Introduzione al registro di Microsoft Windows

di: Robert H. Williams III
CompTIA A+\Net+, Microsoft MCP\MCSA\MCSE (2000), Cisco CCNA

v. 1.2

tradotto da Micaela Gallerini (aka heba)
heba.ry.mg@gmail.com

Su questo lavoro:

Questo tutorial è un'introduzione al registro di Microsoft Windows. E' stato scritto per due tipologie di persone: gli amministratori e gli utenti esperti. Gli amministratori possono essere amministratori di sistema o di reti, dai molti cambiamenti al registro possono essere diffusi tramite Active directory a tutti i computer di rete. Gli utenti esperti vogliono generalmente prendere nota di un uso locale del registro di sistema, e possibilmente delle funzioni remote per controllare come altri pc nella loro rete reagiscono. Per esempio, bloccare l'accesso a Internet Explorer al computer dei vostri figli da remoto.

Introduzione:

Il registro di Windows è spesso un argomento che molte persone evitano. Esse vedono il registro come alcune scatole nere che non si possono aprire, o sembrano pensare che è scritto in qualche linguaggio non mortale anche se possono sempre capirlo. In verità, il registro è veramente semplice. Mentre è più dura o sempre impossibile immaginarsi come alcune chiavi lavorano, il registro in sè è semplice. Non è una confusione di configurazioni che non hanno ordine. Le impostazioni sono messe in una locazione logica. Se conoscete come il registro lavora, potete trovare ciò che volete più velocemente.

Pre-requisiti:

Per usare questo tutorial, tutto ciò di cui avete bisogno è un sistema operativo basato su Windows, e un tool per editare il registro. Regedit e/o Regedt32 caricate di default sulle maggiori versioni di Windows. Per usare una policy di sicurezza locale, avete bisogno di essere su un sistema NT, anche 2000, XP, o 2K3. Per usare Active Directory e per spiegare le maschere amministrative, dovete installare un dominio Active Directory.

Che programma uso per editare il registro?

Windows ha installato in default uno dei tre tools per editare il registro:

RegEdit
Regedt32
Reg

Un altro tool che potete utilizzare è *RegEditX*, un tool gratuito da DC Software (http://www.dcsoft.com), RegEditX aggiunge alcune estensioni a RegEdit. Non sostituisce RegEdit, e non è un programma indipendente.

Che cos'è il registro?

Il registro è niente di più che un programma centrale dove sono immagazzinate tutte le impostazioni del computer. Ma un programma non immagazzina alcun dato nel registro che è un programma gratuito. E' simile alla configurazione dei files per Linux e Unix, ma loro sono immagazzinati in cartelle, in alveari, struttura come le cartelle.

Nota tecnica: Sarebbe possibile notare come nel registro sia implementato dal Configuration Manager parte del Kernel Windows. Come tale, è supportata tutta la sicurezza associata con il kernel tale come il caricamento ring 0 senza il processore.

Cosa sono le chiavi di registro?

Quando aprite il registro con RegEdit, vi si mostreranno 5 chiavi, o alveari. Le cinque chiavi sono:

HKey_Classes_Root (HKCR)
HKey_Current_User (HKCU)
HKey_Local_Machine (HKLM)
HKey_Users (HKU)
HKey_Current_Config (HKCC)
HKEY_DYN_DATA (HKDD) (Win9x Only)

Delle cinque, tre sono attualmente sottoalberi di altre chiavi. **HKey_Users** e **HKey_Local_Machine** sono le due chiavi "intere". Le altre chiavi sono sottochiavi di queste due, o combinazioni di due o più chiavi.

HKey_Users contiene tutte le impostazioni dell'utente nel registro. Se modificate un programma esso lo registrerà nel registro, un altro utente non sarà coinvolto da esso, e sarà in questa sezione. Potete anche usare questa chiave per editare *.default*, la chiave che è usata per creare le chiavi di default per tutti i nuovi utenti. Quando un nuovo utente sarà creato, .default verrà copiato nel nuovo alveare, usando i loro SID per parlarsi a parte.

HKey_Current_User è la chiave *HKey_Users* per l'utente che carica regedit. E' una scorciatoia alle impostazioni dell'utente corrente, così non dovrete trovare cosa avete bisogno di editare della HKey_USers.

HKey_Current _Config è il profilo dello hardware corrente inserito in *HKey_Local_Machine\System\ControllSet001\Hardware Profiles*. HKCC è niente di più che un'indicazione a questa chiave.

HKey_Classes_Root è una combinazione delle chiavi *HKEY_LOCAL_MACHINE\Software\Classes* e *HKEY_CURRENT_USER\Software\Classes*. Il dato è una fusione, se non c'è nessun dato in ascolto per l'utente corrente, nel momento in cui ne viene usato uno per la macchina locale.

Cosa sono le chiavi? gli alveari? i valori?

Quando più persone dicono "alveari", normalmente intendono le cinque (5) chiavi principali, ma qualche volta parlano delle sottochiavi. Le chiavi sono le uniche che sono nel regedit come delle piccole cartelle.
I valori per ognuna delle chiavi possono essere *binario*, *stringa*, *dword*, *multi-stringa*, *stringa espandibile*, e pochi altri. In generale, non avrete bisogno di conoscere cosa queste chiavi indicano quando le editate, ma avrete usato il tipo di valore di cui avete bisogno. Non potrete usare una stringa quando un tipo dword è richiamato. Le stringhe e i dwords sono i più comuni. Su windows 2k, solo regedit supporta le stringhe, dword e i binari. Per poter utilizzare regdt32 dovrete editare stringhe estendibili e multi-stringhe.

I tipi di valori nel registro sono programmate da Microsoft come le seguenti: (Nota: Questa è preso direttamente dal sito Microsoft)

REG_BINARY
REG_DWORD

REG_EXPAND_SZ
REG_MULTI_SZ
REG_SZ
REG_RESOURCE_LIST
REG_RESOURCE_REQUIREMENTS_LIST

REG_BINARY Dato binario al naturale. Più informazioni sui componenti hardware sono immagazzinate come dato binario ed è visualizzato nel Editor del registro in formato esadecimale.

REG_DWORD Dato rappresentato da un numero che è lungo 4 bytes (32-bit intero). Molti parametri per i drivers e servizi delle periferiche sono di questo tipo e sono visualizzati nell'editor del registro in formato binario, esadecimale, o decimale. I valori collegati sono DWORD_LITTLE_ENDIAN (il più piccolo byte a livello di importanza è posizionato al posto più basso) e REG_DWORD_BIG_ENDIAN (il più piccolo byte a livello di importanza è posizionato al posto più alto).

