ADEGUAMENTO ALLE NORME DI SICUREZZA
DEI PERSONAL COMPUTERS IN DOTAZIONE PRESSO L'AMMINISTRAZIONE CENTRALE
PER L'ACCESSO ALLE PIATTAFORME E L'UTILIZZO DEL PROGRAMMA WEBRAINBOW

1. Descrizione qualitativa degli interventi
   - sopralluogo tecnico e classificazione delle piattaforme raggruppate per medesimo HAL (Hardware Abstraction Layer);
   - esecuzione di uno studio di fattibilita' relativo alla definizione un modello di configurazione e sicurezza caratterizzato da:
     - Attivita' di sviluppo e programmazione per l'ottimizzazione e l'automazione relative a:
       - l'aggiornamento dell'impronta virale del software antivirus;
       - la mappatura delle aree di storage distribuito presso i LNF e la connessione delle risorse associate contestualmente al login utente;
       - il cambio password di accesso a Windows ed AFS contestualmente al monitoraggio della stato della quota AFS utente;
       - la connessione guidata e autenticata alle piattaforme di rete per la condivisione di un'unica timbratrice di protocollo tra piu' utenti;
     - definizione del workflow delle procedure da attuare per le installazioni da scratch, per le clonazioni e per gli account utenti come descritto in *Allegato A;*
     - elaborazione di nota tecnica di riferimento per le procedure installazione e configurazione come da *Allegato B;*
   - installazione da scratch per le piattaforme master, appartenenti a profili hardware distinti, con conseguente generazione delle immagini di gruppo;
   - clonazione delle piattaforme in base al gruppo di appartenenza;
   - personalizzazione di ciascuna piattaforma e creazione degli specifici account utente;
   - generazione di un'immagine host di installazione per ogni piattaforma installata;
   - fornitura di una copia di backup di tutti i drivers e dei componenti software installati;
   - svolgimento attivita' di tutoraggio sui principi fondamentali d'uso dei PC nell'ambito di un corso basato su proiezione di slides ed esercitazione pratiche.

2. Presupposti ed obiettivi che contraddistinguono le installazioni

Sicurezza

- sono stati definiti specifici gruppi di utenza ai quali esclusivamente e' stato garantito l'accesso locale/di rete alle piattaforme: mediante restrittivi criteri di sicurezza, e' stato inibito l'accesso ai SID di default;
- gli utenti che utilizzano le piattaforme non sono amministratori delle stesse;
- e' stato implementato un particolare modello di poliche, basato su *Criteri di Gruppo*, mediante il quale ogni account utente eredita un unico profilo di impostazioni e sicurezza, comprensivo della configurazione di *Webrainbow*, che non puo' essere modificato dallo stesso utente;
- ogni utente memorizza i propri files e le impostazioni del proprio environment in un'area locale definita nell'ambito di una partizione specifica, distinta da quella di sistema/boot, mediante implementazione dei *Profili di Roaming* locali: in caso di corruzione del file system proprio del S.O., i profili utente non vengono persi: mediante clonazione dell'immagine di host, l'installazione della piattaforma e' ripristinata *ab origine* ma agli utenti sono disponibili i rispettivi profili aggiornati all'ultimo accesso;
- ogni piattaforma aggiorna con frequenza giornaliera la definizione dei nuovi virus mediante download schedulato notturno del nuovo file relativo all'impronta virale, rilasciato dal fornitore del software antivirus.

Efficienza

- le impostazioni di configurazione a carico dell'utente sono drasticamente ridotte, poiche' ereditate in automatico in fase di login;
- ogni utente effettua il login integrato Windows-AFS, ottenendo un token AFS contestualmente all'accesso alla postazione;
- opportune procedure software semplificano all'utente l'accesso e il monitoraggio del proprio spazio di storage su AFS;
- gli utenti hanno a disposizione degli strumenti di alto livello per il semplice cambio delle password di accesso a Windows ad AFS e per la sincronizzazione delle corrispondenti credenziali di accesso;
- l'utente puo' stampare timbri di protocollo anche su una timbratrice di rete, mediante una procedura guidata di localizzazione e autenticazione delle piattaforme di timbratura disponibili.

