INFN-Laboratori Nazionali di Frascati

ESPORTAZIONE DI UN ENVIRONMENT WINDOWS NELLA WAN

ROAMING E PUNTAMENTO SU AFS

CONFIGURAZIONE CLIENT-SERVER DEI CRITERI DI GRUPPO

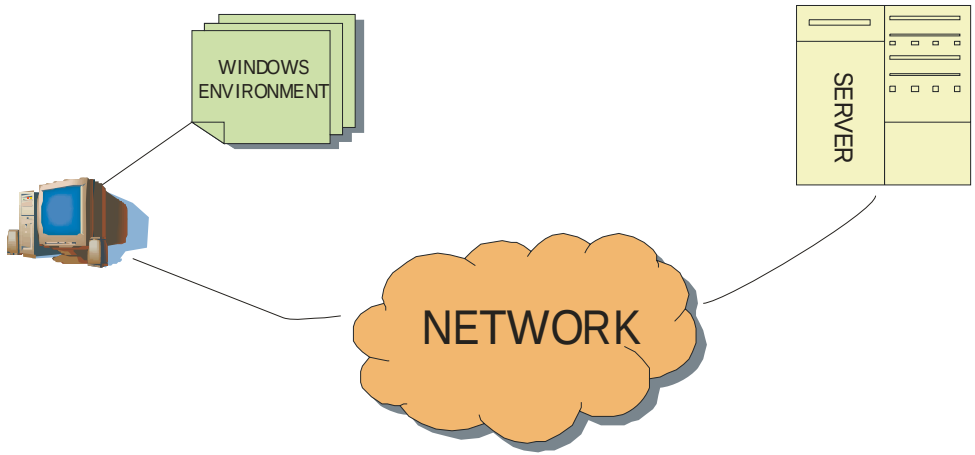
dicembre 2002 - revisione maggio 2003

AMANZI NUNZIO – http://www.lnf.infn.it/~amanzi – nunzio.amanzi@lnf.infn.it

PRESUPPOSTI

Esportare e distribuire in rete un environment windows con le seguenti prerogative:

- collocare la *home dir*, ovvero il *profilo* utente Windows su un server di rete;
- definire le specifiche di accesso e autenticazione in modo tale che lo stesso profilo sia sempre disponibile nella lan e persino nella wan;
- accedere al profilo, ovvero ai propri file, ai bookmarks, alle impostazioni di configurazione, contestualmente alla fase di login dalla postazione client;
- accedere al Windows Environment, e quindi al proprio profilo, anche da postazioni non windows

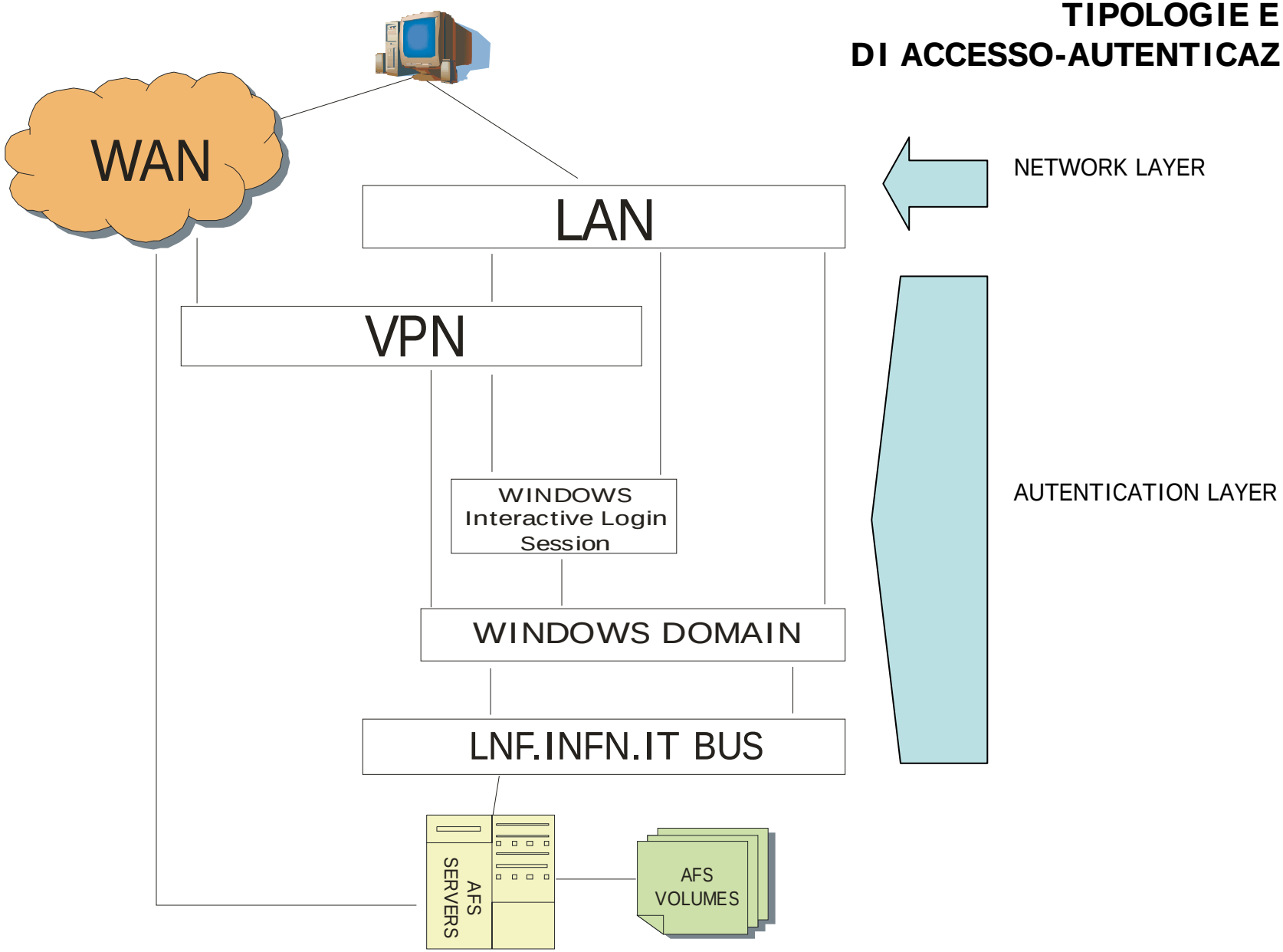


OBIETTIVI

L'interesse di questo complesso studio di fattibilità si è focalizzato sui seguenti aspetti:

- inquadrare gli aspetti connessi con il *Windows Environment Session Login* in forma astratta;
- studiare metodologie di configurazione secondo uno schema client-server;
- implementare nel caso specifico dei LNF – INFN una configurazione basata su:
  - la definizione di gerarchie ed ereditarietà di policies in un ambiente distribuito quale **l'Active Directory**;
  - la *collocazion*e e il *puntamento* del profilo utente windows presso il corrispondente spazio user su **AFS** della cella lnf.infn.it;
  - l'accesso ad AFS nella LAN e nella WAN ottenendo il token contestualmente al login dal client;
  - l'eventuale, fortemente consigliata, autenticazione a livello di **Dominio Windows** in fase di login da client;
  - l'accesso al proprio profilo su AFS mediante apertura di una sessione di login interattivo su server RDP mediante **Windows Terminal Services**.

TIPOLOGIE E FASI
DI ACCESSO-AUTENTICAZIONE



Nell’ambito della definizione di specifiche di configurazione secondo quanto esposto negli *obiettivi* di questo studio sono rilevanti le seguenti problematiche di base:

- Configurazione e gestione di un profilo windows;
- Configurazione e management del *Windows Terminal Services*;
- Active Directory Environment e Criteri di Sicurezza.

PROFILI WINDOWS

• Un profilo utente windows stabilisce una relazione tra account utente e le impostazioni ad esso relative

• Esso contiene le informazioni di configurazione per il desktop, le risorse e le connessioni di rete, le applicazioni

• In particolare, oltre ai file di impostazione, il profilo utente incorpora anche file utente memorizzati all'interno della cartella 'Documenti'

• In tal senso un profilo utente è di fatto un environment utente che, in Windows 2000/XP, è memorizzato per default localmente, all'indirizzo:

unità di sistema\Documents and Settings\nome_user

L'approccio al concetto di Profilo è un tentativo di evoluzione nella gestione, a livello di S.O., di uno spazio utente, emulando quanto avviene in Unix nella directory home.

Nativamente Windows non definisce uno spazio utente specifico, ma utilizza per default la cartella di sistema Windows comune a tutti gli utenti. Le applicazioni sviluppate in questo ambito storico puntano in effetti a questa cartella come unico spazio utente effettuando una query al sistema con la funzione api *getsystemdir()* e sovrapponendo il concetto di home directory con quello di system directory.

Windows 98 intorduce il concetto di Profilo quale sottospazio utente della system dir, al quale accedere mediante nuove funzioni api, disponibili in nuovi file .dll.

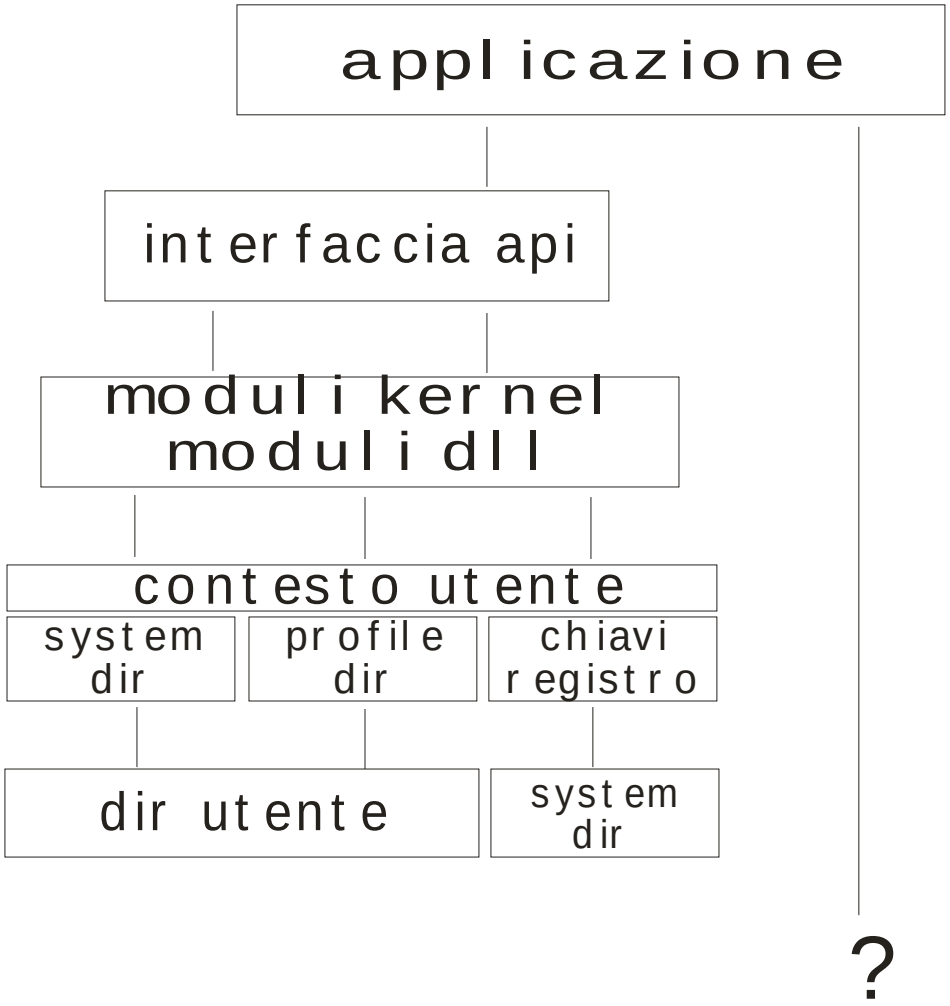
Questa soluzione comporta attualmente la coesistenza di tre fattori che determinano il profilo utente:

• la home dir, alla quale fanno riferimento le applicazioni più vecchie che individuano lo spazio utente nell'ambito della cartella di sistema;

• la cartella che più propriamente definisce il profilo;

• le chiavi di registro di configurazione specifiche per ogni utente memorizzate comunque in un unico file nella cartella di sistema.