REG_EXPAND_SZ Un dato stringa di lunghezza variabile. Questo tipo di dato include variabili che sono risolti quando un programma o un servizio usa il dato.

REG_MULTI_SZ Una stringa multipla. I valori che contengono liste o valori multipli in una forma che le persone possono leggere sono generalmente di questo tipo. Le registrazioni sono separate da spazi, virgole, o altro tipo di punteggiatura.

REG_SZ Un stringa di testo di lunghezza fissa.

REG_RESOURCE_LIST Una serie di array nidificati i quali sono designati a magazzino in una lista di risorsa che è usata da un driver di periferica hardware o una delle periferiche fisiche che controlla. Questo dato è rivelato e scritto nell'albero *\ResourceMap* dal sistema ed è visualizzato nell'Editor di registro in formato esadecimale come un Valore Binario.

REG_RESORCE_REQUIREMENTS_LIST Una serie di array nidificati che sono designati a magazzino in una lista di driver della periferica di possibili risorse hardware il driver o una delle periferiche fisiche che controlla e che possono essere usate. Il sistema scrive un sottoinsieme di questa lista nell'albero *\ResourceMap*. Questo dato è rivelato dal sistema ed è visualizzato nell'Editor di registro in formato esadecimale come un Valore Binario.

REG_FULL_RESOURCE_DESCRIPTOR Una serie di array nidificati che sono designati a magazzino in una lista di risorse che è usata da periferiche hardware fisiche. Questo dato è rivelato e scritto nell'albero *\HardwareDescription* dal sistema ed è visualizzato nell'editor di registro in formato esadecimale come un Valore Binario.

REG_NONE - Dato di nessun particolare tipo. Questo dato è scritto nel registro dal sistema o applicazioni ed è visualizzato nell'editor del registro in formato esadecimale come un Valore Binario.

REG_LINK - Stringa Unicode che nomina un link simbolico.

REG_QWORD Dato rappresentato da un numero che è un intero a 64 bit. Questo dato è visualizzato nell'editor di registro come un Valore Binario ed era stato introdotto per la prima volta in Windows 2000.

Perché per alcuni programmi devo riavviare?

Esistono più chiavi sotto HKey_Users e HKey_Local_Machine. HKU potrebbe essere pensato come l'utente sia parte di tutta la configurazione, mentre HKLM è la parte del computer. Molte impostazioni che sono per computer sono bloccate a quando il computer si avvia, come le impostazioni per i servizi, e sono allora ancora mai controllate. Un riavvio forza tutti i programmi al controllo di alcuni cambiamenti nella sezione del registro della macchina. Questo è una delle ragioni per cui dovete aver bisogno di un riavvio, alcune altre possono essere perchè un file è bloccato durante le normali operazioni, ed ha bisogno di controllare i cambiamenti durante l'avvio.
Alcuni programmi leggono i dati nella chiave HKCU durante il login, e poi mai più. Quando cambiano, questi programmi generalmente vi richiederanno un riavvio, ma attualmente un login è tutto ciò di cui hanno bisogno.

Che cosa è la politica di gruppo?

La politica di gruppo è usata per facilitare i cambi di molte impostazioni di registro su un computer Windows. Questo è generalmente fatto solo su windows 2000, XP, e 2003 o le macchine più nuove. I tools amministrativi possono avere editor di politiche di gruppo, listati come editor di politiche locali. Se non sono listati, dal menu di caricamento, tipo in mmc, e *file -> Aggiungi\Rimuovi Snap in*. Nelle politiche locali del computer, avete due chiavi, *computer* e *configurazione utente*.

Queste impostazioni cambiano in HKU e HKLM. C'è una discreta quantità di opzioni predefinite qui, come le configurazioni del computer, le impostazioni windows, *Inizio\Fine scripts*. Vengono chiamati scripts, anche i file .bat o .exe che vengono caricati quando il computer viene acceso o spento. Questo NON è lo stesso come scrivere *Inizio\Fine sessione*. Molti utenti normali vorranno giocherellare con le configurazioni dell'utente, la configurazione del computer è però suggerita agli utenti di alto livello.

Nella sezione utente, ci sono opzioni per gli scripts del *login\logout*, e le maschere amministrative. Le maschere sono la cosa principale in questa sezione con le quali l'utente vorrà giocherellarci. Cliccate sul desktop, e troverete una lista di opzioni. Questo è soprattutto una cosa semplice, icone nascoste o visibili, niente di tutto questo potrebbe realmente essere considerato avanzato. Queste opzioni che avete dipendono dalla versione di windows che avete installato, 2k ha meno opzioni rispetto a 2k3 e XP.

Andiamo a guardare nel sistema, schiacciando contemporaneamente CTRL+ALT+DEL (il CANC sulle tastiere italiane, n.d.t.). Ci sono opzioni per controllare cosa i bottoni raccolgono in ctrl+alt+del. Ci sono tutte una sorta di opzioni che non è necessario che conosciate e che potete fare, come *Reti -> Connessioni di rete*.

In quasi ogni chiave, cliccando su di esse vi apparirà una finestra di dialogo con tre opzioni, *abilita*, *disabilita*, e *non impostare*. E un tabella esplicativa. Essa crea sicuramente la spiegazione per capire cosa le opzioni fanno che dovrete leggere.

La policy di gruppo non è realmente intesa per cambiare le impostazioni su un singolo computer. Essa è intesa per cambiare le impostazioni su centinaia o migliaia di computer per volta. In una rete Windows Active Directory, avrete ciò che è chiamato OU. Essi sono cartelle fondamentali, e gli amministratori di rete possono aggiungere computer e utenti all'interno di queste OU. Per esempio, è possibile che siate nel *Sales\Users OU.* tutte le persone nel dipartimento di vendita devono avere le stesse impostazioni desktop. L'amministratore crea un'impostazione policy di gruppo su *Sales\Users*. Ora determina tutti gli utenti in vendita. Cosa succede se un utente si sposta a *Tech\Desktop Administrators*? L'amministratore semplicemente cambia l'utente che è in OU, e le impostazioni per i

loro desktop cambiano secondo le nuove regole. Con le maschere della policy di gruppo, ci sono più impostazioni di sicurezza, e le abilità per assegnare i permessi e i programmi agli utenti e/o ai computer, la policy di gruppo è un tool molto potente. Ogni registro può cambiare istruzione in questa sezione che può essere applicata via policy di gruppo per determinare tutti gli utenti in una compagnia.

Come faccio il back-up del registro?