Frascati, 29 aprile 2005

Nunzio AMANZI
Windows System Manager

ALLEGATO A - WORKFLOW DELLE PROCEDURE DI CONFIGURAZIONE

Procedure relative all'installazione da scratch per le piattaforme master

1. OPERAZIONI PRELIMINARI DI INSTALLAZIONE/CONFIGURAZIONE (DA ESEGUIRE FUORI RETE)
   - Installazione drivers componenti hardware
   - Disabilitazione *condivisione file semplice*
   - Abilitazione modalita' di accesso CTRL+ALT+CANC e disabilitazione del *fast switching user*
   - Disabilitazione del *windows snapshot*
   - Installazione Norton Antivirus ed esecuzione updates mediante file aggiornato dell'impronta virale
   - Customizzazione Componenti Windows
     - Installazione *Client LPR*
     - Rimozione *MSN Explorer* e *Windows Messenger*
     - Installazione eventuale servizi fax
   - Ottimizzazione gestione dei profili energetici
2. IMPOSTAZIONI DI RETE
   - Definizione statica del nome host e del suffisso dns primario
   - Impostazone DHCP
   - Attribuzione suffissi dei domini padri di quello primario e specifici della connessione per nomi non qualificati
   - Disattivazione aggiornamento record dns primario e specifico per la connessione
   - Abilitazione *netbios over tcp*
3. PROCEDURE DI PATCHING E UPDATING (CONNESSIONE IN RETE)
   - Aggiornamento impronta virale Norton *on-fly* mediante download nuove definizioni virus
   - Windows Update (incluso .Net Framework 1.1 + patches)
   - Configurazione Windows Update per il download automatico, ma l'installazione presidiata
4. INSTALLAZIONE APPLICATIVI
   - Office + Patches
   - LNF Tools (Emacs, Winscp3, Putty,Ws_FTP, Mozilla, Editpad, AcrobatReader)
   - Client OpenAFS e relativa configurazione
   - Eventuale installazioni componenti e risorse per il protocollo informatico
5. ESECUZIONE WINDOWS UPDATE
6. CREAZIONE ACCOUNT GRUPPI/UTENTI E RELATIVE POLITICHE
7. INSTALLAZIONE E CONFIGURAZIONE SCRIPTS E TOOLS DI GESTIONE
   - Procedure per la mappatura aree AFS e definizione shortcut sul menu'avvio/desktop
   - Installazione *update virus definition script*, disabilitazione dei Norton Automatics Update
   - Installazione utility per la connessione di una timbratrice remota di protocollo (utility *QuickDymo*)
   - Installazione script di login (mapping automatico aree AFS)
   - Installazione Task Scheduler Service, configurazione della modalita' di avvio e definizione dei tasks
   - Definizione di un'attivita' pianificata di scansione eseguita dal software antivirus
8. DEFINIZIONE *CRITERI DI GRUPPO* E POLITICHE DI SICUREZZA
9. IMPOSTAZIONI SUI SERVIZI
   - Disabilitazione *Messenger*
   - Disabilitazione Servizio *SSDP* (UPnP)
   - Abilitazione *RDP-Tcp*
   - Disabilitazione assistenza remota
10. INSTALLAZIONE E CONFIGURAZIONE PERIFERICHE/SERVIZI DI I/O
    - Configurazione stampanti locali/di rete
    - Predisposizione/Configurazione Servizi fax
    - Configurazione timbratrice protocollo, implementazione modello di accesso in locale e da rete
11. ESAME DELLE VULNERABILTA' DEL NODO DI RETE – ESECUZIONE AZIONI DI CONTRASTO
12. DEFINIZIONE DI UN PROFILO UTENTE STANDARD
    - Creazione di un accont *user* temporaneo
    - Imposizione stile classico di windows per la GUI
    - Ottimizzazione delle prestazioni e degli effetti visivi
    - Ottimizzazione impostazioni Desktop
      - Eliminazione sfondo
      - Screen saver di default a 20 min. protetto da password
      - Attivare la visualizzazione del folder *Documenti* e di *Internet Explorer*
    - Ottimizzazione della barra delle applicazioni
    - Impostazioni relative alle cartelle di *Esplora Risorse* (come variazione rispetto a quelle di default)
      - Disattivazione ricerca cartelle e stampanti di rete
      - Disattivazione utilizzo condivisione file semplice
      - Attivazione visualizzazione estensioni anche per i file noti
      - Visualizzazione dei file in modalita' dettagli per tutti i folder
      - Esecuzione Windows Explorer in un processo separato
    - Impostazioni avanzate per *Internet Explorer*
      - Utilizzo FTP passivo
      - Stampa colori e immagini di fondo
    - Impostazioni relative a Mozilla Firefox
      - Disabilitazione controllo browser predefinito
      - Impostazione home page
      - Blocco finestre popup ad eccezione dei siti infn.it
      - Installazione software consentito per i siti infn.it
      - Richiesta del path per il download dei file
    - Esecuzione delle impostazioni relative al programma *Webrainbow*
    - Copia del profilo di *user* in *Default User* e distruzione dell'account temporaneo
13. ATTIVAZIONE PROFILI DI ROAMING LOCALI
    - Definizione e formattazione di una partizione specifica sul disco rigido
    - Configurazione del folder root dei profili
14. PROCEDURE CONCLUSIVE DEL PROCESSO DI INSTALLAZIONE E CONFIGURAZIONE
    - Attivazione snapshot sulla partizione di sistema (~600 Mb)
    - Deframmentazione partizione di Sistema
    - Pulitura registri eventi ed esecuzione immagine della partizione di sistema

Procedure relative all'installazione delle piattaforme cloni

1. CLONAZIONE DELLA PIATTAFORMA
    - Individuazione dell'immagine master ed esecuzione del clonino
    - Esecuzione controllo compatibilità HAL (Hardware Abstraction Layer) ed eventuali misure correttive
    - Correzione dell'associazione Alias-SID specifici per le piattaforme che prevedono *IIS*
    - Definizione nuovo nome host e eliminazione del vecchio nel Registro di Configurazione
2. INTERVENTI DI PERSONALIZZAZIONE DELLA PIATTAFORMA
    - Attivazione dei profili di roaming locali, rif. punto 13 delle procedure relative alla piattaforma master
    - Installazione e configurazione componenti hardware/software specifici

Procedure specifiche per gli account da eseguire successivamente al fasi di mastering o cloning

- Definizione dell'account e della relativa membership, in base alle politiche di accesso e sicurezza
- Definizione del path di roaming del profilo
- Definizione del path del folder Documenti, esterno al profilo di roaming
- Definizione eventuali connessioni a stampanti e risorse di rete proprie del profilo
- Creazione della struttura *Menu' Avvio\LNF Tools\LNF Places\AFS Drivers* nell'ambito del profilo
- Creazione dello shortcut ASF Home -> \\afs\lnf\user\home\%username% nel folder *Menu' Avvio\LNF Tools\LNF Places* propria dell'utente
- Creazione dello shortcut ASF Home -> \\afs\lnf\user\home\%username% nel folder Documenti
- Creazione dello shortcut AFS Home -> H: nel folder *Menu' Avvio\LNF Tools\LNF Places\AFS Drivers* dell'utente e nel Desktop
- Eventuale reset della password AFS/Mail
- Configurazione mail account
- Configurazione/personalizzazione Explorer e Mozilla
- Verifica configurazione programma Webrainbow
- Cambio password login + AFS a cura dell'utente
- Verifica funzionale

