Le trafic du Windows 7/des clients de vista affiche le poste de travail au lieu de l'utilisateur dans les logs d'Access

Contenu

Question

Pourquoi le trafic des clients de Windows 7/vista affiche-t-il le poste de travail au lieu de l'utilisateur dans les logs d'accès ?

Environnement

Microsoft Windows 7, Microsoft Windows Vista, appliance de sécurité Web de Cisco (toutes les versions), type de remplacement : Adresse IP

Symptômes

Certaines lignes de log dans les logs d'accès affichent le nom d'ordinateur d'ordinateurs, au lieu du DOMAINE \ de UTILISATEUR.

Microsoft a introduit une nouvelle caractéristique dans le Windows 7 et les Windows Vista ont appelé le « indicateur d'état de connexion réseau » (NCSI), qui révèle comme petite icône de monde entier qui apparaît au-dessus de l'icône d'interface réseau dans la barre d'état système. Juste après la procédure de connexion, cette caractéristique tentera d'inviter des données de l'Internet afin de savoir s'il y a de connexion Internet.

Il y a des problèmes connus avec NCSI, où il enverra des qualifications d'ordinateur au lieu des identifiants utilisateurs quand l'authentification NTLM est exigée.

Puisque NCSI est le plus susceptible d'envoyer la première demande d'un PC au WSA, ne substituez non existe pourtant et un nouveau substitut basé sur IP avec le nom d'ordinateur au lieu du nom d'utilisateur réel est créé. Ce substitut est utilisé pour chaque demande de l'adresse IP initiale jusqu'aux temps de remplacement et l'utilisateur doit authentifier à nouveau, cette fois avec de vraies qualifications.

Puisque le nom d'ordinateur n'est pas le plus probablement un membre du groupe au commencement destiné d'AD toutes les demandes ne déclencheront pas Access/stratégie corrects de déchiffrement, parfois ayant pour résultat la demande étant bloquée.

Pour plus d'informations sur NCSI, voyez s'il vous plaît l'article suivant de KB Microsoft.

Veuillez voir les instructions ci-dessous au contournement la question :

1. Lancez Registry Editor en recherchant le « regedit » du menu de tâche. Vous devez cliquer avec le bouton droit et sélectionner le « passage comme administrateur ».

2. Naviguez vers : HKEY_LOCAL_MACHINE \ SYSTÈME \ CurrentControlSet \ services \ NlaSvc \ paramètres \ Internet

3. Sous la clé d'Internet, le double clic « EnableActiveProbing », et puis dans des données de valeur, type : **0**.
4. Clic « CORRECT ».

5. Redémarrez l'ordinateur.

Ces modifications peuvent être poussées à tous les clients comme objet global de stratégie (GPO) utilisant le contrôleur de domaine.

Contournement sur le WSA

Créez une identité pour NCSI et exemptez-la de l'authentification basée sur l'URL ou son agent d'utilisateur.

URLs connu auquel NCSI se connecte

ncsi.glbdns.microsoft.com
newncsi.glbdns.microsoft.com
www.msftncsi.com

Agent d'utilisateur NCSI

Microsoft NCSI