Un modo semplice per fare il backup del registro senza altri tools è questo: aprite Regedit, e sull'icona del computer, cliccate con il tasto destro del mouse e selezionate *Esporta*. Crea sicuramente l'icona per il computer che state usando, e non una delle 5 chiavi, altrimenti non vorreste esportare tutte le chiavi. Questo crea un file .reg. Semplicemente cliccando su di esso in explorer lo reimporterà. Questo causerà il suo FONDERSI con il registro corrente, così ogni nuova chiave creata successivamente al backup non sarà colpita. Ci sono altri modi, molti altri modi, per fare il backup del registro, come un backup dello stato del sistema usando la creazione del tool di backup di windows. Ma esportandolo potrebbe essere semplificato.

Potete usare l'*esporta* per esportare ogni chiave. Crea una modifica ordinata del registro e vuole la sua condivisione? Cliccate il tasto destro del mouse sulla chiave, ed esportatela su quella chiave. I file .reg non sono niente di più che dei files di testo, e possono essere editati con facilità. Se avete qualche sorta di programma per scrivere in basic, potete creare un programma che crea files .reg per cambiare le impostazioni del registro.

Cosa è la struttura del registro?

HKey_Classes_Root è dove vengono immagazzinati i files. E' come il computer conoscesse cosa usare per aprire i files .bmp, ed è come conoscesse cosa prendere su menu contestuale, il menu che appare quando cliccate con il pulsante destro del mouse sul file. Apre regedit e apre HKCR, la prima volta che lo fate*.

Questo come potete vedere, è un'eccellente scheda. E' fondamentale per tutti i files. Cliccate sul segno + per aprire la chiave, e selezionate *apri con*, *shell*, e *shellex*. La shell non dovrebbe essere lì, perciò non preoccupatevi. Le chiavi di Shellex sono uniche non giocherellateci, invece modificatele con un editor di registro, sono basate su un rapporto di pari livello, e possono essere molto facili da mettere in disordine. La chiave di shell è l'unica chiave principale che potrete editare a mano, e la più divertente. Se non avete la chiave di shell, cliccate con il pulsante destro del mouse sull'asterisco (*), e cliccate *nuovo -> chiave*. Potreste dire che Nuova chiave#1 è rinominata nella shell.

Ora cliccate con il tasto destro del mouse sulla shell. Nominate questa come *OpenCMD*. Questo metodo non importa realmente la chiave, e può diventare ogni nome che voi volete. Sulla destra del pannello, fate doppio click (Default) e inserite un dato valore, inserite A*pri Comando di Linea Qui*. Ora evidenziamo OpenCMD sulla sinistra del pannello, e inserite una nuova chiave. Nominate questo *comando*, e DEVE essere nominato **comando**. Allora cliccate sul comando, e fate doppio click (Default) ancora. Impostate questo valore come "*cmd /k ver & date /t & time /t*" senza gli apici. Adesso cliccate con il destro del mouse su ogni file, eccetto le cartelle, ed ora avete le opzioni per aprire un comando window in quella directory.

Dopo, cliccate con il destro del mouse la chiave OpenCMD, e inserite *esporta*. Salvatelo sul vostro desktop o qualsiasi cosa vogliate. Cliccate con il destro del mouse il file, e inserite *scrivi*. Potete ora modificare qualunque cosa nella chiave, e reimportarlo indietro. Potete anche prendere questo file con voi (su un floppy o usb, n.d.t.), e aggiungere questo comando a ogni computer che desiderate, con

facilità.

Proviamone un'altra. Cercate la chiave *Folder*. NON .folder, ma FOLDER. Sotto shell, create una nuova chiave, OpenNewWin. Esso è in default *Open Folder In New Window*, modificatelo. Create una nuova sottochiave, con il comando *Modifica*, essa è di default in *explorer %1*. Ora quando aprite una cartella sul vostro desktop, se volete potete aprirne una seconda ed inserite lo stesso albero, cliccatelo con il destro del mouse. Non sembra piacere molto, ma sono sicuro lo userete più di ciò che vi aspettate.

Come usare il software del registro?

Penso al registro come una struttura di directory di contenimento di tutti i files .ini usata per i programmi. Se spesso un file .ini programma, dovete capire alcune delle impostazioni che ci sono in esso, ma senza alcune sorte di lista di comandi non potrete mai raffigurare alcune cose non listate. Quando guardate le chiavi create nel registro da un programma, alcune di queste chiavi potete capirle, altre non le rappresenterete mai senza guardarle o provare e sbagliare.

Il software può immagazzinare ciò che è impostato in una delle due aree, *HKey_Current_User*, o *HKey_Local_Machine*. Se è l'utente corrente, è un'impostazione per-utente, mentre local machine immagazzina le impostazioni per tutti gli utenti. *HKCU\Software* e *HKLM\Software* sono le chiavi di default per le informazioni. Le impostazioni di HKCU si sovrappongono conflittualmente sulle impostazioni di HKLM.

Adesso proviamo un esempio di impostazioni di software. Andate su *HKey_Current_User\Software\Microsoft* da lì, aprite *Windows\CurrentVersion*.

Internamente qui ci sono 5 differenti chiavi caricate, *Run*, *RunEX*, *RunOnceEX*, e *RunServices*. Dipendendo dal sistema non tutte queste chiavi possono essere visualizzate lì per default. Queste chiavi controllano programmi che iniziano al logon. Se avete qualche programma si avvia al logon che volete uccidere, se non è nel menu di Start (Inizio, windows versione italiana, n.d.t.) allora le modifiche sono posizionate nella chiave caricata. Come più impostazioni del software, la chiave *HKCU\Software\Microsoft\Windows\CurrentVersion\Run* è solamente per l'utente corrente, mentre *HKLM\Software\Microsoft\Windows\CurrentVersion\Run* è per tutti gli utenti.

Avete windows 2k, e usate il comando prompt? Avete l'abilità a inserire automaticamente file e directory nominate da voi, come in XP. Se siete in XP, e digitate in win mentre in *c:*, premete *tab* completerete la parola di win alla directory nominata in windows. Questo può essere un grande aiuto se avete qualche file\cartella realmente grossa da nominare. 2k non ha quest'opzione abilitata. *(HKCU|HKLM)\Software\Microsoft\Command Processor* prende le impostazioni per cmd, il comando del processore in windows 2K\XP. Qui dentro, vedrete una chiave di carattere complementare. Fate doppio click su di essa, modificate il valore alla chiave che volete, per esempio TAB chiave ha un valore esadecimale di 9, così mettete un 9 se volete tab per completare il file nominatela. Veloce e semplice. Una lista di chiavi di software differenti saranno in fondo a questa FAQ.