ALLEGATO B - NOTE RELATIVE ALLE PROCEDURE DI INSTALLAZIONE E CONFIGURAZIONE

1 - Gestione delle partizioni

HDA1 – 12,69 Gb C: (NTFS) – Label: System Sistema - Boot	HDA2 – 24,57 Gb S: (NTFS) – Label: Storage Profili Utente Roaming Locale Storage in genere

2 - Parametri generali dell'host di rete

Nome Host: statico corrispondente al nome DNS non qualificato
Suddiffo DNS Princ.: statico: ac.lnf.infn.it
Gruppo: workgroup
Indirizzo IP: DHCP
Netbios: abilitato over TCP
Impostazioni DNS: attribuzione dei suffissi domini padre del suffisso primario abilitata – aggiornamento DNS disabilitato

3 - Profilo energetico

Monitor spento: dopo 20 min. di inattivita'
Dischi disattivati: mai
Standby: mai
Sospensione: attiva
Pulsante alimentazione: nessuna azione associata

4 - AFS Client

Autenticazione Windows Integrata: l'utente locale deve possedere le stesse credenziali del corrispondente account AFS.
Nessuna mappatura di *global e user drives* a livello di client: le mappature sono definite nell'ambito di opportuno script di login, eseguito mediante impostazione di specifico *criterio di gruppo*.
Sono definiti i seguenti submounts:

- afs associato a \afs;
- lnf associato a \afs\lnf.infn.it.

Essi sono considerati dal S.O. come shares standard di windows sotto \\afs, quindi nel caso precedente si avra':

- \\afs\afs tutto afs
- \\afs\lnf cella dei laboratori

In base alla definizione dei submounts lo script rende disponibili i seguenti virtual driver:

L \\afs\lnf
I \\afs\infn.it
W \\afs\afs
H \\afs\lnf\user\home\username

5 - Gruppi, Utenti e politiche di accesso

GRUPPI DI SICUREZZA	
Alias/SID	**Note**
Administrators	Definito per default
Backup Operators	Definito per default
Guests	Definito per default – non ammesso per gli accessi alla piattaforma
Network Configuration Operators	Definito per default – nessun utente appartiene a tale gruppo
Power Users	Definito per default – nessun utente appartiene a tale gruppo
Replicator	Definito per default
Users	Definito per default – gruppo base di appartenenza degli utenti che accedono al pc
AFS Clients Admins	Definito dal Client AFS, coinvolge solo l'amministratore
Utenti desktop Remoto	Definito per default – gruppo non utilizzato: nessun utente deve esserne membro
Help Services Group	Definito per default
Utenti Debugger	Definito per default, coinvolge solo l'ammistratore
LocalApplicationUsers	Vi appartengono gli utenti che hanno accesso locale alla postazione
RemoteUsers	Vi appartengono gli utenti che accedono alla postazione da rete
PrintUsers	Vi appartengono gli utenti che accedono alla tibratrice di protocollo

UTENTI	
Alias/SID	**Note**
Administrator	Definito per default
root	Definito per ridondanza
ASPNET	Definito per default -- utilizzato per l'esecuzione di processi legati ad ASP.NET
Guest	Definito per default – deve essere disabilitato
HelpAssistant	Definito per default – deve essere disabilitato
SUPPORT_xxx	Definito per default – deve essere disabilitato
NomeAccount	Utente che accede alla postazione come da tabella dei profili di accesso Nome account e password di login uguali a quelli relativi ad AFS
ProtPrint	Utenza speciale di accesso da rete alla timbratrice per la stampa etichette di protocollo, da altre piattaforme. Non e' ammesso l'accesso in locale.

PROFILI DI UTENZA PER L'ACCESSO ALLA PIATTAFORMA			
Descrizione profilo	**Gruppi relativi**	**Utenti**	**Note**
Utenza base	Users	--	Non ha alcun tipo di accesso al pc.
Utenza remota	Users RemoteUsers	--	Puo' accedere da rete alle risorse/servizi locali per i quali sono previsti i relativi permessi di accesso. Non ha il diritto di accesso locale.
Utenza remota di accesso alla timbratrice di protocollo	Users RemoteUsers PrintUsers	ProtPrint	Puo' accedere da rete alle risorse/servizi locali per i quali sono previsti i relativi permessi di accesso. Non ha il diritto di accesso locale. Puo' stampare da remoto etichette di protocollo sulla timbratrice locale.
Utenza standard locale – utilizzo del protocollo	Users RemoteUsers LocalApplicationUsers PrintUsers	NomeAccount	Puo' accedere da rete alle risorse/servizi locali per i quali sono previsti i relativi permessi di accesso. Puo' accedere in locale. Puo' stampare, da remoto e in locale, etichette di protocollo sulla timbratrice locale.
Profilo amministrativo standard	Administrators AFS Clients Admins Utenti Debugger	Administrator root	Accedde a tutti I servizi e Applicazioni, in locale, da rete e tramite terminal services. N.B.: L'account root e' utilizzato come ridondanza dell'accesso amministrativo. Si consiglia l'utilizzo di tale account per gli accessi ordinari: Administrator deve essere utilizzato solo per operazioni di emergenza e disaster recovery.