Windows 2000/XP permette la configurazione e il reindirizzamento di un profilo intervenendo sui precedenti primi due aspetti.



ACCESSO AL PROFILO UTENTE

La comunicazione tra applicazione può essere schematizzata in base ai livelli di astrazioni raffigurati nel diagramma a fianco.

Il S.O. esporta moduli, in prevalenza librerie a link dinamico, che costituiscono le API di Sistema.

Il dialogo con gli strati sottostanti non è univoco, ma dipende dalla funzione utilizzata, o 'conosciuta' a livello di applicazione.

Poiché alcune impostazioni non sono locali al profilo, ma memorizzate globalmente nel 'Registro di Configurazione', la definizione e configurazione di profili su un server di remoto non è esaustiva in termini di *contesto utente,* poiché risolve solo il dualismo tra *profile dir* e *system dir* facendo puntare entrambe ad un unico spazio utente.

Dalle versioni di Windows 2000, Microsoft introduce il concetto di *Profilo comune o Roaming.*

Un profilo roaming è un ambiente utente memorizzato in un server della LAN o della WAN che utilizza il profilo locale alla macchina come interfaccia cache con l'utente.

Un profilo remoto può inoltre essere *obbligatorio* sul server: un profilo obbligato è un ambiente che esporta impostazioni e file ad un gruppo di utenti i quali vi accedono in lettura, ma non in scrittura, cioè le variazioni a carico del singolo utente restano locali alla propria postazione e non vengono aggiornate sul server.

Il nostro interesse si focalizza sui profili utente comuni ma non obbligatori, cioè su environments gestiti su server remoto e specifici per ogni account utente.

Il *Windows Roaming Profile* è caratterizzato da:

• E' un profilo basato sul server che viene trasferito tramite download al computer locale quando un utente effettua un accesso e viene aggiornato sia sul computer locale che sul server quando l'utente si disconnette.

• Durante la sessione di login l'utente interagisce con il proprio profilo solo localmente, poiché il profilo locale presente per default agisce come una cache del profilo remoto.

Considerazioni Preliminari per i Profili Comuni

• L'account utente e la relativa password devono essere validi sia per la workstation che per il server

• L'accesso al server in fase di login è ottimizzato, poiché vengono trasferiti solo i file non presenti localmente e/o quelli più aggiornati

• In fase di logout la comunicazione con il server si basa su una copia incrementale dei dati locali

• Quando l'utente opera off-line, Windows utilizza il profilo locale che verrà sincronizzato con quello sul server al prossimo login

• Si possono usare anche più macchine client per uno stesso account utente poiché i file utente presenti su una workstation, dopo essere stati trasferiti sul profilo comune, saranno esportati anche verso le altre postazioni. In pratica se un utente dispone di due client A e B contenenti rispettivamente il file_a e il file_b, dopo la loro connessione sequenziale, ciascuna di esse conterrà localmente sia il file_a che il file_b

• La cartella Documenti del desktop client è una cache locale del server: memorizzare in essa i dati significa effettuare un backup incrementale della stessa ad ogni logout

DEFINIZIONE E CONFIGURAZIONE DEI ROAMING PROFILE SU AFS

La configurazione dei profili windows ai LNF INFN è stata caratterizzata dall'utilizzo dei server AFS come roaming servers.

Nel caso di specie si farà quindi riferimento anche alla configurazione del software IBM AFS client per windows, per il quale si dovrà procedere come segue:

• attivare l'opzione *'Obtain AFS tokens when logging into windows*' nella scheda generale della configurazione;

• eliminare ogni eventuale mappatura di devices logici windows verso percorsi AFS sia come global che user drives;

• modificare opportunamente il file afsdsbmt.ini presente nella system dir (in genere C:\WINDOWS o C:\WINNT), in modo che il suo contenuto sia del tipo:

```
[AFS Submounts]
afs=/
lnf=/lnf.infn.it
```

• riavviare windows per rendere effettive le modifiche.

Particolare attenzione va dedicata all'aspetto della mappatura dei devices logici. In tal senso, poiché:

• il client AFS stabilisce una gateway tra i file system FAT/NTFS e UNIX, esportando puntatori, ovvero collegamenti, verso le celle gestiti in windows come folders;

• in Windows la root del file system AFS, ovvero /afs, viene vista come server di rete all'indirizzo **\\nomehost-afs**, dove **nomehost** si ottiene dai primi 11 caratteri del nome del PC client da quale si esegue l'accesso (è quindi fondamentale che i nomi PC abbiano una lunghezza non superiore al predetto limite);

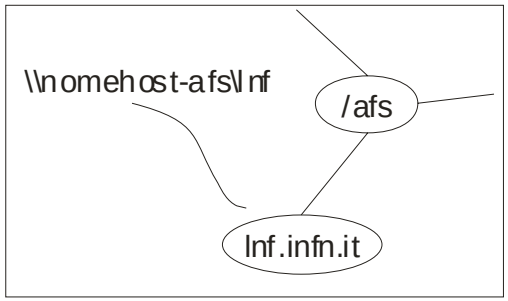
• le celle e le sottodirectory sono accodate alla URL del server in base alla definizione dei submounts di cui al file **afsdsbmt.ini**;

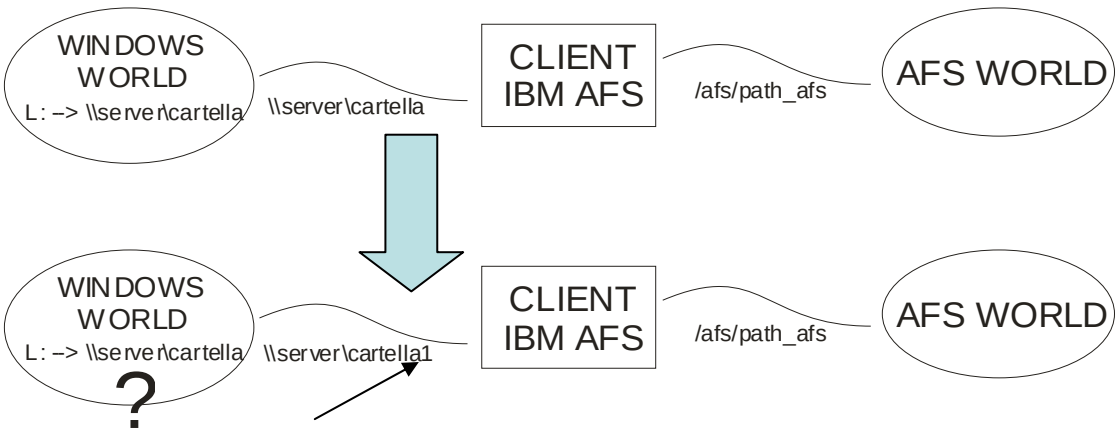
• la mappatura a carico del client AFS non è del tutto robusta, poiché si è riscontrato che modifiche successive alla configurazione dei submounts originale potrebbero rendere le eventuali unità già mappate inservibili;

• nell'ambito della configurazione di un profilo di roaming, la sintassi corretta per indirizzare uno spazio sul server deve avere la forma: **\\nome_server\nome_dir**;

• le specifiche di configurazione devono avere una rilevanza generale, prescindendo dai global drives delle singole postazioni,

Si è preferito, e ritenuto più corretto demadare il compito di mappatura ad opportuni scrips, eseguiti in fase di login, con campo d'azione sia locale che globale (dominio), anche nell'ottica di un approccio astratto alla configurazione client-server.

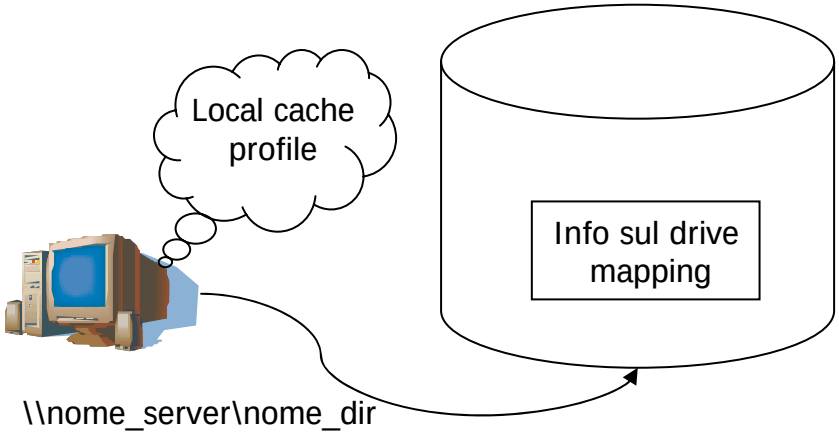




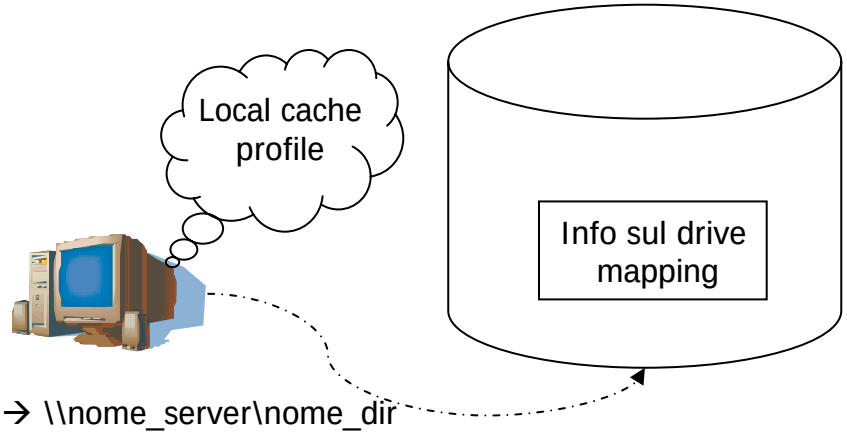
Gatewaying NTFS-NFS

Risoluzione da parte del client windows di un path AFS in un percorso di rete windows in base alle definizioni del file afsdsbmt.ini.

Mancato accesso al path nel caso di utilizzo di devices logici con modifica della definizione dei submounts.