Vedo un numero come questo: {A671EBA0-895B-11D4-98B2-00A0C9EE6FD9} che cos'è?

Questo è un GUID, acronimo di Globally Unique Identifier. E' usata per identificare questo item da ogni altro item come intero ed è generale. Il GUID è generato in pare dagli indirizzi MAC sulla macchina corrente, e ora (spesso), tra altri items. Questi aiuti creano la sicurezza che non ci sono due

GUID simili.

I GUID sono usati per lo più per la programmazione COM, un tipo speciale di programmazione ad Oggetti. Senza entrare in profondità, i GUID sono normalmente usati in chiavi complesse nel registro, e sono un buon segno per stare lontani da quegli items. Essi sono sempre della stessa lunghezza, con 4 trattini al loro interno.

Questi vi permettono di chiamarli a parte dall'uso di SID per identificare gli account degli utenti.

In generale, gli items con GUID sono più complessi, ed hanno più che un pezzo di software che interfaccia con loro. State lontano dai GUID se non sapete cosa fanno esattamente.

Come posso restringere gli accessi al registro?

Ci sono molti modi per restrigere gli accessi al registro. Disabilitare i tools di registro, tali come regedit e regedt32, provate *(HKCU|HKLM)\Software\Microsoft\Windows\CurrentVersion\Policies\System* e aggiungere la chiave *Disabilita Tools di Registro* con un valore di REG_DWORD uguale a 1. Su molti sistemi avrete creato il sistema della sottochiave. Questa policy vi richiederà in generale di riavviare per registrare le modifiche. State attenti nell'usare questa chiave! Se NON siete abili ad usare i tools di editing del registro per fissare questa chiave. Potete importare un file .reg come normale, comunque, e più terze parti dell'editing del registro lavorerà. Solo i programmi regedit e regedt32 controllano questa chiave. Questo non crea la sicurezza del registro, viene disabilitato con un semplice path su di esso. Questo può usare tools terzi, file .reg, il comando reg dal prompt di Dos, o sempre regedit su altre macchine connesse remotamente. Questa chiave ha lo stesso effetto di rimozione file di livello accedendo a regedit.exe e regedt32.exe, ma da un differente messaggio di errore.

Gli alveari nel registro hanno i DACL (Discretionary Access-Control Lists) semplicemente come i file di sistema NTFS in windows. Se non usate windows XP home, cliccate con il tasto destro del mouse su ogni chiave darete i permessi...con *opzioni*. Da lì, semplicemente andate sul *file system*, impostate i permessi per utenti o gruppi, e usate *avanzate* per un controllo più attento. Dando un uso *read-only* (di sola lettura, n.d.t.) all'accesso alla loro stessa chiave HKCU interromperete alcuni programmi, ma preventiverete loro da modifiche su ogni impostazione. Controllate la sezione Active Directory per maggiorni informazioni su questo.

XP home PUÒ editare i permessi di registro come questo, esso richiede un *aggiungi* su programma per windows NT per abilitare la tabella di sicurezza per explorer. Cercate su Google e troverete tale programma.

Come posso accedere al registro di un altro computer?

L'accesso remoto ad un registro è piuttosto simile ad ogni altra attività amministrativa remota. Aprite regedit, *file->connessione di reti del registro*...chiave. Come altri tools di rete, avete bisogno di quelli giusti sull'altra macchina. Se siete su un dominio, allora il vostro account di dominio ha bisogno di essere applicato a un gruppo amministrativo, o se non siete su un dominio, avete bisogno di avere lo stesso username\password come account sul destinatario. Diversamente potrete domandare per un username\password con i permessi.

Per ottenere un registro potente modificate sopra i gruppi dei computers, un gruppo di policy è raccomandato.

Come lavorano Active Directory e le politiche di Gruppo con il registro?

Active Directory è un servizio di sistema di directory Microsoft basato su LDAP. Esso è usato per maneggiare gli utenti, i computers, e altri oggetti in una rete di grandi dimensioni (50~5,000+). Da uso politica di gruppo, potete applicare le modifiche a molte impostazioni di Windows, tali come le politiche delle password e restrizioni differenti di programmi. Per capire la relazione tra Active Directory e il registro, avrete bisogno di comprendere tre argomenti: *Preferenze e policys*, *Registro Tattoing*, e il file *.adm*.

Preferenze o Policy? Quali sono le differenze?

La policy di Gruppo può essere divisa in due sezioni, un'impostazione può essere una *preferenza*, o può essere una *policy*. La differenza qual è? Una preferenza è un'impostazione di default. Quando un utente è loggato, la preferenza è immagazzinata nella policy di gruppo in cui è applicato. Comunque, l'utente ha il pieno controllo sui cambiamenti delle impostazioni. Per esempio, potete impostare un font per Windows Notepad, e dopo caricarlo su notepad, l'utente è libero di creare modifiche al font size. Una volta che l'utente esce dalla sessione di lavoro e si rilogga, le preferenze sono riapplicate, e Notepad ritorna alle impostazioni di default del dominio.

Una policy, comunque, non può essere modificata dal utente finale. La differenza tra le due è semplicemente una questione di permessi: un utente ha il controllo sulle sue chiavi di registro in una preferenza, ma ha solamente letto i permessi al registro con una policy. Dall'uso di Active Directory, potete diffondere i permessi di registro, modificando una chiave a sola lettura, permettendovi di impostare ogni chiave come una politica, piuttosto che una preferenza. Questo è generalmente fatto quando si crea il vostro stesso file .adm, come i programmi Microsoft in generale usa una speciale impostazione di sottochiavi che sarà parlata nella sezione del registro Tatooing.

Per cambiare una preferenza in una policy, avete bisogno di cambiare i permessi dell'utente sulla chiave da *pieni* a *sola lettura*. Facendo questo potreste essere un'attività che gira su se stessa (l'utente entra nel cosidetto loop, n.d.t.). Mentre la policy di gruppo vi permette di digitare i permessi di registro, le preferenze ve lo permette solo su *Classi*, *Hardware*, e *Utenti*. Perchè, non c'è una chiave dell'utente corrente esso può solo impostare i permessi via SID, creando in questo modo un'inutile impostazione di permessi.

Registry Tattooing: che cos'è?

Il registro Tattooing (letteramente registro tatuaggio, n.d.t.) è uno dei problemi che fronteggerete quando userete una policy di gruppo per modificare il registro. Se la policy di gruppo crea una nuova chiave nel registro, quando rimuovete la policy, non rimuovete la nuova chiave. Anche, se modificate un'impostazione via policy di gruppo, rimuovendo l'impostazione creata non ritorna all'impostazione precedente. Questo processo è chiamato tattoing, e può causare problemi imprevisti.