6 - Permessi di accesso alle stampanti locali

Generalmente i diritti di accesso alla stampanti sono quelli di default, fermo restando che per la stampa da rete su netbios, l'utente deve essere membro del gruppo **RemoteUsers**.

Alle impostazioni di default fa eccezione il profilo di accesso alla timbratrice che comporta l'appartenenza al gruppo **PrintUsers** per la stampa locale e anche al gruppo **RemoteUsers** per la stampa da rete, come meglio specificato nella precedente tabella.

Per la timbratrice lo schema delle ACL e' il seguente:

	MODELLO ACL RELATIVE ALLA TIMBRATRICE			
	Administrators	**Administrators**	**CREATOR OWNER**	**PrintUsers**
Print	Allow	-	-	Allow
Manage Printers	Allow	-	-	-
Manage Documents	-	Allow	Allow	-
Read Permissions	Allow	Allow	Allow	Allow
Ch'ange Permissions	Allow	Allow	Allow	-
Take Ownership	Allow	Allow	Allow	-
Apply unto	Printer only	Documents only	Documents only	Printer only
Note	-	-	-	-

Nome condivisione: *dymo*

Sul pc che esporta la timbratrice deve essere definito il folder *c:\usr*, esportato in sharing come *usr*, e garantire al gruppo **PrintUsers** i relativi permessi di lettura, secondo il seguente schema:

MODELLO PERMESSI PER IL FOLDER DI AUTENTICAZIONE REMOTA		
Gruppi	**Permessi locali**	**Permessi di sharing**
Administrators	Full Control	Read
SYSTEM	Full Controll	-
Users	Default: Read/Traverse	-
PrintUsers	Default: Read/Traverse	Read

7 - Stampa su una timbratrice di rete

Per stampare da rete sulla timbratrice locale e' necessario accedere con le credenziali dell'utente locale abilitato al protocollo, ovvero accedere con privilegi ridotti utilizzando l'account **ProtPrint**.

Per connettere una timbratrice di rete, utilizzare lo specifico tool *Connetti Timbratrice* presente sul menu'/desktop utente.

8 - Impostazione *Criteri di Gruppo*

Tali impostazioni sono caratterizzate da quanto segue:

- i criteri computer sono validi per tutti gli utenti;
- i criteri utente sono applicati a tutti gli account ad eccezione di quelli appartenenti al gruppo *Administrators*.

Questa implementazione basata sul filtraggio delle politiche di gruppo e' ottenuta negando a regime la lettura del file:

C:\windows\system32\GroupPolicy\User\Registry.pol

al gruppo *Administrators*: l'accesso in lettura puo' essere temporaneamente ripristinato solo per operazioni di management.

Poiche' i criteri applicati sono memorizzati (cache) nel profilo dell'utente, e' opportuno predisporre un file di impostazioni che possa essere attivato temporaneamente durante operazioni di management: tale file definisce un insieme minimale di criteri rispetto a quello ordinario applicato agli utenti non mministrativi.

In tal senso nello stesso folder di cui sopra sono presenti, oltre al file *Registry.pol*, i file *Registry_Admin.pol* e *Registry_User.pol*, rispettivamente copie delle impostazioni amministrative e delle impostazioni a regime definite per gli utenti non amministrativi.

Procedure operative per la definizione dei criteri:

1) definire i criteri computer in base alla tabella relativa a seguito
2) definire i criteri utente riservati agli amministratori come da relativa tabella a seguito
3) copiare il file *C:\windows\system32\GroupPolicy\User\Registry.po*l in *.\Registry_Admin.po*;
4) per ogni account amministrativo eseguire il login/logoff per l'applicazione e caching dei criteri
5) definire i criteri utente per tutti gli utenti come da relative tabella a seguito
6) copiare il file *C:\windows\system32\GroupPolicy\User\Registry.pol* in *.\Registry_User.pol*
7) negare l'accesso in lettura agli Administrators per il file *Registry.pol*

Da notare che le impostazioni/modifiche dei criteri sono effettive dopo il successivo logoff/login utente.