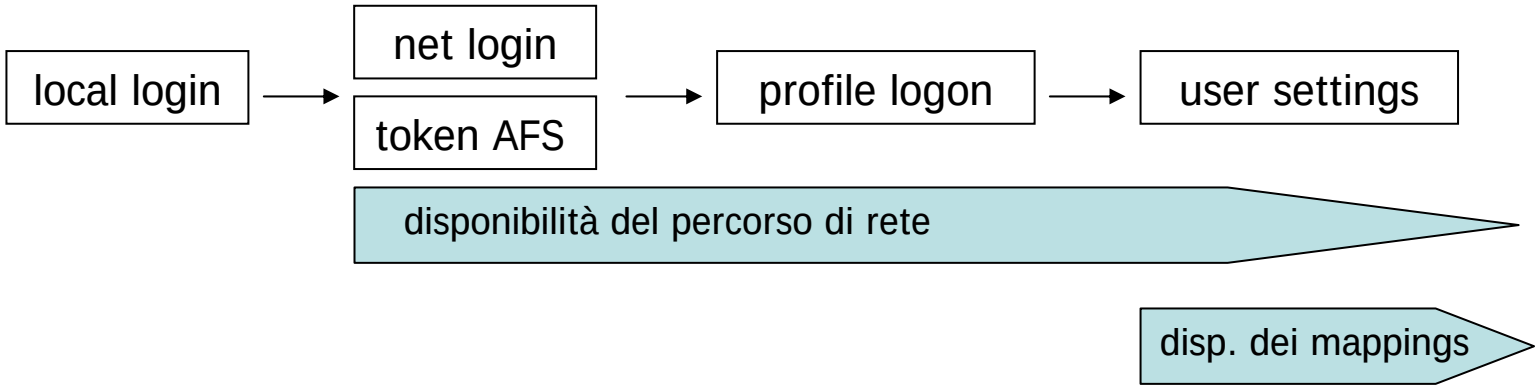


Accesso al profilo mediante URL di rete

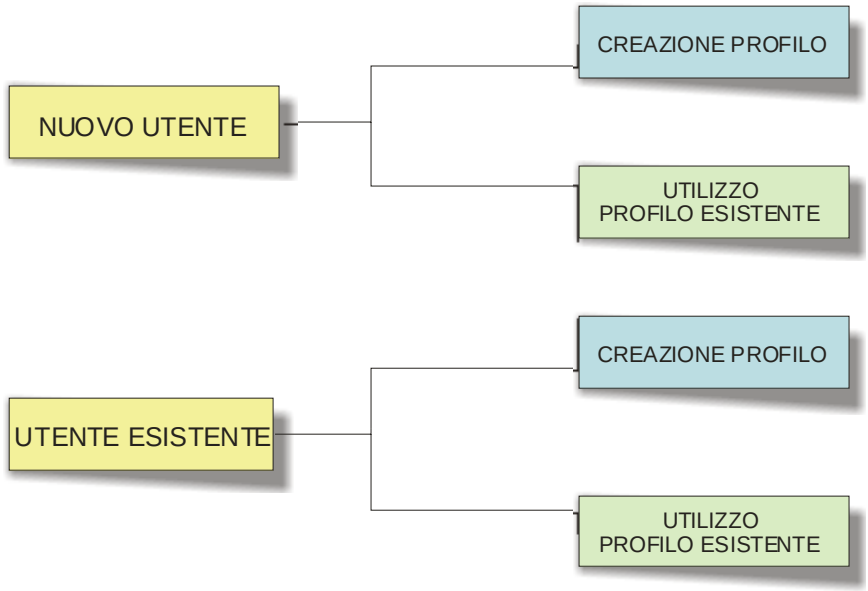


Accesso al profilo mediante logical drive

Poiché le informazioni sulla mappatura dei logical drives utente sono contenute nel profilo residente sul server, accedere ad esso mediante unità logica in fase di login potrebbe rappresentare un assurdo...Di fatto, il ripristino delle connessioni di rete avviene nella fase immediatamente successiva a quella di login al client, alla rete, al profilo.



Nell'ambito dell'esportazione di un profilo windows su un server di rete si deve generalmente affrontare il complesso di situazioni rappresentate dal seguente schema:

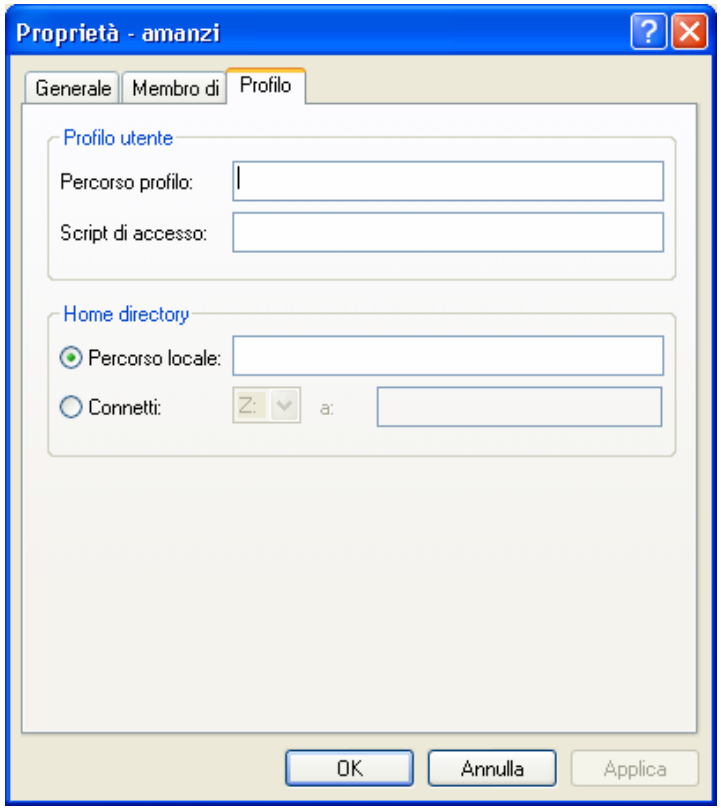


Ogni caso è comunque caratterizzato da:

- la creazione di una directory profilo sul server;
- il trasferimento sul server degli eventuali dati locali per i profili preesistenti;
- il puntamento allo spazio sul server come configurazione utente.

Il nostro interesse si focalizza sui nuovi profili, per i quali è richiesta solo la configurazione di cui al punto 3.

CREAZIONE DI UN NUOVO UTENTE E DEL RELATIVO PROFILO ROAMING



Operando come amministratore del client procedere come segue:

- prendere il token AFS;
- creare il nuovo account utente;
- nelle properties avanzate dell'utente, scheda profilo, digitare il percorso del profilo nella forma:

  \\%computername%-afs\Inf\user\home\%username%\private\pc\Winprofile

  dove <%computername%> e <%username%> sono variabili d'ambiente;
- il percorso locale relativo alla home dir può invece assumere la forma:

  C:\Documents and Settings\%username%

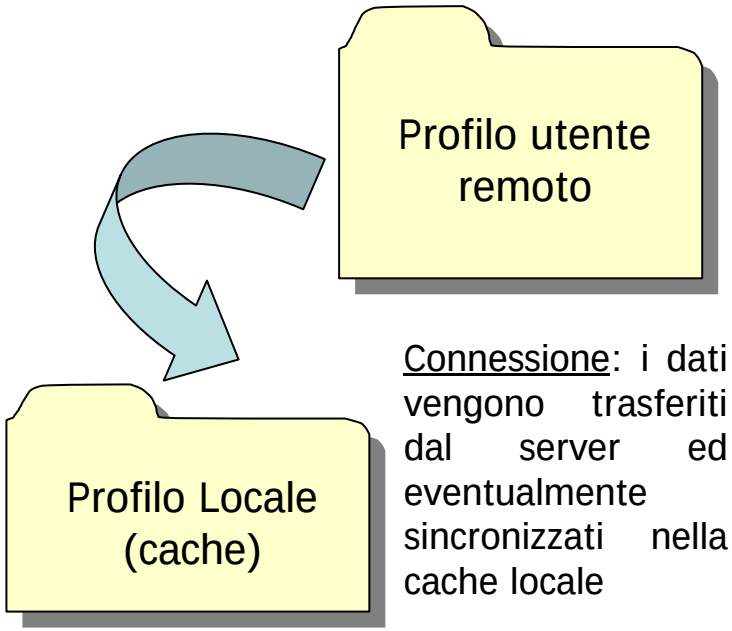
E' importante osservare che:

- Non è necessaria la creazione preventiva della cartella <Winprofile> su AFS
- Il percorso locale può essere omesso per S.O. almeno Windows 2000 Pro

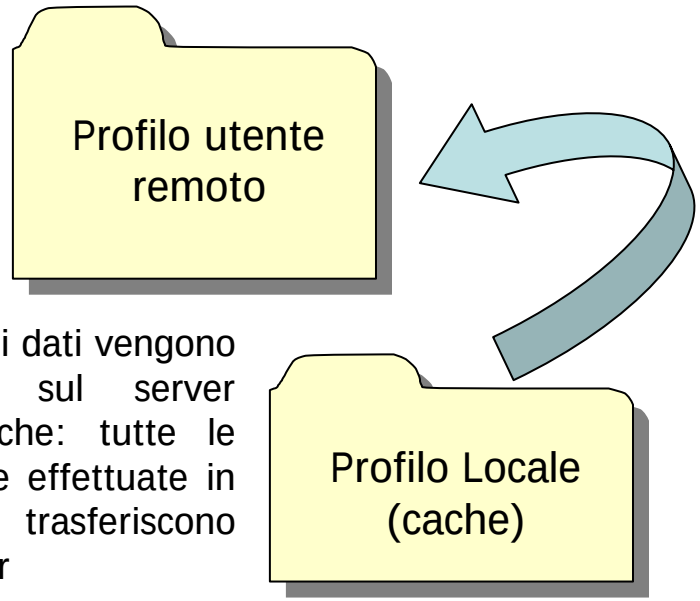
Per rendere operativa la configurazione sarà necessario effettuare in sequenza il login – logoff come nuovo utente.
Infatti il primo login sarà caratterizzato da:

- la creazione del profilo cache locale configurato per il roaming su AFS;
- la creazione della dir <Winprofile> come sottodirectory dello spazio utente su AFS.

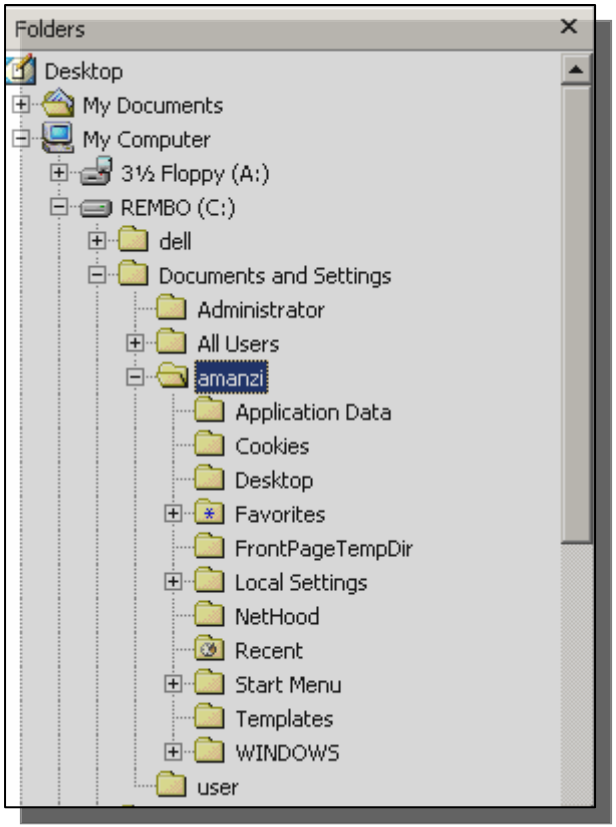
L'effettiva scrittura sul server dei dati di profilo avverrà solo in fase di logout.



