

NVCnet per terminal server

Un approccio unico alle sfide di WTS

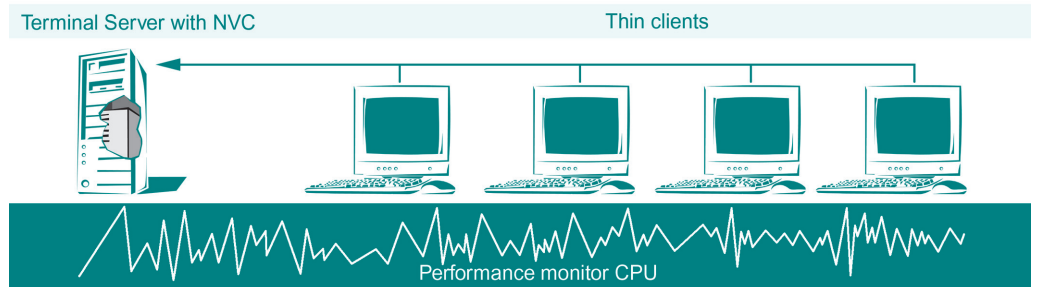
L'adozione dei Windows Terminal Services (WTS) sta diventando sempre più frequente nel settore della piccola e media impresa. Ciò è dovuto principalmente alla sempre maggiore capacità di ampiezza di banda delle moderne reti ed all'esigenza di una gestione centralizzata, al fine di ridurre le violazioni di sicurezza che avvengono nella rete. I Terminal Server riducono il costo totale di proprietà (TCO) all'interno di un'organizzazione.

Le società che utilizzano soluzioni WTS hanno bisogno di software antivirus specificamente progettato per questo ambiente, diverso dai software antivirus tradizionali per server e workstation. Norman ha preso sul serio questo trend ed ha messo a punto NVCnet per Terminal Server – un approccio unico nel suo genere alle sfide poste dai WTS.

La sfida della scansione AV per Terminal e File Server

Un problema che si verifica sui Terminal e File Server con la scansione antivirus al momento dell'accesso sono i picchi imprevedibili di utilizzo della CPU che si raggiungono durante la scansione stessa. Alcuni file assorbono parecchia potenza dalla CPU per stabilire se sono infettati o no, inoltre, ci sono momenti in cui molti utenti copiano o salvano contemporaneamente file sui Terminal e File Server, p.es. all'inizio della giornata di lavoro. Queste situazioni possono inaspettatamente rallentare il server, interrompendo così il normale flusso di lavoro su tutti i terminali.

(Fig.: mostra la scansione on-access tradizionale sul server)

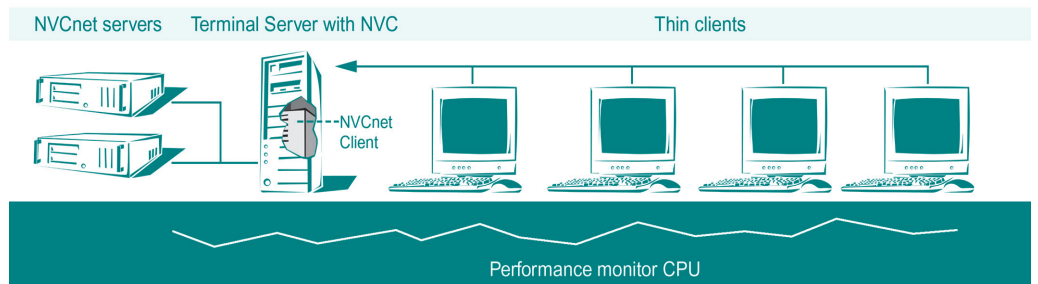


Le prove eseguite hanno dimostrato che questo è un problema comune a tutti gli scanner antivirus e la semplice migrazione verso altri software antivirus non servirebbe a risolverlo. Una possibile soluzione è stata quella di acquistare altri server per distribuire l'elevato carico su più CPU.

La soluzione NVCnet

In un ambiente Terminal e File Server, NVCnet aggiunge flessibilità e prevedibilità all'ambiente stesso. Aggiungendo server NVCnet dedicati alla rete, questa trasferisce il carico di lavoro di scansione dal Terminal o File Server stesso ad un Server NVCnet di scansione antivirus specifico. Di conseguenza, la maggior parte delle risorse dei Terminal e File Server può essere utilizzata per la gestione di file ed utenti, senza le tipiche interruzioni causate dalla scansione antivirus.

(Fig.: mostra la scansione on-access associata a NVCnet)



Riunendo la scansione all'accesso alla tecnologia NVCnet, un amministratore di rete è in grado di prevedere con maggiore esattezza quali sono le risorse necessarie per la scansione antivirus e quelle richieste per i terminal service. Quando il carico di lavoro della CPU sul Terminal o File Server supera un limite predefinito, la scansione antivirus viene trasferita al server NVCnet dedicato. Il carico di lavoro della CPU sul Terminal e File Server risulterà in tal modo minore, più stabile e non dipenderà dal tipo di file gestito dallo scanner.

Norman è una delle società leader nel campo della sicurezza dei dati. Con i suoi prodotti antivirus, antispamming, di controllo delle e-mail e dei download e con i suoi firewall personali l'azienda gioca un ruolo determinante nel settore del trattamento dei dati.



NORMAN
www.norman.com

Requisiti essenziali

Native Norman Virus Control per Terminal e File Server installato su ogni Terminal o File Server dove è installato NVCnet per Terminal e File Server. (Controlla la scansione antivirus con l'NVCnet per client del Terminal e File Server.

Native Norman Virus Control per server installato su ogni server NVCnet (gestisce tutti gli update dei file con le definizioni dei virus, del motore, del Norman SandBox, ecc.