CRITERI COMPUTER		
Criterio	**Impostazione**	**Note**
Computer Settings/Impostazioni Windows/Protezione/Criteri locali/diritti utente		--
Accesso locale	Administrators LocalApplicationUsers	
Accesso dalla rete	Administrators RemoteUsers ASPNET	
Consenti Accesso Servizi Terminal	Administrators	
Computer Settings/Impostazioni Windows/Protezione/Criteri locali/opzioni di protezione		
Non richiedere CTRL+ALT+CANC	Disabilitato	
Consenti di arrestare il sistema senza effettuare l'accesso	Disabilitato	
Computer Settings/Modelli amministrativi/componenti windows/netmeeting		
Disattiva condivisione desktop remoto	Attivato	
Computer Settings/Modelli amministrativi/componenti windows/Internet explorer		
Basa impostazioni proxy sul computer	Attivato	
Disattiva l'installazione automatica dei componenti	Attivato	
Disattiva controllo periodico aggiornamenti	Attivato	
Disattiva avvisi shell per aggiornamenti	Attivato	
Disattiva la visualizzazione dell'area di avvio	Attivato	
Computer Settings/Modelli amministrativi/componenti windows/Utilita' di pianificazione		
Non consentire la creazione di una nuova operazione	Attivato	
Computer Settings/Modelli amministrativi/componenti windows/Servizi Terminal		
Limita gli utenti a una sola sessione remota	Attivato	
Imponi rimozione sfondo desktop	Attivato	
Limita numero connessioni	Attivato = 1	
Rimuovi il comando disconnetti	Attivato	
Controllo remoto	Attivato: full senza aut.	
Reindirizzamento/Appunti	Disattivato	
Rendirizzamento/smartcard	Attivato	
Reindirizzamento/Audio	Disattivato	
Reindirizzamento/COM	Attivato	
Reindirizzamento/Stampante client	Attivato	
Reindirizzamento/Porta LPT	Attivato	
Reindirizzamento/Unita' client	Disattivato	
Reindirizzamento/Stampante client predefinita	Attivato	
Crittografia/Richiedi sempre password	Attivato	
Crittografia/Livello crittografia	Attivato: liv. Princ. 128 bit	
Sessioni/Limite per sessioni disconnesse	Attivato: 30 min.	
Sessioni/Limite sessioni attive	Attivato: 3 ore	
Sessioni/Limite sessioni inattive	Attivato: 1 ora	
Sessioni/Consenti riconnessione dal client originale	Disattivato	
Sessioni/Termina la sessioni ai limiti di tempo	Disattivato	
Computer Settings/Modelli amministrativi/componenti windows/Messenger		
Non consentire l'esecuzione di Messenger	Attivato	
Non avviare automaticamente Messenger	Attivato	
Computer Settings/Modelli amministrativi/Sistema/Accesso		
Esegui questi programmi all'accesso utente	Attivato:	C:\windows\OpenAfsDrvMap.vbs 1
Computer Settings/Modelli amministrativi/Sistema/Accesso		
Attendi disponibilita' di rete all'avvio	Attivato	
Computer Settings/Modelli amministrativi/Sistema/Criteri di gruppo		
Disattiva aggiornamento in background	Attivato	
Computer Settings/Modelli amministrativi/Sistema/Assistenza remota		
Assistenza remota su richiesta	Disattivato	
Offri assistenza remota	Disattivato	

segue **CRITERI COMPUTER**		
Criterio	**Impostazioni**	**Note**
Computer Settings/Modelli amministrativi/Sistema/Servizio Ora/Provider Configura client Windows NTP	Attivato	Ntp.lnf.infn.it Tipo:ntp

CRITERI UTENTE PER AMMINISTRATORI		
Criterio	**Impostazioni**	**Note**
UserSettings/Impostazioni windows/Manutenzione Explorer Impostazioni connessione	Impostazioni Manuali	Nessuna connessione di accesso remoto Impostazioni LAN: Rilevazioni automatiche disattivate Elimina impostazioni di connessioni esistenti
Configurazione automatica browser	Disattiva impostazioni automatiche	
Url importanti	Home Page	http://www.ac.infn.it
Protezione/Aree di protezione	Imposta Aree di Prot.	Siti Attendibili: https://gestdoc.lnf.infn.it http://w2kservices.lnf.infn.it Disattiva flag verifica https Attiva tutti gli ActiveX
Programmi	Attivato	Editor: Word Posta: Thunderbird News: Thunderbird Explorer browser predefinito: attivato
UserSettings/Modelli amministrativi/Componenti windows/Internet Explorer Pannello controllo/Disattiva scheda avanzate	Disattivato	-
UserSettings/Modelli amministrativi/Componenti windows/Esplora Risorse Rimuovi la voce opzioni cartella	Disattivato	-
UserSettings/Modelli amministrativi/Desktop Proibisci di cambiare il percorso Documenti	Disattivato	-

CRITERI UTENTE PER ACCOUNT NON AMMINISTRATIVI		
Criterio	**Impostazioni**	**Note**
UserSettings/Modelli amministrativi/Componenti windows/Netmeeting		
Impedisci invio file	Attivato	
Impedisci ricezione file	Attivato	
UserSettings/Impostazioni windows/Manutenzione Explorer		
Impostazioni connessione	Impostazioni Manuali	Nessuna connessione di accesso remoto Impostazioni LAN: Rilevazioni automatiche disattivate Elimina impostazioni di connessioni esistenti
Configurazione automatica browser	Disattiva impostazioni automatiche	
Url importanti	Home Page	http://www.ac.infn.it
Protezione/Aree di protezione	Imposta Aree di Prot.	Siti Attendibili: https://gestdoc.lnf.infn.it http://w2kservices.lnf.infn.it Disattiva flag verifica https Attiva tutti gli ActiveX
Programmi	Attivato	Editor: Word Posta: Thunderbird News: Thunderbird Explorer browser predefinito: attivato
UserSettings/Modelli amministrativi/Componenti windows/Internet Explorer		
Disattiva personalizzazione esterna Browser	Attivato	
Disattiva modifica home page	Attivato	
Disattiva connessione guidata Internet	Attivato	
Impedisci l'utilizzo delle identita'	Attivato	
Configura outlook express	Attivato	Blocca gli allegati:attivo
Utilizza rilevamento automatico per le connessioni remote	Disattivato	
Disabilita modifica imp. Configurazione automatica	Attivato	
Disabilita modifica controllo browser predefinito	Attivato	
Pannello Controllo/disattiva la scheda protezione	Attivato	
Pannello Controllo/Disattiva scheda connessioni	Attivato	
Pannello controllo/Disattiva scheda programmi	Attivato	
Pannello controllo/Disattiva scheda avanzate	Attivato	Questo criterio comporta che le impostazioni vengano prima salvate come profilo standard da memorizzare in DefaultUser
UserSettings/Modelli amministrativi/Componenti windows/Esplora Risorse		
Nascondi le unita' specificate in risorse computer	Attivato	Tutte le unita'
Rimuovi la funzione creazione CD	Attivato	
Rimuovi la scheda protezione	Attivato	
Disattiva interfaccia per modifica imp. Animazioni	Attivato	
Rimuovi la voce opzioni cartella	Attivato	Questo criterio comporta che le impostazioni vengano prima salvate come profilo standard da memorizzare in DefaultUser
Esclusione di Tutta la rete da Esplora Risorse		
UserSettings/Modelli amministrativi/Desktop		
Proibisci di cambiare il percorso Documenti	Attivato	Relativo ai profili di Roaming Da attivare dopo la creazione degli account
UserSettings/Modelli amministrativi/Pannello Controllo		
Imponi pannello controllo classico	Attivato	
UserSettings/Modelli amministrativi/Sistema/Profili Utente		
Escludi directory nel profilo comune	Attivato	Documenti Relativo al profilo di Roaming