Connessione: i dati vengono trasferiti dal server ed eventualmente sincronizzati nella cache locale



Log out: i dati vengono trasferiti sul server dalla cache: tutte le modifiche effettuate in locale si trasferiscono sul server



ASPETTI CONNESSI CON I PROFILI

La possibilità di esportare su un sererver i profili induce le seguenti considerazioni:

• Alcune sottocartelle del profilo sono relative contengono informazioni che dipendono dalla configurazione specifica del client dal quale si esegue l'accesso;

• In particolare i folders Desktop e Start Menu contengono puntatori (Shortcuts) a file (eseguibili o no) locali al client: la sincronizzazione in roaming di detti folders da più di un client potrebbe rendere questi puntatori indefiniti;

• La fase di sincronizzazione coinvolge anche i file temporanei, creando inutile traffico in rete e rischiando l'overflow di quota utente sul server;

• Come già accennato, alcuni dati di configurazione utente, non solo locali al profilo, ma definiti nel *Registro di Configurazione;*

Occorre dunque estendere la configurazione ad un contesto più ampio di quello del *Roaming Profile*, definendo un modello astratto di impostazioni utente e pc risolutivo degli aspetti sopra elencati. Questo modello sarà rappresentato dai *Criteri di Gruppo* in un ambito client-server.

WINDOWS TERMINAL SERVICES

DEFINIZIONE DEL SERVIZIO

Windows Terminal Services è un servizio che permette da un client di rete l'apertura di una sessione windows interattiva su un server.

Esso costituisce quindi un ambiente multisessione che offre a computer remoti la possibilità di accedere a programmi windows-based eseguiti sul server.

L'accesso da remoto è esplicato tramite un software client, ovvero un terminale che emula in remoto un desktop windows, ovvero un'interfaccia utente. L'I/O tra l'applicazione sul server e il terminale remoto si esplica mediante lo specifico protocollo *RDP* che agisce sul server a livello di Video Device Driver esportando a basso livello procedure di implementazione delle *API GDI*.

Il Management delle sessioni sul server si esplica attraverso uno stack di record di attivazione. Un record di attivazione contiene puntatori a:

- I task locali alla sessione;
- Il Contesto utente, ovvero l'account, il profilo e relative chiavi di registro;
- Le policies utente relative al servizio RDP;
- L'indirizzo IP, il netbios-name del client e i parametri di connessione del terminale.

PREMESSE ALLA CONFIGURAZIONE ED USO DEL SERVIZIO

Controllo remoto del server

Il primo record del predetto stack è relativo alla sessione di login locale al server, detta Console. Solo attraverso la Console si ha interazione completa con il server in ambito amministrativo.

Infatti, poiché la Console non è esportabile mediante RDP (gli I/O si esplicano sul device video fisico del server), l'eventuale feedback di alcuni servizi potrebbe non essere visibile tramite connessione in Terminal Services.

E' quindi opportuno stabilire una differente connessione **CAS** da remoto per accedere alla Console.

Ai LNF – INFN si è sperimentato con successo l'utilizzo del *Remote Desktop Sharing* di Netmeeting quale servizio di controllo remoto della Console.

Chiusura di sessione

Una sessione generalmente può essere chiusa per *logoff* o per *disconnessione.* Una disconnessione, diversamente dal logoff, termina la comunicazione client-server, ma non termina la sessione sul server. Poiché la chiusura del client TS per default disconnette la sessione, è opportuno configurare il servizio per evitare inutili impegni di CPU.

Disciplina degli accessi

E' opportuno che ciascun utente acceda in TS con il proprio account, evitando l'utilizzo comune e contemporaneo dell'account *administrator*. In questo modo infatti:

- è possibile disciplinare e monitorare gli accessi, in un ambiente di rete, *ad personam;*
- non vi è rischio di conflitti di configurazione derivanti da sessioni contemporanee di uno stesso account da postazioni differenti;
- la gestione dello stack è più efficiente, sia per il sistema che per gli amministratori;
- si riduce il rischio di *rovinare* l'account *administrator* ed il relativo profilo;
- si riduce in ambito amministrativo l'impegno delle risorse a carico dei singoli tasks.

Per quanto sopra detto è inoltre opportuno utilizzare l'account administrator solo per la Console interagendo con essa in CAS.

CONFIGURAZIONE DEL SERVER RDP

Il Server RDP è costituito da una piattaforma Windows 2000 Advanced Server.
Si accede alla configurazione tramite gli *Administrative Tools/Terminal Services Configuration.*
Nella sezione *Connections* accedere alle properties della connessione RDP, attraverso le quali procedere come segue.

Scheda Logon Settings

Settare le opzioni *Use client-provided logon information* e *Always prompt for password*.

Scheda Session

Settare *Override user settings/End a disconnected session* a 30 minuti.
Settare *Active session limit* a 1 giorno e *Idle session limit* a 1 ora.
Settare *Override user settings/Disconnected from session*, per il timeout di sessione.
In tal senso ogni sessione potrà essere attiva al massimo per un giorno e inattiva (idle) per 1 ora. Quando sopraggiugono tali limiti o la comunicazione client-server è interrotta la sessione sarà disconnessa. In ogni caso una sessione disconnessa può essere rinnovata mediante ulteriore connessione entro e non oltre 30 minuti senza perdita di dati o tasks.

Scheda Environment

Flag *Override settings from user profile...* non impostato.
Flag *Disable wallpaper* settato.

Scheda Remote Control

Use remote control with default user settings impostato.

Il controllo remoto su Terminal Services consiste nel controllo di una sessione RDP da un client diverso da quello di login. Impostando tale opzione si possono controllare solo le sessioni associate ad accounts che permettono il controllo da remoto.

Scheda Client Settings

Use connection settings from user settings impostato.

COM mapping impostato.

Tutti gli altri flag non impostati.

Scheda Network Adapter

Impostare il numero massimo delle connessioni al valore delle licenza disponibili per il TS.

Scheda Permission

In Active Dyrectory sono stati definiti due gruppi di utenti autorizzati all'uso del Terminal Services oltre al gruppo degli Administrators: W2kRDPUsers e W2kRDPPowerUsers.

La differenza sostanziale nelle autorizzazioni consiste nella possibilità del controllo remoto delle sessioni RDP.

In tal senso si sono raggiunti i seguenti obiettivi:

• solo un sottoinsieme degli utenti di dominio può utilizzare TS.

• un sottoinsieme degli utenti TS può controllare le sessioni per non avendo altri diritti amministrativi.

L'appartenenza di un utente ai precedenti due gruppi deve essere mutuamente esclusiva.

In tal senso nella scheda permessi andranno definiti solo i tre gruppi:
Administrators, W2kRDPPowerUsers, W2kRDPUsers
Nella tabella seguente sono elencate in dettaglio le autorizzazioni per i tre gruppi

Tipo Autorizzazione	Administartors		W2kRDPUsers		W2kRDPPowerUsers	
	Allow	Deny	Allow	Deny	Allow	Deny
Query information	X		X		X	
Set Information	X					
Reset	X			X	X	
Remote Control	X			X	X	
Logon	X		X		X	
Logoff	X		X		X	
Message	X		X		X	
Connect	X		X		X	
Disconnect	X		X		X	
Virtual Channel	X					

Le impostazioni della sezione *Server Settings* sono invece le seguenti:

Terminal server mode	Application Server
Delete temporary folders on exit	Yes
Use temporary folders per session	Yes
Internet connector licensing	Disable
Active desktop	Enable – L'effettiva policy viene impostata nei criteri di gruppo
Permission compatibility	Windows 2000 users

ACTIVE DIRECTORY
CRITERI DI SICUREZZA

PREMESSA

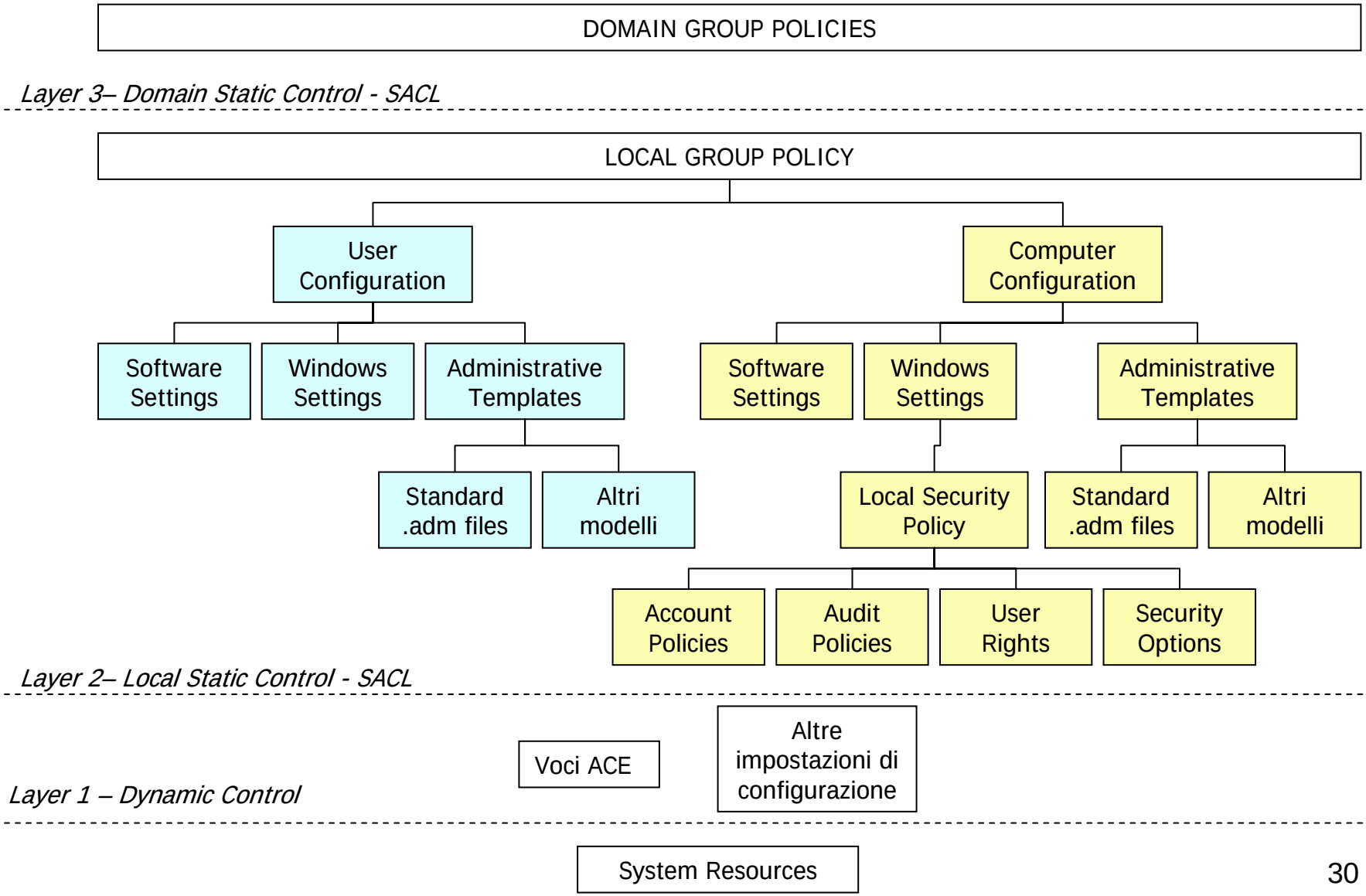
Active Directory è un database nel quale sono definiti e distribuiti, tra l'altro, computer e utenti le cui policies hanno validità in ambito di dominio.

