Il traffico proveniente da client Windows 7/Vista mostra la workstation anziché l'utente nei log degli accessi

Sommario

Domanda

Perché il traffico proveniente dai client Windows 7/Vista mostra la workstation anziché l'utente nei log degli accessi?

Ambiente

Microsoft Windows 7, Microsoft Windows Vista, Cisco Web Security Appliance (tutte le versioni), Tipo di surrogato: Indirizzo IP

Sintomi

In alcune righe dei log degli accessi viene visualizzato il nome del computer del computer, anziché DOMINIO\UTENTE.

Microsoft ha introdotto in Windows 7 e Windows Vista una nuova funzione denominata "Network Connectivity Status Indicator" (NCSI), che viene visualizzata come una piccola icona a forma di globo sulla barra delle applicazioni. Immediatamente dopo l'accesso, questa funzionalità tenterà di richiedere i dati da Internet per verificare la presenza di connettività Internet.

Si sono verificati problemi noti con NCSI, in cui verranno inviate le credenziali del computer anziché quelle dell'utente quando è richiesta l'autenticazione NTLM.

Poiché è molto probabile che NCSI invii la prima richiesta da un PC al WSA, non esiste ancora alcun surrogato e viene creato un nuovo surrogato basato su IP con il nome del computer anziché il nome utente effettivo. Questo surrogato viene utilizzato per ogni richiesta dall'indirizzo IP iniziale fino al timeout del surrogato e fino a quando l'utente deve eseguire nuovamente l'autenticazione, questa volta con credenziali reali.

Poiché il nome del computer non è probabilmente un membro del gruppo AD inizialmente

previsto, tutte le richieste non attiveranno i criteri di accesso/decrittografia corretti, talvolta causando il blocco della richiesta.

Per ulteriori informazioni su NCSI, vedere il seguente articolo della Microsoft KB.

Per risolvere il problema, consultare le istruzioni riportate di seguito:

1. Avviare l'Editor del Registro di sistema cercando "regedit" dal menu delle operazioni. Fare clic con il pulsante destro del mouse e selezionare "Esegui come amministratore".

2. Accedere a: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NlaSvc\Parameters\Internet

3. Sotto la chiave Internet, fare doppio clic su "EnableActiveProbing", quindi in Dati valore digitare: **0.**
4. Fare clic su "OK".

5. Riavviare il computer.

Èpossibile eseguire il push di queste modifiche in tutti i client come oggetto Criteri di gruppo globale utilizzando il controller di dominio.

Soluzione del WSA

Creare un'identità per NCSI ed esentarla dall'autenticazione in base all'URL o al relativo agente utente.

URL noti a cui si connette NCSI

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

Agente utente NCSI

Microsoft NCSI