9 - Esecuzione delle impostazioni utente: procedure per il management e la disattivazione dei *Criteri di Gruppo Utente*

L'esecuzione delle seguenti impostazioni utente dipendono dalla definizione del relativo criterio come da seguente tabella:

Operazione	Criterio coinvolto
Definizione path documenti dell'utente	**UserSettings/Modelli amministrativi/Desktop** Proibisci di cambiare il percorso Documenti
Impostazioni avanzate di Internet Explorer	**UserSettings/Modelli amministrativi/Componenti windows/Internet Explorer** Pannello controllo/Disattiva scheda avanzate
Modifica delle opzioni utente di Esplora Risorse	**UserSettings/Modelli amministrativi/Componenti windows/Esplora Risorse** Rimuovi la voce opzioni cartella

Al fine di poter definire correttamente il profilo di ciascun account e' quindi necessario ripristinare temporaneamente l'esecuzione dei criteri utente meno restrittivi (riservati agli amministratori) come da seguente procedura:

1) accedere come amministratore, ripristinando i permessi di lettura per il file *Registry.pol*
2) eliminare il file *Registry.pol*
3) copiare il file *Registry_Admin.pol* in *Registry.pol*
4) aprire il file *Registry.pol* (gpedit.msc)
5) agire su un qualunque criterio utente in modo da aggiornare la data di modifica dello stesso file
6) effettuare il logoff come amministratore ed accedere come utente
7) eseguire le impostazioni utente
8) effettuare il logoff utente ed accedere come amministratore
9) eliminare il file *Registry.pol*
10) copiare il file *Registry_User.pol* in *Registry.pol*
11) agire su un qualunque criterio utente in modo da aggiornare la data di modifica dello stesso file
12) negare l'accesso in lettura agli *Administrators* per il file *Registry.pol*

10 - Profili di Roaming

Ad eccezione degli account *Administrator* e *root*, tutti gli account utenti possiedono un *profilo di roaming locale* definito nella seconda partizione.

Per le impostazioni fare riferimento alla specifica *Documentazione Tecnica*: al fine di poter definire il path del folder *Documenti* dell'utente, eseguire le procedure definite al precedente punto 9.

11 - Attivita' schedulate

Al fine di eseguire operazioni programmate e' installato un servizio opportuno per lo scheduling dei processi denominato *Task Scheduler Service*.
Tale servizio e' avviato in automatico ed eseguito come *SYSTEM*.
Gli eseguibili relativi al servizio e al pannello di controllo sono residenti in *C:\Windows\TaskScheduler*.
Le ACL del folder devono far riferimento al seguente schema:

ACL PER C:\WINNT\TASKSCHEDULER **Disattivare l'ereditarieta' dei criteri dal folder padre**		
	Administrators	SYSTEM
Traverse foldes	Allow	Allow
List Folder	Allow	Allow
Read Attributes	Allow	Allow
Read Extended Att.	Allow	Allow
Create Files/Write	Allow	Allow
Create Folders/Append	Allow	Allow
Write Attributes	Allow	Allow
Write Ext. Attrib.	Allow	Allow
Delete Subf./Files	Allow	Allow
Delete	Allow	Allow
Read Permission	Allow	Allow
Change Permis.	Allow	Allow
Take Ownership	Allow	Allow
Apply unto	Folder/SubF./Files	Folder/SubF./Files
Note	-	-

L'eventuale definizione di uno shortcut di accesso al pannello di controllo deve essere definita solo per l'amministratore.
In tal senso puo' essere creato all'interno del profilo utente amministrativo dentro *menu' avvio\programmi\strumenti di amministrazione.*
Gli script schedulati sono installati nel folder C:\AdminsScripts per il quale e' definito lo stesso modello di ACL come da suddetta tabella.
Impostazione delle attivita' schedulate:

Descrizione	**Comando**	**Orario**	**Note**
Update virus definition	C:\winnt\adminscripts\naup_ftp_run.vbs	02.00	Eseguito ogni notte, tolleranza = 30 min.