Active Directory definisce quindi di fatto un environment distribuito, il Dominio Windows, ovvero un *campo di azione* nel senso che indipendentemente da dove si effettua il login al dominio, risultano sempre definiti gli stessi oggetti:

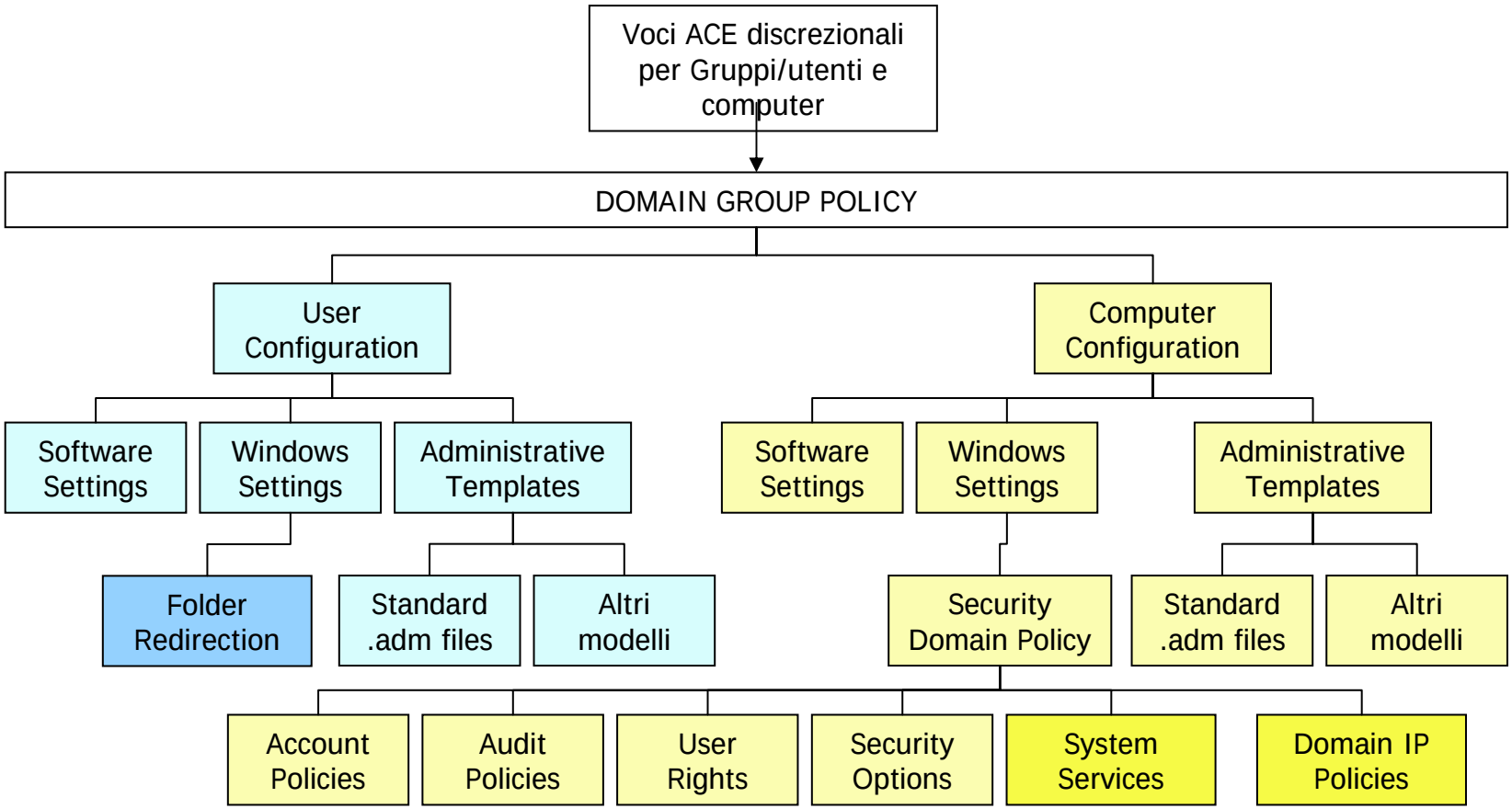
- Accounts computers
- Accounts utenti
- Policies utente e Criteri di Gruppo

Il concetto di ambiente e di campo di azione risulta più chiaro nell'ambito dell'esame dei criteri di protezione di Windows 2000

CRITERI DI GESTIONE E SICUREZZA GLOBALE - SCHEMA



CRITERI DI GESTIONE E SICUREZZA NEL DOMINIO
SCHEMA



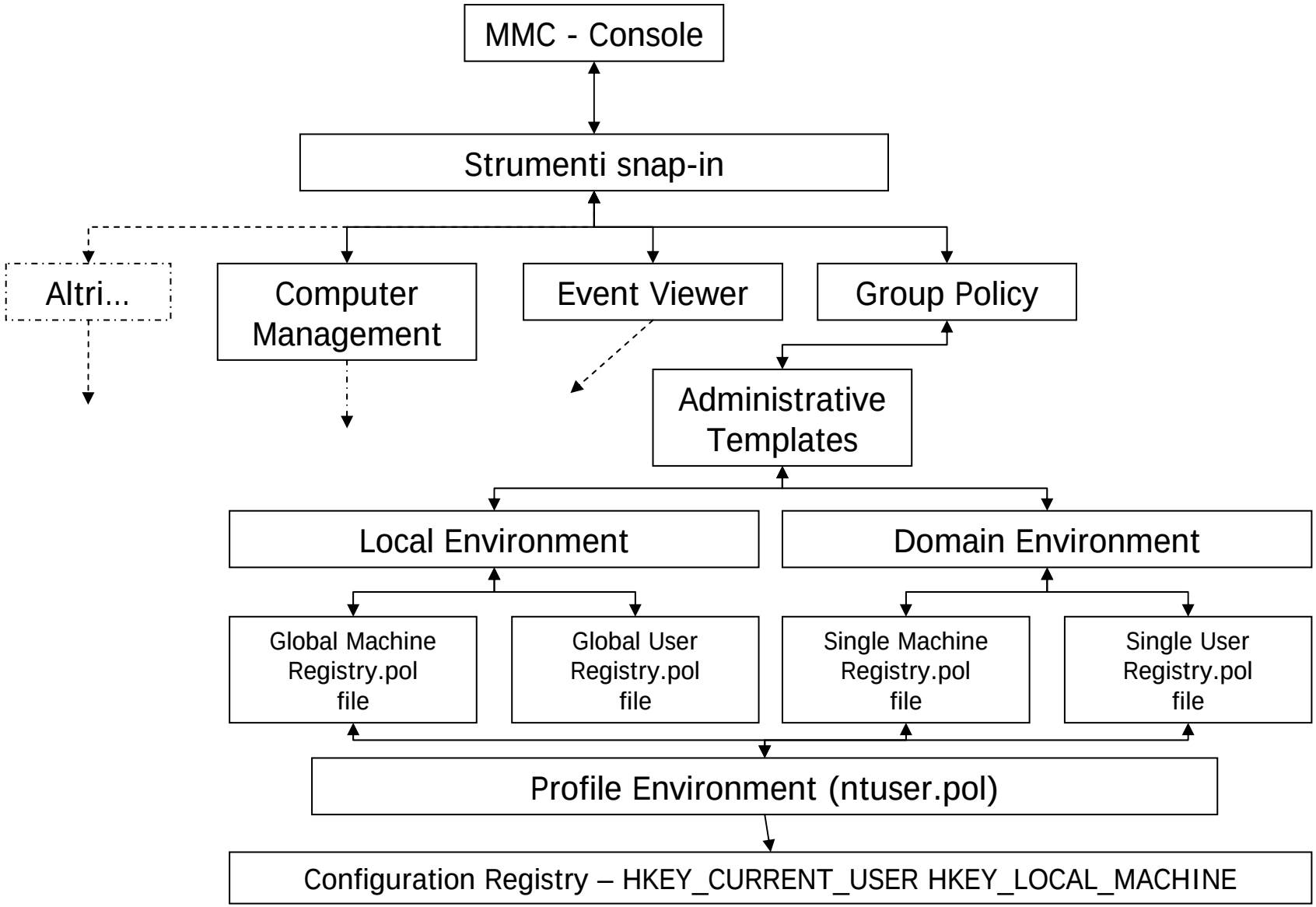
CRITERI DI GRUPPO

Globalmente e ad alto livello una piattaforma windows viene amministrata attraverso una speciale interfaccia denominata **Microsoft Management Console**.

Questa Console, attivabile in Start/Run con il comando *mmc,* esporta file di configurazione, di tipo .msc, residenti in %systemroot%\system32, che sono dei strumenti di gestione e di interfaccia con la configurazione di sistema denominati *snap-in*.

Criteri di gruppo è un sistema di management di componenti windows e risorse.
Lo snap-in Criteri di Gruppo (gpedit.msc) permette in particolare:

- Gestire i criteri basati sul Registro di sistema con Modelli amministrativi
  Infatti esso crea files di impostazioni che interessano e sovrascrivono le sezioni del *Registro di Configurazione* **HKEY_CURRENT_USER** e **HKEY_LOCAL_MACHINE**
- Assegnare scripts
- Reindirizzare cartelle (criteri di gruppo di dominio)
- Gestire applicazioni
- Specificare opzioni di protezione


MMC - Console
Strumenti snap-in
Altri...
Computer Management
Event Viewer
Group Policy
Administrative Templates
Local Environment
Domain Environment
Global Machine Registry.pol file
Global User Registry.pol file
Single Machine Registry.pol file
Single User Registry.pol file
Profile Environment (ntuser.pol)
Configuration Registry – HKEY_CURRENT_USER HKEY_LOCAL_MACHINE

Criteri di Gruppo si applica a membri di siti, unità organizzative, oggetti locali.

Le policies di *Criteri di Gruppo* definite a layer superiore determinano l'applicabilità e la risultante di quelle a livello inferiore, poiché esse:

• possono essere combinate con quelle a layer inferiore per determinare un criterio risultante;

• possono sostituire quelle a layer inferiore per determinare il criterio risultante;

• possono essere sostituite da quelle a layer inferiore per determinare il criterio risultante;

• possono rendere inapplicabili i criteri e metodi definiti a layer inferiore;

• in ambito non locale possono essere definiti filtri di applicabilità dei criteri per PC e utenti.

Le regole per la definizione di un criterio risultante tra 2 layer adiacenti possono essere definite a layer più basso o a quello più alto.