Se create una modifica al registro che causa errori in un programma in un modo imprevisto, rimuovete la chiave che non è possibile rimuovere via policy di gruppo. E' possibile solo modificare le chiavi, non rimuoverle. Così, avrete sicuramente testato il risultato della chiave prima del tempo. Creando una modifica alle impostazioni di registro di firefox, per esempio, non potrete controllare come ogni altro programma sul vostro computer lavora, così diventa una minaccia minore.

Per aiutare ad evitare questo problema, Microsoft ha creato quattro chiavi speciali nel registro, le chiavi

di policy:

HKEY_LOCAL_MACHINE\Software\Policies
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies
HKEY_CURRENT_USER\Software\Policies
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies

Come potete vedere, ci sono due chiavi ognuno per HKLM e HKCU. Queste chiavi hanno due speciali modifiche che creano più chiavi differenti. Primo, solo gli utenti normali hanno letto i permessi di queste chiavi, ma non possono modificarle. Secondo, queste chiavi sono tolte quando certi dati ricorrono, come quando la policy di gruppo è riapplicata. Questo significa che ogni modifica a queste chiavi sarà eliminata quando una policy verrà rimossa.

Mentre più software di Microsoft leggono le informazioni in queste chiavi, normalmente software non Microsoft non lo fanno. questo significa che se volete modificare le impostazioni di software non Microsoft, dovete essere pienamente preparati al registro tattooing. Anche, queste impostazioni saranno *preferenze*, e non *policies*, a meno che impostiate ad un livello HKLM o i permessi (e quello potrebbe essere un nuovo tipo di worms).

Se avete creato software con impostazioni che un amministratore può voler controllare, dovete voler permettere al software di interrogare anche queste chiavi. Ogni cosa costruita in queste chiavi potrebbe sovrascrivere le chiavi non-policy. Per esempio, se la chiave di *HKCU\Software\Program\Excecute* è a 0, e quella di *HKLM\Software\Policies\Program\Execute* è a 1, allora potrebbe avere un effettivo valore di 1. Così, quando create un programma, *HKLM\Software\Policies* potrebbe sovrascrivere tutti le altre impostazioni, *HKCU\Software\Policies*, *HKLM\Software* e *HKCU\Software* potrebbero entrambi essere controllati come vedete adattarsi. Dovete desiderare di permettere a HKCU di sovrascrivere HKLM, non dovete, dipendente su come desiderate per il software che lavora. Anche, se il programma scopre una politica su una di queste chiavi, dovete desiderare disabilitare l'opzione che vi permette di modificare queste opzioni, così essi sono forzati come una politica. Facendo questo, e spedendo il programma con un file .adm, potete ora dire al vostro software che è pienamente amministrato via Active Directory. Se state vendendo un programma sicuramente se non desiderate che più compratori cooperino allora avrete un intero lotto.

Cosa sono i file .adm?

I file adm sono file di aggiunte complementari alla policy di gruppo. Essi vi permettono di avere con facilità, un GUI per il controllo guidato delle impostazioni del registro. Tutte le parti delle maschere amministrative sono controllate via files .adm. Per aggiungere o rimuovere files .adm, prima aprite il gruppo della policy MMC cliccando una volta con il mouse su di essa, e cliccate con il pulsante destro del mouse una delle due maschere amministrative, una per computer, una per utente. Da lì, potete importare i vostri file .adm.

Molte applicazioni, come Microsoft Office, hanno i loro file .adm installati di default. Questi programmi devono sempre essere importati, dipendendo dall'installer. In più casi, questi file .adm sono ciò che è conosciuto come "totalmente modificabile". Questo è semplicemente un modo carino per dire che loro usano una chiave della policy e non avete problemi con tattooing. Esso significa anche che vi permette di impostarli come policys, non preferenze.

Se importate un file .adm e non sembra mostrarle, allora non dovrebbero essere totalmente modificabili. Quando i programmi non sono totalmente modificabili, allora sono, di default, *filtrati*. Per

rimuovere questi filtri, cliccate con il pulsante destro del mouse nella parte destra della sezione del pannello amministrativo (Dove le machere stesse sono visualizzate) e selezionate *guarda->filtri*... e deselezionate l'opzione "*Visualizza solo la politica delle impostazioni che possono essere totalmente modificabili*".

Come creo un file .adm? (Sezione In-depth)

I file .adm sono la linfa vitale di una policy di gruppo , contengono tutte le policies e preferenze. Se create un nuovo programma e volete che sia controllabile via Active Directory, avrete bisogno dei file .adm. Creando i files .adm potrebbero essere un modulo su se stesso, ma qui è una breve visione d'insieme. Prima, un semplice file .adm:

```
CLASS USER
  CATEGORY "GPTest Program"
    POLICY "Set level of restrictions"
      EXPLAIN "Set level of restrictions"
      KEYNAME Software\Policies\Ozzy_98\GPTest
      VALUENAME "Restriction Level"
      VALUEON NUMERIC 1 VALUEOFF NUMERIC 0
    END POLICY
  END CATEGORY
```

Questo è un semplice programma che ho creato per questo tutorial, esso sarà usato più tardi in una dimostrazione su come maneggiare programmi che avete creato via policy di gruppo. I principali comandi nel file sono CLASS, CATEGORY, POLICY, EXPLAIN, e KEYNAME.

CLASS chiama il sistema se è una policy della macchina, o una policy dell'utente. Se è di una macchina, allora comincia nella chiave HKEY_LOCAL_MACHINE. Se è una policy dell'utente, allora comincia in HKEY_CURRENT_USER. Esso controlla anche le funzioni amministrative del file .adm. Quando spiegate gli oggetti delle politiche di gruppo (GPO) potete impostarli per ignorare le impostazioni della macchina o dell'utente per aiutare la velocità del processo del login.

CATEGORY chiama la policy di gruppo dalla sezione per prendere le opzioni che ci sono sotto. Le categorie campione includono *Desktop* e *Pannello di Controllo*. E' raccomandato che creiate le vostre categorie, per aiutare a modificare le vostre impostazioni da questi formati integrati in Active Directory. CATEGORY ha bisogno di un END CATEGORY. All'interno di ogni CATEGORY mettete le POLICIES.

POLICY e semplicemente il nome della policy che si deve effettuare. E ciò che si vede quando si digita la GPO. Attenzione esso è di piccole dimensioni e descrittivo. POLICY ha bisogno di un END POLICY. EXPLAIN, KEYNAME, e tutti i valori di impostazione devono essere all'interno della sezione POLICY.

