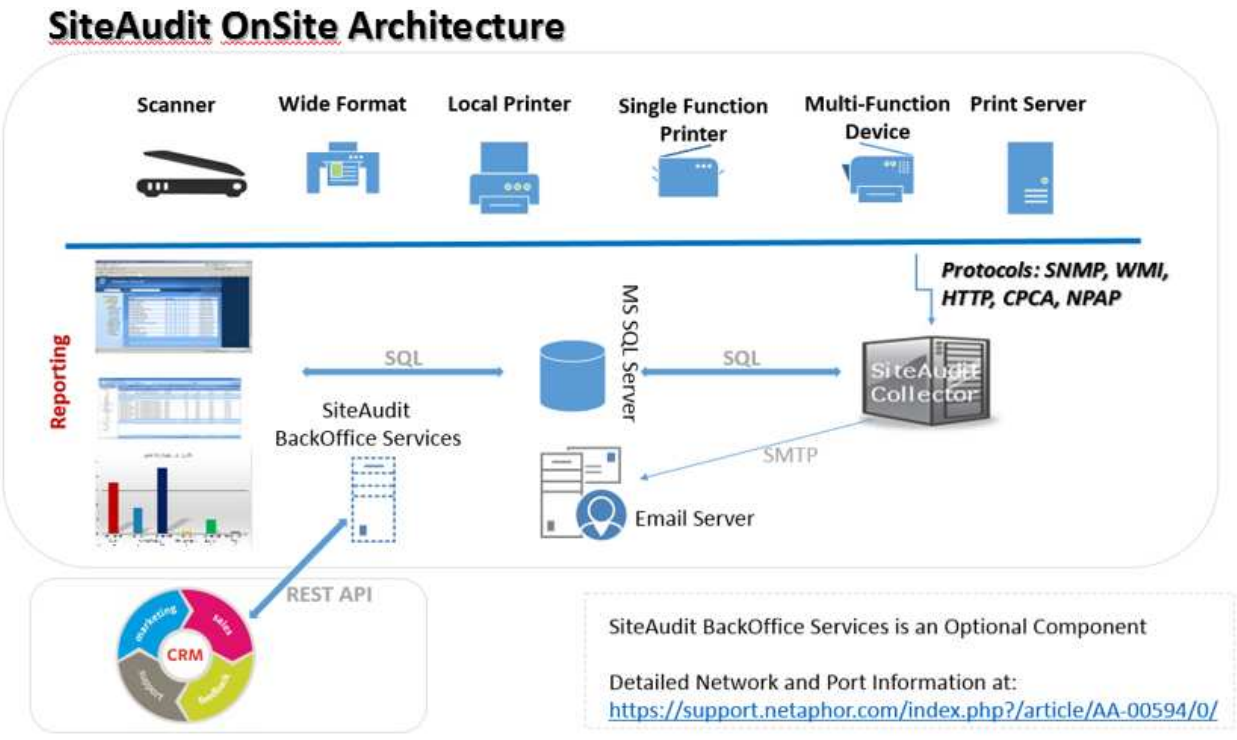
SiteAudit OnSite est une application MPS pour la collecte des données d'imprimantes locales et en réseau. Elle utilise un agent de collecte de données qui s'exécute chez le client et un ou plusieurs afficheurs. Les données sont collectées sur le site du client et envoyées vers une base de données Microsoft 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.

Le diagramme suivant représente SiteAudit OnSite et ses différents composants

Composants

SiteAudit comprend les composants principaux suivants :

- **SiteAudit Viewer** –SiteAudit Viewer est utilisé pour afficher, modifier et personnaliser les rapports
- **SiteAudit Monitor** – service Microsoft Windows qui effectue la découverte d'imprimante, collecte les données d'utilisation et stocke les données dans une base de données
- **SiteAudit Reporting Website** – site web installé utilisant IIS pour fournir l'accès aux rapports



Découverte et collecte des données

SiteAudit effectue une découverte en utilisant SNMP. Discovery via SNMP v1 / v2c et SA V6.4 ou version ultérieure SNMPv3
La découverte permet à la fois l'inclusion et l'exclusion d'adresses IP.