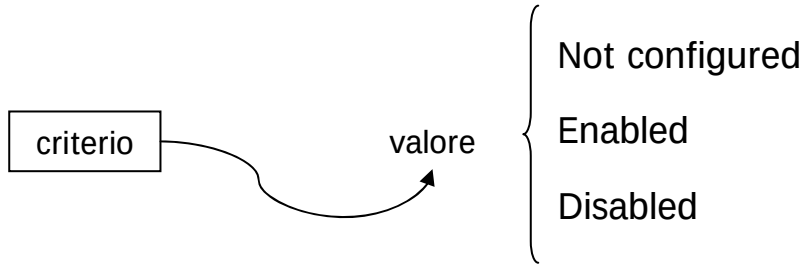
E' sconsigliabile però agire in ambito locale, ma definire il comportamento nei criteri di dominio poiché:

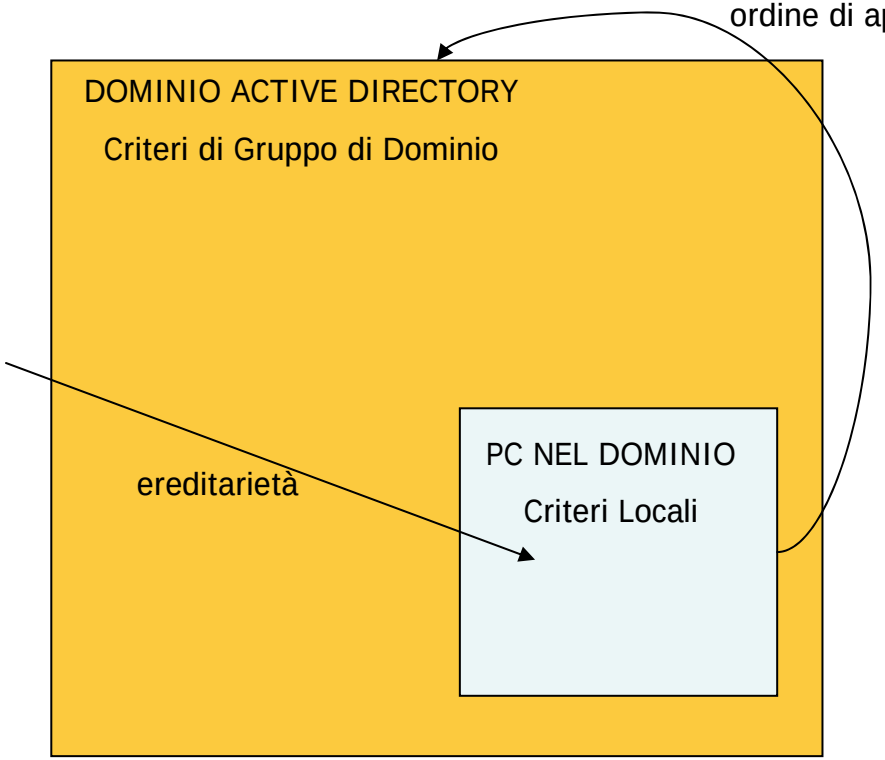
•si impone un comportamento a livello di dominio standard per tutti gli oggetti;

•si riduce la configurazione locale di ogni client.

EREDITARIETA' E PRIORITA' DEI CRITERI DI GRUPPO NEL DOMINIO

Criteri di gruppo è un elenco di criteri organizzati in categorie. La maggior parte di essi, di default non cofigurati, può assumere, se definito, due valori opposti.





Vengono prima applicati i criteri definiti in locale.
Successivamente vengono nell'ordine applicati i criteri definiti, dall'environment più esterno a quello più interno.

Per default:

- Un criterio definito nel dominio, viene ereditato in locale, se qui esso non è definito;
- In caso di doppia definizione e conflitto di valori, viene considerato valido il valore locale.

MECCANICA DEI CRITERI DI GRUPPO NEL DOMINIO

DEFINIZIONE DOMINIO	DEFINIZIONE LOCALE	RISULTANTE DEFAULT		NO OVERRIDE (FLAG DOMINIO)	SOTITUZIONE (FLAG LOCALE)	UNIONE (FLAG LOCALE)
Null	Null	Null	-	Null	Null	Null
Null	En./Dis.	En./Dis.	Nessuna sovrascrittura	En./Dis.	Null	En./Dis.
Enabled	Disabled	Disabled	Conflitto Definizione dominio sovrascritta	Enabled	Enabled	Enabled
Disabled	Enabled	Enabled	Conflitto Definizione dominio sovrascritta	Disabled	Disabled	Disabled
En./Dis.	Null	En./Dis.	Ereditarietà	En./Dis.	En./Dis.	En./Dis.
En./Dis.	En./Dis.	En./Dis.	Nessuna sovrascrittura	En./Dis.	En./Dis.	En./Dis.

Le varianti *sostituzione* e *unione* sono definite localmente e impongono, in caso di conflitto, che il sia valido il valore attribuito per ultimo ovvero quello definito nel dominio.
La variante scelta ai LNF – INFN è stata *no override*, definita nei criteri di gruppo di dominio. In questo modo tutte le policies difinite a layer superiore avranno priorità di applicazione, le policies a layer inferiore non in conflitto saranno ugualmente applicate.

CONFIGURAZIONE CLIENT-SERVER

Ai LNF – INFN è stata implementata un'opportuna configurazione dei *Criteri di Gruppo* basata su un modello client-server, con la quale si sono raggiunti gli obiettivi seguenti:

• Gli utenti che da client si autenticano sul dominio importano un environment windows con profilo windows in roaming con AFS

• Un sottoinsieme degli utenti di dominio può aprire una sessione di login sul server tramite Terminal Services

• Alcuni utenti Terminal Services, oltre agli amministratori, possono assumere da remoto il controllo delle sessioni di login

• Tutti gli utenti che aprono una sessione sul server (in locale o in remoto tramite TS) importano un windows environment in roaming con AFS

• Tutti gli utenti che aprono una sessione sul server (in locale o in remoto tramite TS) sono soggetti a elevati criteri di sicurezza nell'accesso alle risorse e alle applicazioni del server, mediante la definizione di policies di gruppo, locali al server e globali nel dominio

• Gli amministratori che aprono una sessione sul server non sono sottoposti ai detti criteri

• L'account *administrator* ha un profilo locale e non ha accesso ad AFS

• Da profili roaming vengono esclusi particolari folders locali i cui contenuti cambiano in base alle configurazione dei client di accesso

• Il folder *My Documents* è escluso dal caching, ma è direttamente puntato su AFS

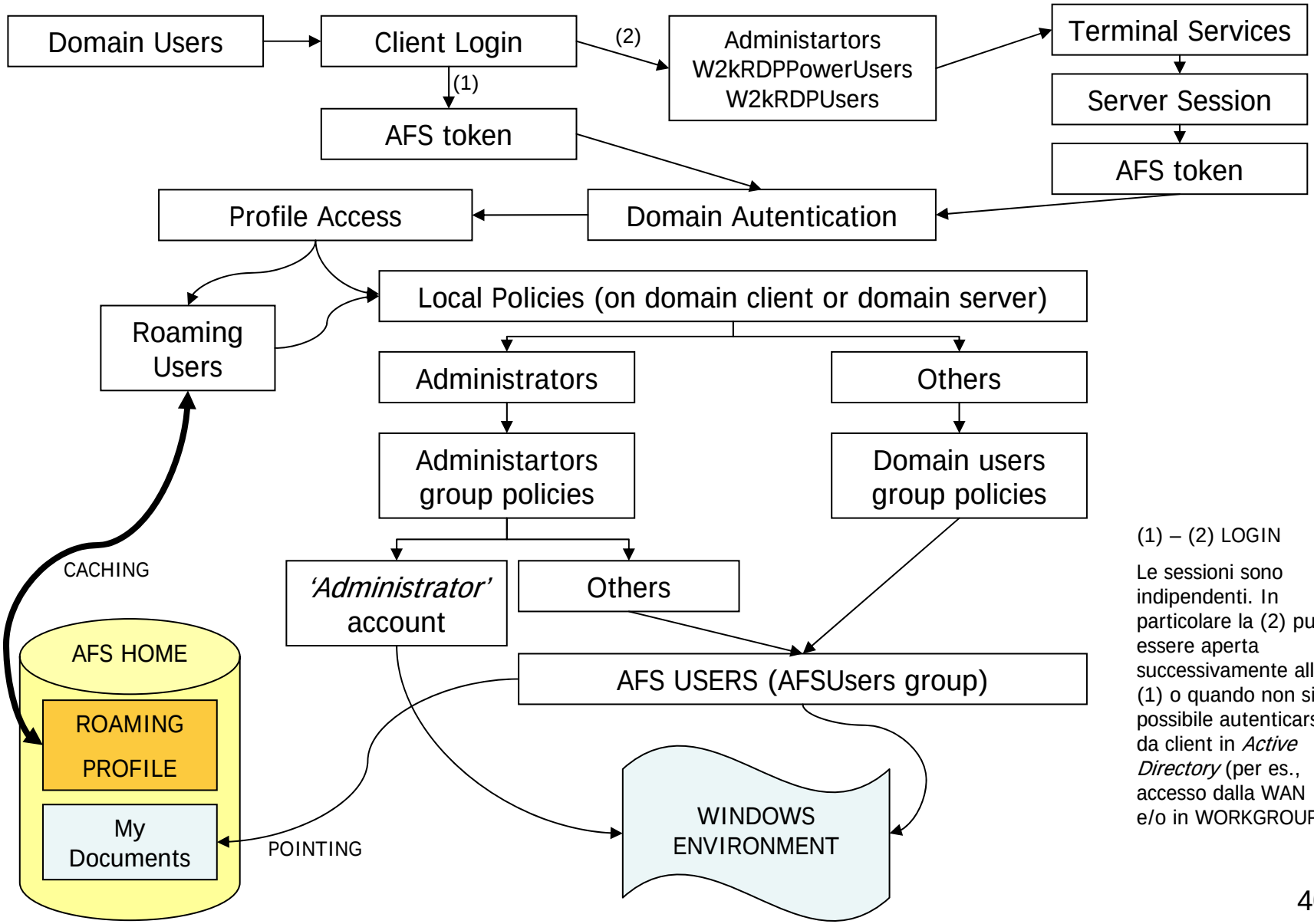
• Ogni profilo roaming è quotato a livello di dominio; il folder My Documents non è sottoposto a predetta quotazione, ma solo a quella utente imposta per AFS

I presupposti di base questa configurazione sono caratterizzati da:

- S.O. almeno Windows 2000 pro per tutti i clients
- Unica lingua (inglese) del S.O.per i clients
- Nome pc non superiore a 11 caratteri
- Stessa configurazione per il client AFS, nessuna mappatura statica di unità logiche, unica definizione del file afsdsbmt.ini nella forma:

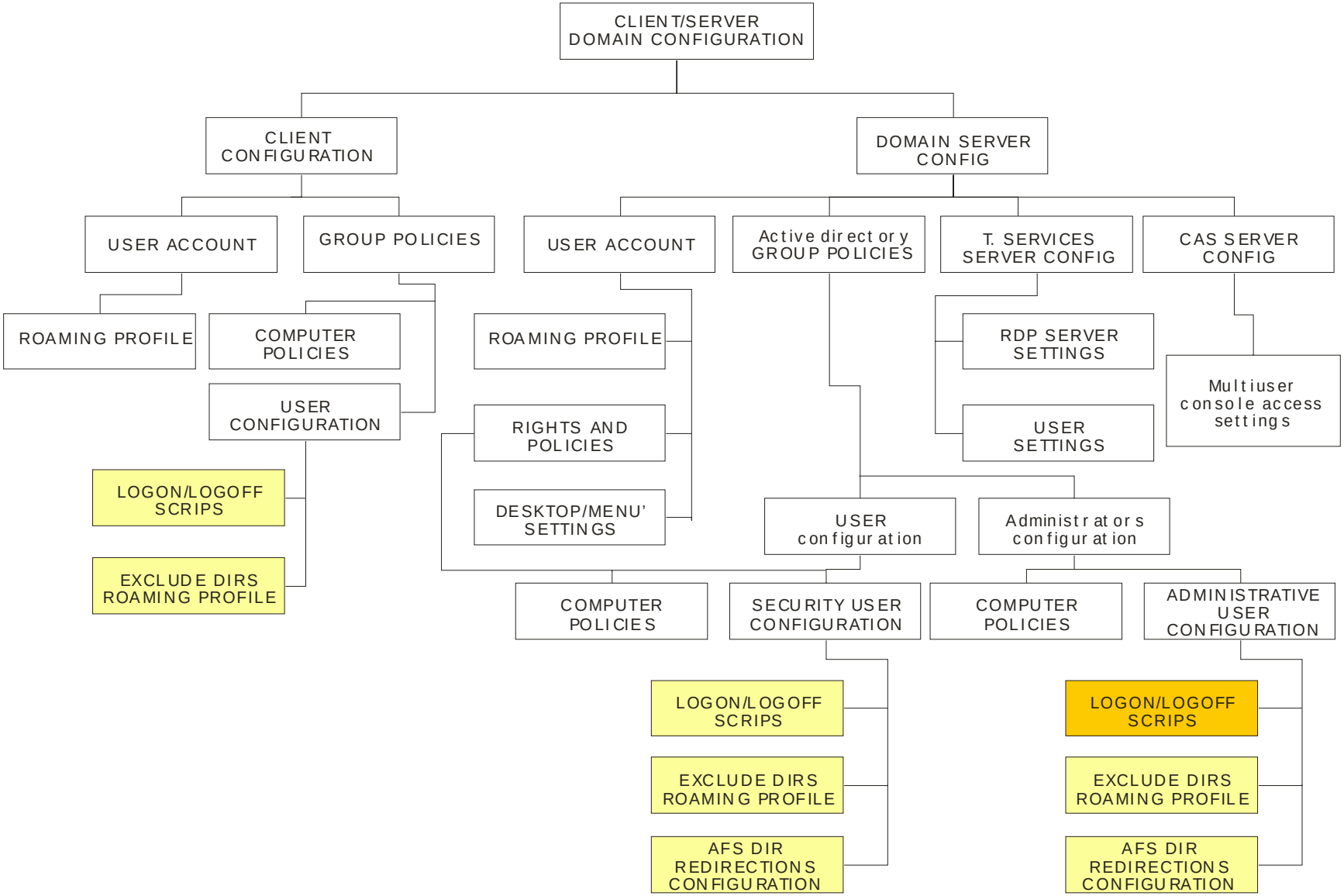
```
afs=/
lnf=/lnf.infn.it
```

ACCESSO CENTRALIZZATO AL WINDOWS ENVIRONMENT



(1) – (2) LOGIN

Le sessioni sono indipendenti. In particolare la (2) può essere aperta successivamente alla (1) o quando non sia possibile autenticarsi da client in *Active Directory* (per es., accesso dalla WAN e/o in WORKGROUP)


CLIENT/SERVER DOMAIN CONFIGURATION
CLIENT CONFIGURATION
DOMAIN SERVER CONFIG
USER ACCOUNT
GROUP POLICIES
USER ACCOUNT
Active directory GROUP POLICIES
T. SERVICES SERVER CONFIG
CAS SERVER CONFIG
ROAMING PROFILE
COMPUTER POLICIES
USER CONFIGURATION
LOGON/LOGOFF SCRIPS
EXCLUDE DIRS ROAMING PROFILE
ROAMING PROFILE
RIGHTS AND POLICIES
DESKTOP/MENU' SETTINGS
RDP SERVER SETTINGS
USER SETTINGS
Multiuser console access settings
USER configuration
Administrators configuration
COMPUTER POLICIES
SECURITY USER CONFIGURATION
COMPUTER POLICIES
ADMINISTRATIVE USER CONFIGURATION
LOGON/LOGOFF SCRIPS
EXCLUDE DIRS ROAMING PROFILE
AFS DIR REDIRECTIONS CONFIGURATION
LOGON/LOGOFF SCRIPS
EXCLUDE DIRS ROAMING PROFILE
AFS DIR REDIRECTIONS CONFIGURATION

CONFIGURAZIONE CLIENT – SERVER

CLIENT

La configurazione è rilevante per le sessioni di login nella WAN e in tutti i casi nei quali non sia possibile l'autenticazione a livello di dominio.

- Creare un account utente locale ed impostare il percorso del profilo di roaming nella forma:

  \\%computername-afs\Inf\user\home\%username%\private\pc\Winprofile

  Come già visto nella sezione dei profili. Non creare preventivamente su AFS la cartella Winprofile.

- Impostare le policies locali di criteri di gruppo: Start/Run mmc.exe, quindi aprire il file gpedit.msc in %systemroot%\system32. Le chiavi da configurare sono descritte in analisi negli allegati a queste slides e riguardano in particolare:

  - I folders di profilo eslusi dal caching con AFS
  - La quotazione del profilo
  - Gli spripts di login

- Creare nella system root (generalmente C:\WINNT o C:\WINDOWS) i file net_login.bat, net_login.bat.lnk (shortcut) e local_login.bat in base a quanto descritto nella sezione degli scripts.

SERVER – CONFIGURAZIONI PRELIMINARI

E' opportuno procedere in base alle seguenti fasi preliminari:

- In *Active Directory Users and Conputers* definire i seguenti gruppi di protezione:

  - AFSUsers: utilizzato per reindirizzare il folder My Documents su AFS;
  - W2kRDPUsers: per gli utenti che accedono al server via TS
  - W2kRDPPowerUsers: per gli utenti TS autorizzati al controllo delle sessioni

- Configurare il servizio Terminal Services in base a quanto detto nell'opportuna sezione di queste slides
- Disciplinare eventualmente l'acesso ai folder e alle risorse locali, a basso livello, mediante il setting opportuno delle voci ACE;
- Riconfiguare il Desktop e lo Start Menu per il profilo locale Administrator e All User in modo da limitare l'accesso di alcune applicazioni solo all'amministratore.

SERVER – CONFIGURAZIONE ACCOUNTS

In *Active Directory Users and Conputers* creare gli account utente come segue:

•Attribuire il percorso del profilo di roaming nella forma (escluso l'account *Administrator*):

\\%computername-afs\Inf\user\home\%username%\private\pc\Winprofile

•Il profilo relativo alle connessioni in TS non dovrà essere impostato;

•Abilitare il Remote Control per controllare le sessioni associate all'account;

•L'appartenenza ai gruppi di protezione è così definita:

Default Standard User	Terminal S. User	Terminal S. User with Session Control	Administrators (*)	Administrator account (*)
Domain Users AFSUsers	Domain Users AFSUsers W2kRPDUsers	Domain Users AFSUsers W2kRDPPowerUsers	Domain Users AFSUsers Administrators Domain Admins Enterprice Admins Group Policy Creator Schema Admins	Domain Users Administrators Domain Admins Enterpice Admins Group Policy Creator Schema Admins

(*) L'utente '*administrator*' non ha accesso ad AFS, non beneficia di roaming e puntamento e quindi non appartiene al gruppo *AFSUsers*

SERVER – CONFIGURAZIONE CRITERI DI GRUPPO

Per la configurazione del server è stata prestata particolare attenzione alla configurazione dei criteri di gruppo locali per elevare il livello di sicurezza delle sessioni di login in T.S. .

La definizione di policies locali ha imposto l'implementazione di due criteri di gruppo di dominio, uno relativo agli utenti standard, l'altro applicato agli amministratori con lo scopo di eliminare le restrinzioni applicate per i login sul server, in base alle seguenti specifiche:

- Aprire, in Administrative Tools, la Console di Active Directory Users and Computers
- Selezionare le properties del dominio e quindi la scheda *Group Policy*;
- Disabilitare il flag Block Policy inheritance;
- Creare i due file di policy Default Domain Policy e Administrators Domain Policy (*New*);
- Per entrambi settare il flag *no override* (pulsate *Options*);
- Il file relativo agli amministratori dovrà essere il primo in lista (priorità più alta);
- Impostare per i file le voci ACE per l'accesso e l'esecuzione (pulsante *Properties*)

DEFAUL GROUP POLICY	Administartors	Autenticated Users	CREATOR OWNER	Domain Admins	Enterprice Admins	SYSTEM
Full Control	-	-	-	-	-	-
Read	Allow	Allow	-	Allow	Allow	Allow
Write	Allow		-	Allow	Allow	Allow
Create all Child Objects	Allow		-	Allow	Allow	Allow
Delete all Child Objects	Allow		-	Allow	Allow	Allow
Apply Group Policy	Deny	Allow	-	-	-	-

ADMINISTRATORS GROUP POLICY	Administartors	Autenticated Users	CREATOR OWNER	Domain Admins	Enterprice Admins	SYSTEM
Full Control	Allow	-	-	-	-	-
Read	Allow	Allow	-	Allow	Allow	Allow
Write	Allow	-	-	Allow	Allow	Allow
Create all Child Objects	Allow	-	-	Allow	Allow	Allow
Delete all Child Objects	Allow	-	-	Allow	Allow	Allow
Apply Group Policy	Allow	-	-	-	-	-

Mediante la combinazione Domain e Local Group Policy è stato in particolare possibile:

- Monitorare gli eventi di login sul server
- Imporre i programmi di default per il client di posta elettronica e il browser internet;
- Definire la home page dei laboratori;
- Limitare l'utilizzo di netmeeting sul dominio in termini di CAS e risorse audio/video;
- Limitare sul sever l'accesso alla configurazione di Internet Explorer;
- Limitare sul server l'accesso alla configurazione delle connessioni di rete;
- Limitare sul server l'accesso alle risorse locali;
- Limitare sul server la personalizzazione del Desktop e della Start Menu;
- Proibire sul server l'accesso al Control Panel;
- Proibire sul server l'installazione di software e l'utilizzo di alcuni devices;
- Proibire sul server la gestione delle modalità del display;
- Proibire sul server la creazione di connessioni RAS Dial-up e la visualizzazione delle properties per le altre connessioni di rete;
- Limitare sul server l'utilizo del Task Maneger;
- Quotare il profilo roaming;
- Escludere dal caching di roaming le cartelle temporanee, il Desktop, lo Start Menu e My Documents.

In particolare per il folder *My Documents* è stato definito il puntamento ad un folder corrispondente su AFS mediante impostazione di un persorso di ridirezione nella forma:

\\%computername%-afs\Inf\user\home\%username%\private\pc\Windocs

Da notare che la directory dei documenti su AFS è esterna al profilo: ciò è obbligatorio se si vuole evitare la cancellazione della stessa dal momento che il sub-folder *My Document* è escluso dal processo di roaming.

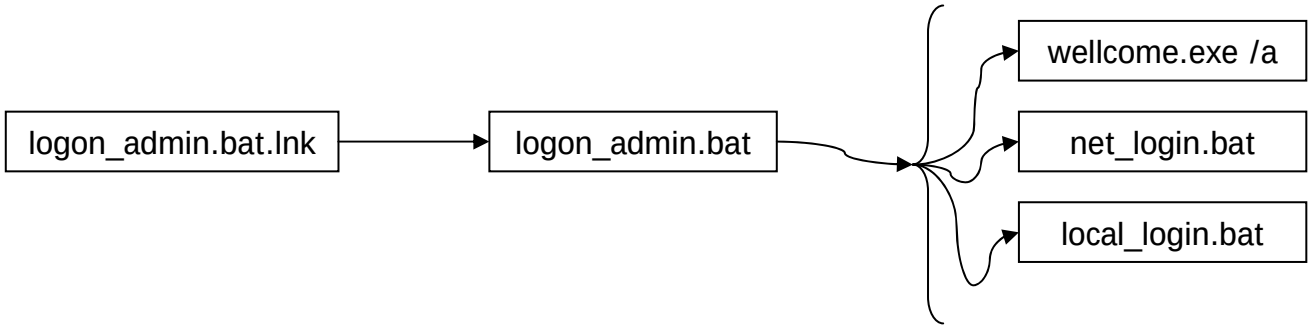
E' anche da sottolineare che la predetta cartella non deve essere creata preventivamente.