EXPLAIN è il testo sulle tabelle explain. Non ce n'è un reale bisogno, semplicemente da più informazioni sull'impostazione della policy.

KEYNAME è la chiave del registro che fa ricadere sotto le impostazioni. Ricordate di includere la KEY, non l'intero valore. La KEY è la parte sul pannello sinistro in RegEdit, mentre i VALORI sono gli items nel pannello DESTRO.

L'utente seleziona un valore, ci sono molti tools differenti, tanti di loro garantiscono i loro lavori. Due di loro, comunque, ricoprono più dei loro bisogni reali, il pulsante ON\OFF (Radio buttons) e DROPDOWNLIST (Un menu drop-down, a cascata). Il pulsante selezionato di default è il radio buttons, così noi includeremo questo come prima scelta. Da questa scelta di default non avete bisogno di una sezione a PARTE (inclusa più tardi). Questa impostazione di default vi da uno standard di tre opzioni, *abilita*, *disabilita*, e *non configurata*, e vi permette di impostare un valore per abilitare e disabilitare. Così il prossimo item ha bisogno di VALUENAME.

L'uso di VALUENAME è semplice. E' semplicemente il testo contrassegnato sopra le selezioni. Può essere impostato come preferite, è semplicemente un'altra descrizione dell'impostazione della policy di gruppo.

Dopo VALUENAME avete bisogno di impostare i valori per abilitare e disabilitare. VALUEON NUMERIC 1 imposta l'abilitazione del valore al numero 1.

Come posso vedere quali programmi accedono a quali chiavi nel registro?

Regmon è un programma gratuito da Sysinternals che monitora tutte le attività del registro. Siate pronti ad uno shock nel vedere come spesso i programmi accedono al registo. Avrete bisogno di usare i filtri per trovare ogni singolo programma\chiave d'accesso. Il programma si può trovare qui:

http://www.sysinternals.com/ntw2k/source/regmon.shtml

Quali sono alcune buone chiavi da editare?

Note: Chiavi con (1) e (2) devono essere usate insieme.

Impostazioni di Sistema

Note: *Le impostazioni qui applicate alle configurazioni del sistem-wide. Queste impostazioni sono tutte applicate al computer, non agli utenti.*

Proprietario Registrato
Key: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
Value Name: RegisteredOwner
Value Type: REG_SZ
Set To: **Nuovo nome del proprietario**
Note: *Questa chiave controlla il nome del proprietario nel sistema tabellare del pannello di controllo, e in ogni programma che legge questo dato. Questo non ha un effetto reale in Windows, è una mera modifica cosmetica.*

Impostazioni di Explorer

Note: *Tutte le impostazioni in questa sezione lavorano con explorer. Esse non dovrebbero essere usate per un solo mezzo di sicurezza, come non rimuovono i diritti per operare sulle azioni. Esse rimuovono meramente le abilità a fare un'azione via Explorer.*

Disabilita il tasto destro del mouse sul Desktop
Key: (HKCU|HKLM)\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

Value Name: NoViewContextMenu
Value Type: REG_DWORD
Set To: **1 per abilitare, 0 per disabilitare (0 Default)**
Notes: *Usa questa chiave per disabilitare il tasto destro del mouse del menu contestuale del desktop.*

Guarda la versione di Windows sul Desktop
Key: HKCU\Control Panel\Desktop
Value Name: PaintDesktopVersion
Value Type: REG_DWORD
Set To: **1 per abilitare, 0 per disabilitare (0 Default)**
Notes: *Visualizza la versione corrente di Windows in alto del desktop come wallpaper.*

Disabilita lo spegnimento del pc
Key: (HKCU|HKLM)\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer Value Name: NoClose
Value Type: REG_DWORD
Set To: **1 per abilitare, 0 per disabilitare (0 Default)**
Note: *Rimuove l'opzione di spegnimento dal pulsante del menu Start (Inizio). Questo potrebbe essere usato con la rimozione corretta dello spegnimendo del sistema. Questa chiave non previene l'utente dallo spegnimento automatico per anomalie del computer, esso rimuove solo il pulsante di spegnimento dal menu Start.*

Rifiutare il Caricamento di Questi Programmi (1)
Key: (HKCU|HKLM)\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer Value Name: DisallowRun
Value Type: REG_DWORD
Set To: **1**
Note: *Questo abilita il rifiuto del caricamento. Ogni programma dopo essere stato aggiunto alla sottochiave Riufiuto di caricamento non sarà caricato da explorer. I programmi possono ancora essere caricati da altre attività, e possono essere rinominati per aggirare questa disabilitazione.*

Rifiuto del caricamento di questi programmi (2)
Key: (HKCU|HKLM)\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun
Value Name: 1+
Value Type: REG_SZ
Set To: **Nome dell'applicazione**
Note: *Questa è il contenuto per la chiave Rifiuto di caricamento. Ogni programma dovrebbe essere messo nella chiave Rifiuto di caricamento (1). Il primo valore del programma dovrebbe essere chiamato 1. E se il programma fosse, per esempio, cmd.exe, allora il valore delle stringhe dovrebbero essere cmd.exe. Rinominando i files aggireranno questa opzione.*

Permette SOLO a Questi Programmi di caricarsi (1)
Key: (HKCU|HKLM)\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer Value Name: RestrictRun
Value Type: REG_DWORD
Set To: **1**
Note: *Questa chiave abilita le Restrizioni di caricamento. Questo è come Rifiuto di caricamento, ma explorer caricherà solo i programmi listati in questa chiave. Abilitate sicuramente regedit per il vostro account, o avete qualche altra attività per invertire questa chiave. Questo è la sicurezza Opt-In.*

Permette SOLO a Questi Programmi di caricarsi (2)

Key: (HKCU|HKLM)\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\RestrictRun
Value Name: 1+
Value Type: REG_SZ
Set To: **Nomi delle Applicazioni**
Note: *Questa chiave è il contenitore per la chiave Caricamento restrittivo. Ogni programma dovrebbe essere messo nella chiave Caricamento restrittivo. Il primo valore del programma dovrebbe essere chiamato 1. E se il programma fosse, per esempio, cmd.exe, allora il valore della stringa dovrebbe essere cmd.exe. Rinominando i files si aggirerà questa chiave.*

Cartelle della Shell
Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
Value Name: Various
Value Type: REG_SZ
Set To: **Nuovo Path**
Note: *Questa chiave contiene differenti paths delle cartelle speciali per l'utente, come desktop, CD Burning, Programmi, Menu Start e simili. Io personalmente preferisco usare NTFS Junctions spesso che modificare la locazione della cartella, alcuni programmi scrivono la locazione di default senza controllare il loro valore corretto.*