- 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

Le processus de découverte fonctionne comme suit :

1. SiteAudit effectue des diffusions pour trouver les machines et routeurs si une adresse de diffusion est explicitement incluse en tant qu'une des adresses de découverte.
2. SiteAudit effectue un balayage de ping pour trouver les machines en réseau

SiteAudit analyse les ports suivants pour trouver les imprimantes :

- 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
- 47545 (CPCA) et 9300 (NPAP) peuvent aussi 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/

Pare-feu Windows

Si le pare-feu Windows est activé, il doit être configuré pour permettre à SiteAudit d'accéder à RIP, ICMP, SNMP, serveur SQL et aux hôtes distants pour les imprimantes connectées directement. Sur les hôtes distants auxquels accède SiteAudit, le pare-feu Windows doit autoriser l'entrée des paquets correspondants et la sortie des réponses. L'activation de la « surveillance à distance » permet tous les accès au pare-feu dont à besoin SiteAudit sur un hôte distant.

L'accès au port TCP 135 doit être activé sur la machine hôte SiteAudit Monitor et sur tous les ordinateurs Windows cibles.

Imprimante connectée directement (locale)

SiteAudit détecte les imprimantes connectées directement (via connexions USB ou parallèle) à un hôte Windows. Pour accéder à l'hôte, SiteAudit a besoin des identifiants d'un utilisateur qui est un administrateur sur cet hôte. Pour vous assurer que la découverte réussisse, vous devez :

- Fournir des identifiants qui fonctionneront sur tous les hôtes
- Assurer que ces identifiants ne sont PAS verrouillés après un certain nombre de tentatives échouées
- Exécuter les rapports « Unauthenticated Hosts » pour voir quels sont les hôtes qui n'autorisent pas l'accès et ajouter les identifiants pour ces hôtes

Identifiants

SiteAudit a besoin d'identifiants dans quatre cas :

- Installation de SiteAudit sur un serveur ou un poste de travail qui nécessite un compte local exécuté en tant que service.
- Installation de la base de données SQL Server ou SQL Server Express nécessitant un mot de passe d'administrateur système (SA) ou, si la sécurité intégrée est utilisée, les identifiants de connexion d'une personne ayant un accès à la base de données au niveau administrateur
- Pour la découverte d'imprimantes connectées directement, les identifiants d'administrateur Windows pour les hôtes avec imprimantes raccordées.
- La découverte d'imprimante directe en utilisant WMI nécessite un compte ayant des autorisations complètes à l'espace de noms ROOT WMI.
- Également pour la découverte SNMPv3

SiteAudit stocke tous les mots de passe dans Windows Protected Storage et ils ne peuvent être déchiffrés que sur la machine sur laquelle ils ont été saisis. Si le DCA est déplacé vers une nouvelle machine, ces mots de passe doivent être saisis à nouveau sur cette machine.

Sécurité de l'accès

- Les utilisateurs ont accès aux données de SiteAudit stockées dans une base de données MS SQL Server à l'aide de leurs comptes Windows ou alternativement, via un compte MS SQL Server. L'accès permettant d'exécuter l'application SiteAudit est attribué via la connexion Active Directory.
- La sécurité fonctionnelle Netaphor SiteAudit est facultative et est conçue pour contrôler l'accès à diverses fonctions de SiteAudit. Le contrôle est maintenu en affectant des rôles à des utilisateurs, comme un administrateur Windows attribue des rôles à des utilisateurs pour autoriser ou refuser des fonctionnalités sur un ordinateur Windows. Les rôles SiteAudit sont définis et gérés dans la base de données SQL Server utilisée par SiteAudit. L'accès est attribué par l'administrateur système/bade de données.
- Les utilisateurs sont authentifiés à l'aide du mécanisme utilisé pour se connecter. Le compte Active Directory est utilisé avec la sécurité intégrée et un nom d'utilisateur/mot de passe est utilisé avec un compte SQL
- Aucun contrôle d'accès séparé n'est maintenu par l'application. L'accès s'effectue soit via Active Directory, soit via des comptes SQL Server.
- Les identifications d'utilisateur ne sont pas utilisées en dehors du réseau client.