La configurazione completa delle policies di gruppo è riportata negli allegati alle slides.

MECCANICA DEGLI SCRIPTS

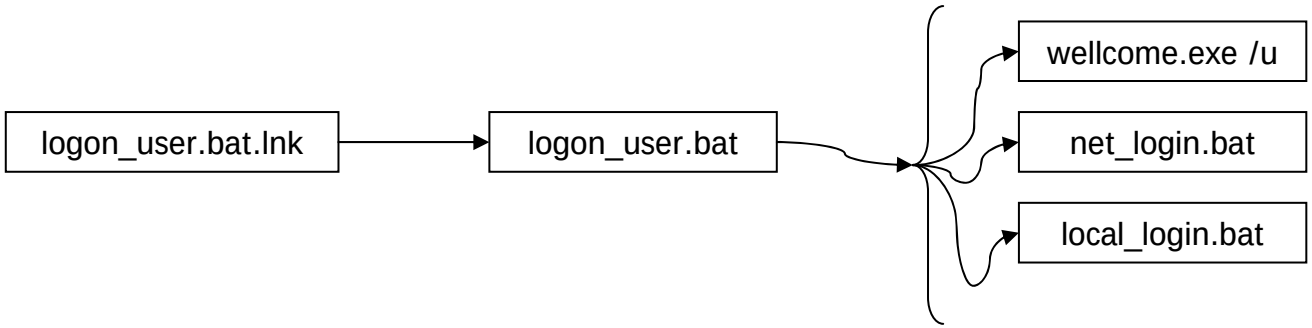
Gli scripts principali sono definiti a livello di dominio, memorizzati in un folder del server ed eseguiti sul client in fase di login.

Gli scripts di dominio hanno una struttura modulare poiché contengono chiamate ad altri scripts indipendenti per ogni client e personalizzabili dall'utente.



Schema di esecuzione degli scripts, in fase di login al dominio da client, localmente al server o in remoto via TS per gli amministratori.

Definito in *Administrators Domain Policy*.



Schema di esecuzione degli scripts, in fase di login al dominio da client, localmente al server o in remoto via TS per gli utenti di dominio.

Definito in *Default Domain Policy*.

SCRIPTS MEMORIZZATI SUL SERVER

Creare un nel system drive il percorso usr\logon_off con i permessi di lettura ed esecuzione concessi a tutti gli utenti autenticati;

Creare nel suo interno il file *logon_admin.bat*, *logon_user.bat*, *net_login.bat* il cui contenuto è rispettivamente il seguente:

Logon_admin.bat

```
\\w2ksrv\usr\logon_off\wellcome.exe /a
Call \\w2ksrv\usr\logon_off\net_login.bat
Call %systemroot%\local_login.bat
```

Logon_user.bat

```
\\w2ksrv\usr\logon_off\wellcome.exe /u
Call \\w2ksrv\usr\logon_off\net_login.bat
Call %systemroot%\local_login.bat
```

Net_login.bat

```
net use L: \\%computername%-afs\lnf /persistent:no
net use I: \\%computername%-afs\afs\infn.it /persistent:no
net use W:\\%computername%-afs\afs /persistent:no
net use H: \\%computername%-afs\lnf\user\home\%username% /persistent:no
```

Dove *w2ksrv* è il nome del server e *wellcome.exe* è un eseguibile che visualizza un messaggio di benvenuto che rende noto all'utente l'applicazione delle policies a livello di dominio e il tipo di autorizzazioni concesse (utente o amministratore).

Il file local_login.bat del server, collocato nella sua system root, contiene una chiamata all'eseguibile wellcome_local.exe che visualizza un ulteriore messaggio di benvenuto per i login effettuati sul server indicando i tempi massimi di sessione nel caso di connessione mediante Terminal Services.

Per i file *logon_admin.bat* e *logon_user.bat* si possono definire le rispettive shurtcuts *logon_admin.bat.lnk* e *logon_user.bat.lnk* configurati in modi da edeguire i corrispondenti batch files in una finestra iconizzata per evitare la visualizzazione di una *shell command* durante la loro esecuzione.

SCRIPTS MEMORIZZATI SUI CLIENTS

Nella system root di ogni client creare il file *local_login.bat* con i comandi che si desidera eseguire dopo il login dal dominio.

Analogamente creare i file *net_login.bat* e la sua shortcut *net_login.bat.lnk*. Il file .bat ha la medesima implementazione di quella usata per il server. Esso viene chiamato dalle policies locali quando non sono disponibili quelle di dominio. In questo caso anche per i login generici in WAN risultano mapati gli stessi devices logici.

DEFINIZIONE DEGLI SCRIPTS DI LOGON NEI CRITERI DI GRUPPO

SCHEMA RIASSUNTIVO

Administrators Domain Policies	\\w2ksrv\usr\logon_off\logon_admin.bat.lnk (*)
Default Domain Policy	\\w2ksrv\usr\logon_off\logon_user.bat.lnk (*)
Local Server Gruop Policy	Not configured
Local Client Group Policy	C:\WINNT\net_login.bat.lnk

(*) Sul server di dominio è stata creata un'opportuna cartella *usr* condivisa in rete . I permessi di accesso (voci ACE) devono essere tali da permetterne la lettura e l'attraversamento/esecuzione ai membri del gruppo *Autenticated Users*.

RIASSUNTO CONFIGURAZIONE CLIENT-SERVER

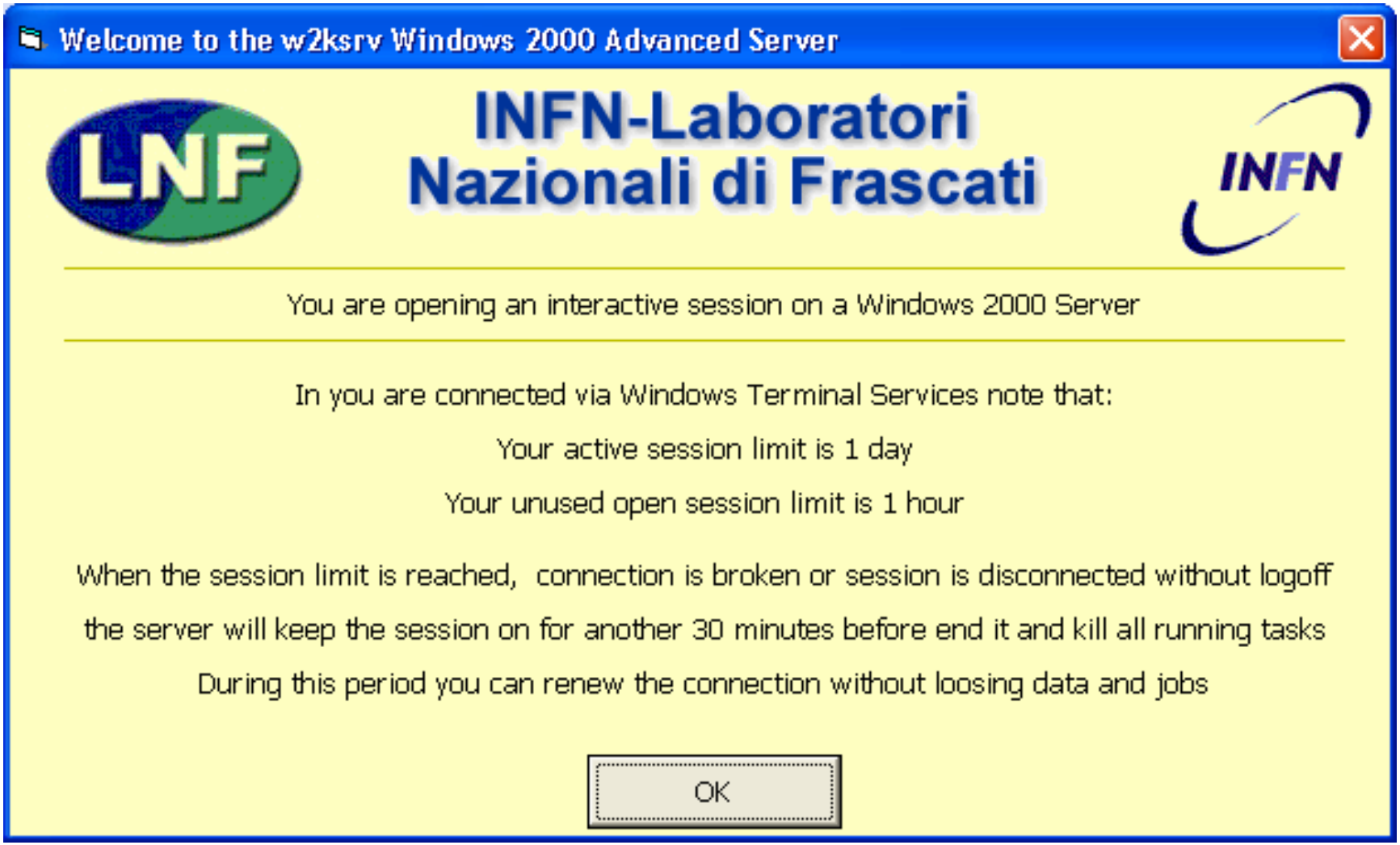
Client Dominio	Creazione account utente locale con stessa nome e password di AFS Impostazione del Profilo Roaming Modifica file afsdsbmt.ini Creazione files net_login.bat, net_login.bat.lnk, local_login.bat in system root Configurazione policies di gruppo locali
Server Dominio	Creazione account utente di dominio con stessa nome e password di AFS Attribuzione dei gruppi di protezione all'utente Impostazione Profili di Roaming Configurazione servizio RDP Modifica file afsdsbmt.ini Creazione in c:\usr\logon_off dei file: • logon_user.bat e logon_user.bat.lnk • logon_admin.bat e logon_admin.bat.lnk • net_login.bat, wellcome.exe e wellcome_local.exe Creazione in system root del file local_login.bat Configurazione Default Domain Policies Configurazione Administrators Domain Policies Configurazione Local Group Policy

Path profilo: \\%computername-afs\Inf\user\home\%username%\private\pc\Winprofile

Path documenti: \\%computername-afs\Inf\user\home\%username%\private\pc\Windocs

DOMAIN LOGIN WELLCOME BOX

DOMAIN SERVER LOGIN WELLCOME BOX



ASPETTI DI CONFIGURAZIONE PER IL CLIENT

Sono stati definiti criteri di gruppo anche per il client con riguardo alla definizione di quelle policies la cui mancata applicazione altererebbe l'assetto del profilo su AFS in caso di login nella wan ovvero senza autenticazione centralizzata in Active Directory.

Queste policies riguardano:

- L'esclusione di alcuni subfolders dal processo di roaming
- La quotazione del profilo di roaming
- Il timeout di connessione al profilo di roaming
- La definizione ed esecuzione degli scrips