O tráfego de Windows 7/clientes da vista mostra a estação de trabalho em vez do usuário nos logs do acesso

Índice

Pergunta

Por que o tráfego dos clientes de Windows 7/vista mostra a estação de trabalho em vez do usuário nos logs do acesso?

Ambiente

Microsoft Windows 7, vista de Microsoft Windows, ferramenta de segurança da Web de Cisco (todas as versões), tipo substituto: Endereço IP

Sintomas

Determinadas linhas de registro nos logs do acesso estão mostrando o nome de máquina dos computadores, em vez do DOMÍNIO \ USER.

Microsoft introduziu uns novos recursos em Windows 7 e Windows Vista chamou da “o indicador de status conectividade de rede” (NCSI), que aparece como um ícone pequeno do globo que apareça sobre o ícone da interface de rede na bandeja do sistema. Imediatamente depois do início de uma sessão, esta característica tentará pedir dados do Internet a fim saber se há uma conectividade de Internet.

Há uns problemas conhecidos com NCSI, onde enviará credenciais da máquina em vez das credenciais do usuário quando a autenticação de NTLM é exigida.

Desde que NCSI é mais provável enviar o primeiro pedido de um PC ao WSA, nenhum substituto existe contudo e um substituto com base em IP novo com o nome de máquina em vez do nome de usuário real é criado. Este substituto é usado para cada pedido do endereço IP inicial até os tempos substitutos para fora e o usuário tem que autenticar novamente, esta vez com credenciais reais.

Desde que o nome de máquina não é o mais provavelmente um membro do grupo inicialmente pretendido AD todos os pedidos não provocarão o acesso/política de descriptografia corretos, às vezes tendo por resultado o pedido que está sendo obstruído.

Para obter mais informações sobre de NCSI, veja por favor o seguinte artigo de Microsoft KB.

Veja por favor as instruções abaixo à ação alternativa a edição:

1. Lance o editor de registro procurando pelo “regedit” do menu da tarefa. Você deve clicar com o botão direito e selecionar “para ser executado como o administrador”.

2. Navegue a: HKEY_LOCAL_MACHINE \ SISTEMA \ CurrentControlSet \ serviços \ NlaSvc \ parâmetros \ Internet

3. Sob a chave de Internet, o clique duas vezes “EnableActiveProbing”, e então em dados do valor, datilografe: **0**.
4. Clique o " OK ".

5. Reinicie o computador.

Estas mudanças podem ser empurradas a todos os clientes como um objeto global da política (GPO) que usa o controlador de domínio.

Workaround no WSA

Crie uma identidade para NCSI e isente-a da autenticação baseada na URL ou em seu agente de usuário.

URL conhecidas a que NCSI conecta

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

Agente de usuário NCSI

Microsoft NCSI