Requisiti di sistema

Bilanciamento di carico e soluzione failover

È anche possibile avere diversi server NVCnet collegati al Terminal o File Server. Ciò assicura quindi una flessibilità di sistema ancora maggiore consentendo al server NVCnet successivo nella serie di prendere il controllo qualora il primo server NVCnet fosse già sovraccaricato.

L'impiego di almeno due server NVCnet garantisce inoltre una soluzione failover, assicurando la continuazione della scansione antivirus all'accesso, anche in caso di guasto di un server NVCnet. Questa soluzione consente anche di aggiornare i server con patch, ecc. senza dover arrestare la scansione AV con il conseguente rischio di potenziale infezione.

Il concetto NVCnet

NVCnet è studiato per rimuovere il carico di lavoro dalla CPU e in tal modo impedire i picchi di carico della stessa su server che ospitano file oggetto di scansione da parte di applicazioni antivirus. La soluzione NVCnet si divide in due parti - NVCnet server, dove avviene la scansione vera e propria dei file e NVCnet client, situato sul Terminal o File Server dove risiedono i file che devono essere esaminati. NVCnet client comunica con NVCnet server e trasferisce file o frammenti di essi a NVCnet server che quindi provvede alla scansione antivirus dei file.

Grazie alla logica ed al design avanzato di NVCnet e del nostro motore di scansione, nella maggior parte dei casi saranno sufficienti frammenti di file per rivelare la presenza di eventuali infezioni. Il risultato di tutto ciò è un aumento della velocità ed un minore utilizzo della larghezza di banda.

Non c'è limite al numero di server NVCnet che si possono installare in una rete e, con due server NVCnet, è possibile realizzare un sistema dotato di funzionalità di fail-over e di bilanciamento del carico. Per il bilanciamento del carico, il server principale può essere impostato per trasferire un nuovo procedimento di scansione ad un altro server NVCnet qualora il carico raggiungesse certi limiti di soglia. Inoltre, nel caso un server NVCnet per qualsiasi ragione si guastasse o dovesse essere fermato per manutenzione, l'altro subentrerebbe nell'espletamento della procedura di scansione.

Per quanto riguarda le prestazioni, la velocità di una sessione di scansione è limitata dalla velocità della rete. Ma, diversamente da altri tipi di scanner che trasferiscono l'intero file nella rete per la scansione, NVCnet effettua trasferimenti di masse di dati relativamente piccole tra client e server aumentando così al massimo l'efficienza della sessione di scansione.

Funzioni aggiuntive per l'individuazione di virus

Norman SandBox v2

La tecnologia SandBox della Norman rivela virus di computer binari, nuovi e sconosciuti. Al giorno d'oggi, un worm annidato in un'e-mail può infettare decine di migliaia di workstation in pochi secondi. I distributori di programmi antivirus sono chiamati a trovare una soluzione, aggiornare i file di definizioni di virus e distribuirli immediatamente ai propri clienti. È ovvio che la velocità è di vitale importanza.

SandBox di Norman è un mondo virtuale di computer all'interno di una rete, simulato nel programma di controllo del virus. Un emulatore crea un ambiente dove possibili programmi eseguibili infettati da virus sono eseguiti proprio come succederebbe in un sistema reale. SandBox è impostato specificamente per trovare nuovi worm per e-mail, reti e di tipo peer-to-peer.

Recent test from AV-Test GmbH shows that the Norman SandBox has the best proactive protection of new and unknown viruses. For more details please visit

http://www.norman.com/News/Press_releases/17613/en

Aggiornamento dei file di definizioni di virus

Una versione funzionante di NVC per server deve essere installata sul server NVCnet e gli aggiornamenti dei file con le definizioni dei virus saranno poi gestiti dal modulo di aggiornamento NVC standard - Norman Internet Update (NIU). Norman Internet Update può essere configurato per cercare regolarmente i file nuovi ed aggiornati sui server dei prodotti Norman.

NIU fornisce aggiornamenti completi e l'aggiornamento del software NVC per garantire che le definizioni dei virus siano mantenute aggiornate e che l'utente stia sempre utilizzando la versione più recente del software. Norman Internet Update utilizza aggiornamenti cumulativi dei file con le definizioni per limitare il più possibile le dimensioni degli aggiornamenti, riducendo in tal modo il carico della rete ed aumentando la velocità di distribuzione degli stessi.

For more information please visit; www.norman.com/Product

Requisiti di sistema

Per Windows NT versione 4 con SP4 (o superiore) ed Internet Explorer 4.0 (o superiore).
Server Windows 2000 e 2003

Norman soluzioni per clienti/workstation: Norman Virus Control per Windows 95, 98, Me, NT4.0, 2000, XP, OS/2, Linux (scansione su domanda) • Norman Internet Control per Windows 95, 98, Me, NT4.0, 2000, XP • Norman Personal Firewall • Norman Ad-Aware

Norman soluzioni per server: Norman Virus Control per Microsoft Windows NT4.0, 2000, 2003 • Norman Virus Control Firebreak per Novell Netware 4.11 e seguenti • Norman Virus Control per Linux • Norman Virus Control per OS/2

Norman soluzioni per web/gateways/mailservers: GFI MailEssentials • GFI MailSecurity • GFI DownloadSecurity • NVCnet • Norman Virus Control per Lotus Domino (Win32, OS/2) • Norman Virus Control per Firewall-1 NG • Norman Virus Control per Microsoft Internet Information Server • Norman Virus Control per Microsoft Exchange • Norman Virus Control per Microsoft Exchange 5.5 • Norman Virus Control per MIMESweeper



NORMAN[®]
www.norman.com