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

Accès SNMP

Le protocole SNMP inclut une disposition pour le contrôle d'accès en utilisant des chaînes de « communauté ». Une chaîne de communauté est requise pour accéder à une machine. SiteAudit entretient une liste de chaînes de communauté qu'il utilise pour tenter d'accéder aux données SNMP provenant d'une machine.

La liste est ordonnée et SiteAudit essaye chaque chaîne tour à tour jusqu'à ce que l'une d'elle réussisse ou jusqu'à ce qu'il n'y ait plus de chaîne à essayer. La liste est pré-remplie (avec un jeu de chaînes de communauté couramment utilisées) mais un utilisateur peut retirer ou ajouter des chaînes et peut modifier l'ordre dans lequel les chaînes sont essayées.

Certains agents SNMP au sein d'une machine peuvent être configurés pour générer des interruptions « Échec d'authentification » lorsqu'une chaîne de communauté est utilisée et n'est pas valide pour cette machine. Pour éviter d'obtenir ces interruptions d'échec d'authentification, vous devez :

- Assurer que la liste des chaînes de communauté ne contient que les chaînes nécessaires
- Ignorer les interruptions d'échec d'authentification si elles indiquent que la source de la requête (l'application qui envoie le message avec la chaîne de communauté invalide) est SiteAudit
- Désactiver les interruptions d'échec d'authentification sur la machine

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	**Fournitures**	**Compteurs**
Constructeur	Niveau de fournitures restant %	Total pages
Modèle	Niveau fourniture original	N/B tout
Adresse IP	Pourcentage de fournitures utilisées	Impression N/B
Nom imprimante	Date détection toner	Copie N/B
Numéro produit	Date de remplacement	N/B grand
Numéro de série	Description fournitures	Couleur tout
Étiquette ressource	Type fournitures	Impression couleur
Emplacement	Référence fournitures	Copie couleur
Adresse MAC imprimante	Numéro de série fournitures	Couleur grand
Adresse MAC hôte	Date d'installation fournitures	Grand
		Petit
Erreurs	**Erreurs (suite)**	Copies
Code alerte	Nom accord de niveau de service	Impressions
Niveau gravité	Contact	Fax
Niveau formation	Total erreurs	Numérisations
État	Temps de fonctionnement %	
État résolution	Dernière communication réussie	
Description incident	Dernière notification	
Durée incident	État machine (prête/erreur/avertissement)	
Début et fin incident	Temps de réponse	

Aucune donnée de carte de crédit ou personnelle n'est stockée. Les données de travaux peuvent être collectées si SiteAudit 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/

Questions courantes sur la collecte de données

- Collecte de données de périphérique : Seules les données du 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 personnellement identifiable (PII), telle que les mots de passe des utilisateurs, les informations de carte de crédit, le numéro de sécurité sociale, etc. n'est collectée ou stockée par SiteAudit.
- La collecte des données de travail est facultative. Ces données sont collectées à partir du spouleur Windows mais doivent être activées par l'utilisateur pour permettre cette opération.
- Les données sont stockées sur un serveur SQL : Le client contrôle le serveur SQL dans un environnement SiteAudit OnSite et peut éventuellement décider de chiffrer les données sur le serveur.
- Communication externe – en dehors du pare-feu : elle est sous le contrôle du client. La seule communication externe se fait par e-mail de notification ou par rapports programmés. Le client peut contrôler quelles sont les notifications envoyées et à qui. Il en est de même pour les rapports planifiés

Netaphor Software Inc.

SiteAudit OnSite a été lancé en octobre 2006 et ses ventes couvrent plus de 40 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 et 6.0 est le gagnant du prix Winter 2012 et 2015 Pick en qualité de solution de gestion de parc exceptionnelle décerné par les rédacteurs de Buyers Laboratory Inc LLC (BLI).