Specifica dell'applicazione

Note: *Le impostazioni qui descritte sono solo per le applicazioni listate. Questo può essere usato per impostare le opzioni su tutti i computer su una rete remota, o per bloccare nelle impostazioni di rifiuto dei permessi scritti della chiave.*

Applicazione: Notepad

Impostazione dei Font (Notepad)
Key: HKCU\Software\Microsoft\Notepad
Value Name: lfFaceName
Value Type: REG_SZ
Set To: **Nome del Font (Per esempio: Lucida Console)**
Note: *Imposta il font di default usato in notepad.*

Italics (Notepad)
Key: HKCU\Software\Microsoft\Notepad
Value Name: lfItalic
Value Type: REG_DWORD
Set To: **0 per disabilitare, 1 per abilitare (di default è 0)**
Note: *Imposta il font italics per notepad.*

Font Size (Notepad)
Key: HKCU\Software\Microsoft\Notepad
Value Name: iPointSize
Value Type: REG_DWORD
Set To: **Font size desiderato.**
Note: *Questa impostazione controlla la grandezza del carattere. Il valore della grandezza desiderata dovrebbe essere 10x. Per esempio, impostare una grandezza del font a 24, esso inserirà un valore decimale pari a 240.*

Window Size (Notepad)

Key: HKCU\Software\Microsoft\Notepad
Value Name: iWindowPosDX & iWindowPosDY
Value Type: REG_DWORD
Set To: **Grandezza della finestra desiderata**
Note: *Modificate questi due valori per controllare la grandezza di default di notepad quando è aperto.*

Internet Explorer

Note: *Queste impostazioni controllano la sicurezza per internet explorer. Dopo averle impostate, potrete voler rimuovere il pieno controllo della chiave da un non amministratore.*

Rifiuta l'abilità di chiudere il browser (Internet Explorer)
Key: (HKCU|HKLM)\Software\Policies\Microsoft\Internet Explorer\Restrictions
Value Name: NoBrowserClose
Value Type: REG_DWORD
Set To: **1 per abilitare, 0 per disabilitare (0 è dato per default)**
Note: *Quando l'utente pressa il bottone di chiusura, o prova a chiudere la finestra del menu File, l'azione è negata con un messaggio standard "L'operazione è stata cancellata dovuta alle restrizioni effettuate su questo computer. Siete pregati di contattare l'amministratore di sistema" IE può ancora essere chiuso soltanto uccidendo il processo. Se questa restrizione è in un posto sull'account dell'utente, e IE è caricanto sotto il contesto di un differente utente, il primo utente non può uccidere il processo del secondo utente. Questo permette ad internet explorer di essere sempre attivo nel computer kiosk.*

Rimuove i Favoriti
Key: (HKCU|HKLM)\Software\Policies\Microsoft\Internet Explorer\Restrictions
Value Name: NoFavorites
Value Type: REG_DWORD
Set To: **1 per abilitare, 0 per disabilitare (0 dato per default)**
Note: *Rimuove i Favoriti dal menu di Internet Explorer.*

Rifiuta un Menu contestuale (Tasto destro del mouse)
Key: (HKCU|HKLM)\Software\Policies\Microsoft\Internet Explorer\Restrictions
Value Name: NoBrowserContextMenu
Value Type: REG_DWORD
Set To: **1 per abilitare, 0 per disabilitare (0 dato per default)**
Note: *Rimuove l'abilità di poter cliccare con il tasto destro del mouse in IE*

Rimuovi File -> Apri Menu
Key: (HKCU|HKLM)Software\Policies\Microsoft\Internet Explorer\Restrictions
Value Name: NoFileOpen
Value Type: REG_DWORD
Set To: **1 per abilitare, 0 per disabilitare (0 dato per default)**
Note: *Rimuove il File->Apri che può essere usato per lanciare altri programmi. Aiuta a mantenere ripulito una macchina Kiosk, ma i permessi di NTFS potrebbero anche essere usati per limitare che i programmi siano conclusi dall'utente finale.*

Rimuove File -> Salva come Menu
Key: (HKCU|HKLM)Software\Policies\Microsoft\Internet Explorer\Restrictions
Value Name: NoBrowserSaveAs
Value Type: REG_DWORD

Set To: **1 per abilitare, 0 per disabilitare (0 dato per default)**
Note: *Rimuove il File->Salva Come che può essere usato per lanciare altri programmi. Aiuta a mantenere ripulito una macchina Kiosk, ma i permessi di NTFS potrebbero anche essere usati per limitare che i programmi vengano caricati dall'utente finale.*

Rimuove la barra degli indirizzi (Address Bar)
Key: HKLM\Software\Policies\Microsoft\Internet Explorer\Toolbars\Restrictions
Value Name: NoAddressBar
Value Type: REG_DWORD
Set To: **1 per abilitare, 0 per disabilitare (0 dato per default)**
Note: *Rimuove la barra degli indirizzi, e disabilita Explorer, potete usare una singola pagina HTML come l'interfaccia del computer su una macchina kiosk.*

Impostazioni automatiche di update

Note: *Queste impostazioni permettono all'utente di schiarire i toni come gli Updates automatici che vengono caricati dal sistema. Inoltre, molte di queste impostazioni possono essere impostate via Policy di Group usando le maschere di default spediti in 2k e 2k3.*

Updates automatici
Key: HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU
Value Name: NoAutoUpdate
Value Type: REG_DWORD
Set To: **1 per abilitare, 0 per disabilitare (0 dato per default)**
Note: *Questa è la chiave per DISABILITARE gli update automatici. Perciò se viene impostata ad 1 abilita il rifiuto automatico degli updates. In altre parole, impostate a 1 per evitare che il computer faccia gli updates automatici.*

Updates automatici- Opzioni
Key: HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU
Value Name: AUOptions
Value Type: REG_DWORD
Set To: **2, 3, 4, 5**
Note: *Queste opzioni controllano se il pc esegue il download degli updates su se stesso, o se esso chiama l'utente quando cè un nuovo download degli updates pronto. Esso anche controlla se il servizio installerà gli updates, o l'utente li installerà più tardi dal prompt del Dos. 2 vi chiamerà quando ci sono gli updates da scaricare. 3 li scaricherà automaticamente, e domanderà per un installazione. 4 farà tutto automaticamente, ma non dovrà finire l'installazione fino a che non ci sarà il riavvio del pc. per usare 4, dovete avere* ScheduledInstallDay *e* ScheduledInstallTime impostati. *5 forza automaticamente gli updates per essere abilitati, ma permette di configurarli all'utente finale.*