In aggiunta alle suddette procedure relative alle attivita' schedulate, e' prevista una scansione programmata della partizione C: e S: nell'ambito del Norton Antivirus.
Nome attivita': completo settimanale
Tipo: settimanale
Giorno/ora: venerdi, 20.00
Unita': C:, S:

ALLEGATO C - CONFIGURAZIONE DEI PROFILI DI ROAMING SU UNA PARTIZIONE LOCALE

Questa procedura descrive le impostazioni da eseguire su una macchina Windows 2000 Pro/XP Pro per definire i profili di roaming definiti su una partizione locale (detta di storage) distinta da quella di boot/sistema.
Un profilo di roaming e' un profilo utente memorizzato su un server di rete o su una partizione di storage locale che non sia di boot.
Al login i folders utente sottoposti a roaming e residenti nella partizione di storage vengono sincronizzati con gli omonimi residenti nello spazio utente sotto %systendrive%\Documents and Settings. Tale spazio e' utilizzato come cache di profilo: durante la sessione di login l'utente interagisce con la propria cache di profilo che e' sincronizzata con lo spazio corrispondente nella partizione di storage al momento del logout.
Poiche' per default la cartella My Document e' interna al profilo, per evitare inutile speco di spazio dovuto ai processi di sincronizzazione, si puo' ottimizzare il roaming in modo che la cartella documenti sia direttamente puntata sulla partizione di storage.
In tal senso la configurazione e' caratterizzata da:

- tutti gli utenti sono sottoposti a roaming del profilo ad eccezione dell'Administrator;
- nel processo di roaming sono conivolti tutti i folder del profilo ad eccezione del folder My Documents;
- il forder My Documents e' memorizzato nella partizione di storage, ma in un'area separata dal profilo (non interna ad esso per non essere convolta nel caching e nel sync.) e linkato come cartella speciale attraverso i puntatori del desktop/Menu' avvio.

In tale scenario:

- L'utente accede al proprio profilo in forma trasparente alle procedure di sincronizzazione;
- Quando viene aperta la cartella Documenti egli accede direttamente al relativo folder nella partizione di storage;
- Se si corrompe la partizione di boot, tutto il profilo e i dati utente sono integri poiche' risiedono in un'altra partizione.

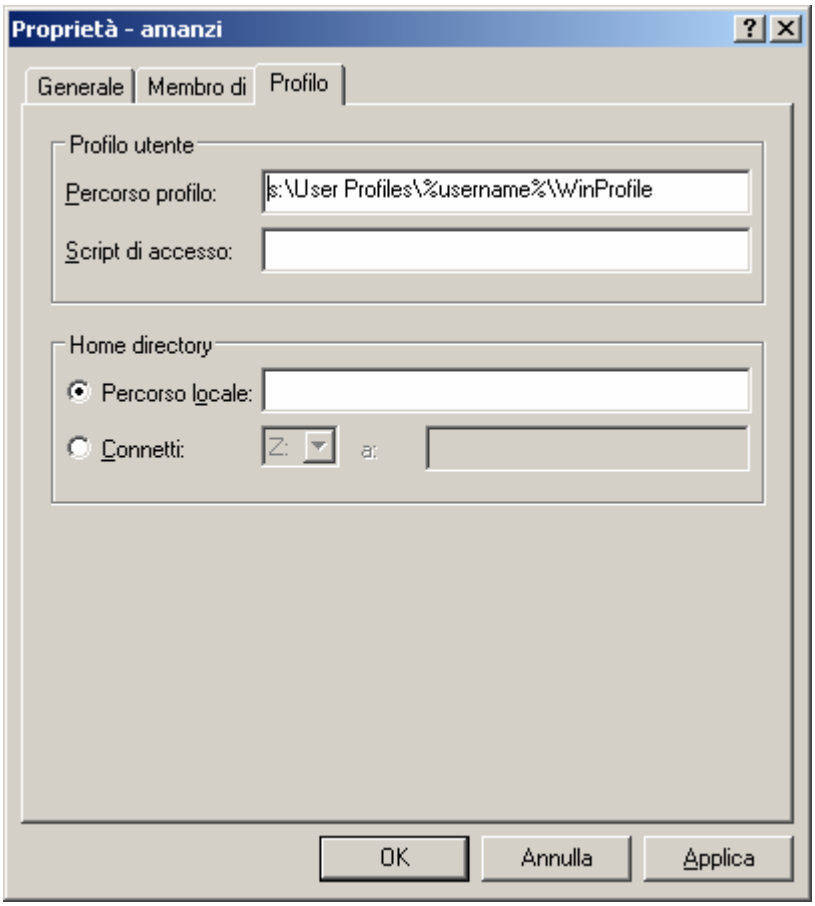
1 – DEFINIZIONE DELLA PARTIZIONE E PREDISPOSIZIONE DELL'AREA DEDICATA AI PROFILI

Sia S l'identificativo della partizione di storage.
Creare il folder s:\User Profiles e definire per esso il seguente modello di protezione per gli accessi. Tale definizione dovra' essere impostata nelle proprieta' avanzate del tab *Protezione.*

ACL PER S:\User Profiles (deve essere **disattivato** il flag relativo all'ereditarieta' delle impostazioni dal padre)						
	Administrators	SYSTEM	CREATOR OWNER	Users	Users	Users
Traverse foldes	Allow	Allow	Allow	Allow	-	-
List Folder	Allow	Allow	Allow	Allow	-	-
Read Attributes	Allow	Allow	Allow	Allow	-	-
Read Extended Att.	Allow	Allow	Allow	Allow	-	-
Create Files/Write	Allow	Allow	Allow	-	-	Allow
Create Folders/Append	Allow	Allow	Allow	-	Allow	-
Write Attributes	Allow	Allow	Allow	-	-	-
Write Ext. Attrib.	Allow	Allow	Allow	-	-	-
Delete Subf./Files	Allow	Allow	Allow	-	-	-
Delete	Allow	Allow	Allow	-	-	-
Read Permission	Allow	Allow	Allow	Allow	-	-
Change Permis.	Allow	Allow	Allow	-	-	-
Take Ownership	Allow	Allow	Allow	-	-	-
Apply unto	Folder/SubF./Files	Folder/SubF./Files	SubFolders and Files	Folder/SubF./Files	Folder and SubFolders	Subfolders only
Note	-	-	Solo l'utente che crea gli oggetti, puo' esercitare il privilegio di owner e come tale puo' assumerne il controllo completo	Permessi standard di lettura/attraversamento esecuzione	Nel folder utente possono esser creati solo subfolders	I file possono esser creati solo nei subfolder del folder utente

2 – CREAZIONE DEGLI UTENTI E DEFINIZIONE DEL PROFILO DI ROAMING
Ad eccezione dell'Administrator, creare gli utenti che devono essere sottoporti al roaming del profilo.
Per ogni utente:

- aprire la relativa finestra delle proprieta' dalla console di management degli utenti;
- rendere l'utente membro del gruppo **Users;**
- mediante il tab *Profile* impostare il *Profile Path* al valore **s:\User Profiles\%username%\WinProfile;**
- effettuare un login e il successivo logout come utente di roaming.



Al termine della sequenza ogni utente avra' creato il proprio spazio sotto **s:\User Profiles.**

3 – PUNTAMENTO DELLA CARTELLA DOCUMENTI
Con questa procedura si evita che i documenti transitino temporaneamente per la cache di profilo, evitando spreco di spazio disco e allungando i tempi di login/logoff.
Per ogni utente:

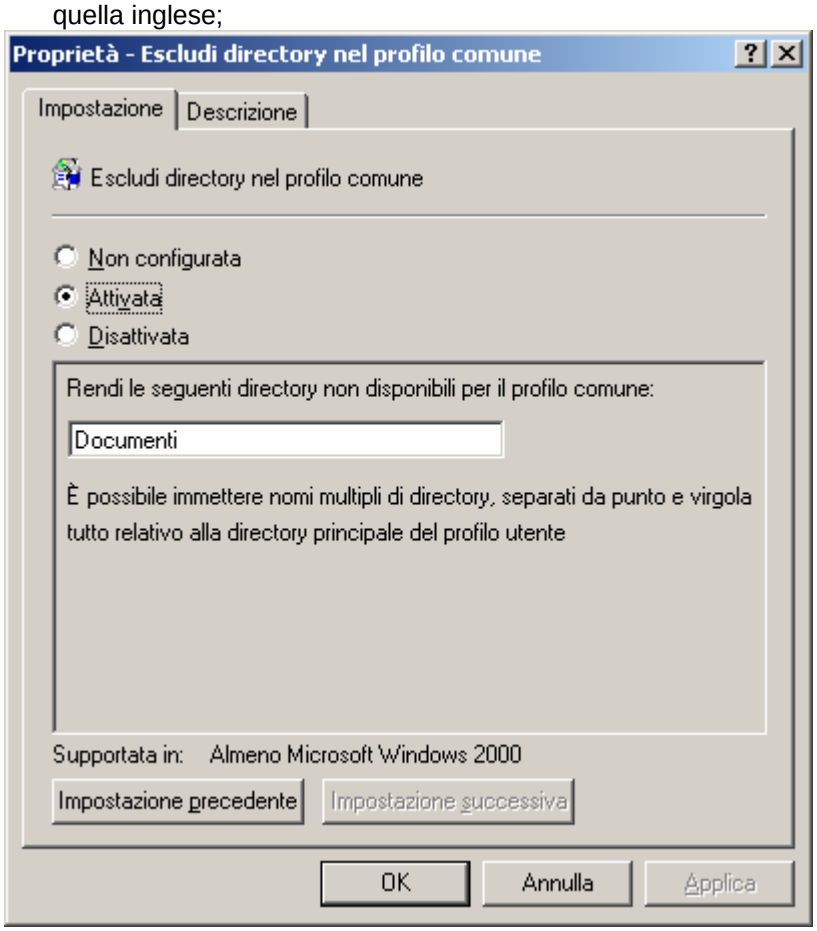
- effettuare il login a windows;
- abilitare l'icona My Documents sul Desktop (proprieta' dello schermo/desktop, tab *Desktop*, click su *Personalizza Desktop*);
- cliccare con il tasto desto sull'icona documenti e selezionare le proprieta';
- nella casella destinazione digitare il percorso della cartella documenti utente: **S:\User Profiles\%username%\WinDocs;**
- premere Applica/OK e confermare sia la creazione del nuovo folder sia lo spostamento del contenuto nella nuova destinazione;
- effettuare il logout da windows.

4 – OTTIMIZZAZIONE DEL PROCESSO DI ROAMING E DI PUNTAMENTO DEI DOCUMENTI
Occorre a questo punto:

- escludere dal roaming la cartella documenti in modo che non venga inutilmente sottoposta al caching di sessione
- inibire all'utente la possibilita' di cambiare il percorso di destinazione della stessa cartella Documenti

Procedere come segue:

- fare login come Administrator (che non e' sottoposto a roaming);
- aprire la console di management gpedit.msc
- localizzare l'impostazione **Escludi directory nel profilo comune** sotto *Configurazione Utente/Modelli amministrativi/Sistema/Profili Utente;*
- aprire le proprieta' della voce, ciccare su attivato e digitare **Documenti**, per la versione italiana, **My Documents**, per quella inglese;



- localizzare l'impostazione Proibisci di cambiare il percorso di Documenti sotto *Configurazione Utente/Modelli amministrativi/Desktop;*
- aprire le proprieta' della voce, ciccare su attivato e confermare;
- chiudere la console di management e da riga di comando digitare: **gpupdate + INVIO.**