Updates automatici - Installazione delle Opzioni
Key: HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU
Value Name: ScheduledInstallDay
Value Type: REG_DWORD
Set To: **0~7**
Note: *Controlla su cosa verranno installati gli aggiornamenti ogni giorno. 0 è giornalmente, mentre 1~7 è l'impostazione di un giorno della settimana, Domenica (1, n.d.t.) a Sabato (7, n.d.t.).*

Updates automatici- Installazione Opzioni 2
Key: HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU

Value Name: ScheduledInstallTime
Value Type: REG_DWORD
Set To: **0~23**
Note: *Controlla in quante ore Windows installerà gli aggiornamenti, formate in 24 ore*

Updates automatici - Riavvio automatico quando l'utente si logga
Key: HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU
Value Name: NoAutoRebootWithLoggedOnUsers
Value Type: REG_DWORD
Set To: **0 or 1**
Note: *Controlla se Windows riavvia automaticamente quando un utente è loggato. Impostato a 1 l'utente si riavvierà dal prompt del Dos, mentre impostato a 0 causerà l'aggiornamento automatico per notificare all'utente che il computer sarà riavviato. Il tempo di default fino al riavvio è di cinque minuti.*

TCP\IP impostazioni in Windows 2003

Note: *Queste impostazioni sono basate su Windows 2003. Qualcuna può esser applicata a 2k e XP, e poche chiavi di esse possono lavorare su sistemi basati su 9x. Ma queste sono primariamente mirate per Windows 2K3 servers. Tutte le chiavi listate qui possono essere cercate all'interno del lavoro "*Microsoft Windows Server 2003 TCP/IP Implementation Details*", listato nella sezione delle referenze di questo lavoro.*

Permette Raw Sockets per gli utenti (Windows 2003)
Key: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
Value Name: AllowUserRawAccess
Value Type: REG_DWORD
Set To: **1 per abilitare, 0 per disabilitare (0 dato per default)**
Note: *Di default, solo gli amministratori posso accedere al raw sockets su un sistema Windows 2003. Impostato con il valore 1 permette di usare il raw-sockets per tutti gli utenti.*

Arp Cache Keep Alive
Key: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
Value Name: ArpCacheLife
Value Type: REG_DWORD
Set To: **0 to 0xFFFFFFFF (4,294,967,295 Decimale)**
Note: *Controlla il tempo, in secondi, che un pacchetto ha in entrata senza la cache ARP. Senza questa chiave, di defaults sono due minuti per le entrate non usate, e 10 minuti per le entrate usate.*

Data Base Path
Key: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
Value Name: DatabasePath
Value Type: REG_EXPAND_SZ
Set To: **Path to files. (Default: %SystemRoot%\system32\drivers\etc)**
Note: *Questo controlla il path di TCP\IP dei files database, Hosts, Lmhosts, Reti, Protocolli, Servizi. Qualche volta modificati da malware per aggirare le restrizioni sugli hosts dei files.*

Default Time To Live
Key: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
Value Name: DefaultTTL
Value Type: REG_DWORD

Set To: **0~0xFF (0~255 Decimale, 128 Default)**
Note: *Aggiunge il TTL uscente dal pacchetto IP. Alzare il valore di TTL può causare un largo aumento di ping in broadcast se i routing loops sono formati in network topology.*

Disabilita Offloading sulla scheda di rete
Key: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
Value Name: DisableTaskOffload
Value Type: REG_DWORD
Set To: **1 per abilitare, 0 per disabilitare (0 dato per default)**
Note: *Permette le funzioni nello stack del TCP\IP per essere svolto dall'hardware nella scheda di rete. Disabilitando questa chiave verrà causato un sovraccarico nella CPU siccome il sistema deve trattare tutte le funzioni e non una sola. La sua abilitazione è usata solo per ricercare dei guasti.*

Abilitare Detect Dead Gateway
Key: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
Value Name: EnableDeadGWDetect
Value Type: REG_DWORD
Set To: **1 abilitare, 0 per disabilitare (1 dato per default)**
Note: *Questo causa TCP per scoprire se il gateway principale è caduto, e svierà a ogni gateway secondario configurato nelle proprietà di TCP\IP.*

Abilitare Multicast Forwarding
Key: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
Value Name: EnableMulticastForwarding
Value Type: REG_DWORD
Set To: **1 per abilitare, 0 per disabilitare (0 dato per default)**
Note: *Questo controlla se il computer inoltrerà i pacchetti di Multicasts incrociandosi sulle reti. Questo è solo usato quando il computer è caricato come un Routing e Server di Accesso Remoto (RRAS).*

Abilitare Path MTU Discovery
Key: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
Value Name: EnablePMTUDetect
Value Type: REG_DWORD
Set To: **1 per abilitare, 0 per disabilitare (1 dato per default)**
Note: *Controlla se windows cercherà di scoprire il Maximum Transmission Unit (MTU) sul path a un host remoto. Se il MTU usato è grande quanto ciò che è supportato, allora il pacchetto verrà frammentato nel trasporto. La frammentazione può causare una congestione della rete ed eccede il caricamento sui dispositivi di rete come essi assemblano i pacchetti di nuovo in un'unità intera.*

Syn Attack Protection
Key: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
Value Name: SynAttackProtect
Value Type: REG_DWORD
Set To: **1 per abilitare, 0 per disabilitare (1 dato per default su Windows 2K3 con SP1, 0 dato per default su 2K3 con SP0)**
Note: *Abilita la protezione SYN attack nei flussi SYN-ACK. Siete pregati di vedere le Implementazioni nella sezione delle referenze di Windows 2003 TCP\IP per più informazioni. E' raccomandato che sia impostato a 1 su tutte le configurazioni SP0, se SP1 non può installarlo per alcune ragioni.*

Referenze usate:

Configure Automatic Updates in a Non-Active Directory Environment:
http://technet2.microsoft.com/WindowsServer/en/Library/75ee9da8-0ffd-400c-b722-aeafdb68ceb31033.mspx

Microsoft Windows Server 2003 TCP/IP Implementation Details:
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/networking/tcpip03.mspx

Description of the Microsoft Windows registry:
http://support.microsoft.com/default.aspx?scid=kb;EN-US;256986

Differences between Regedit.exe and Regedt32.exe:
http://support.microsoft.com/kb/141377/

Registry Functions:
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/sysinfo/base/registry_functions.asp

Inside the Registry - By Mark Russinovich (Windows NT Magazine)
http://www.microsoft.com/technet/archive/winntas/tips/winntmag/inreg.mspx

Understanding Policy "Tattooing":
http://www.gpoguy.com/FAQs/tattoo.htm