INFN Istituto Nazionale di Fisica Nucleare
Laboratori Nazionali di Frascati

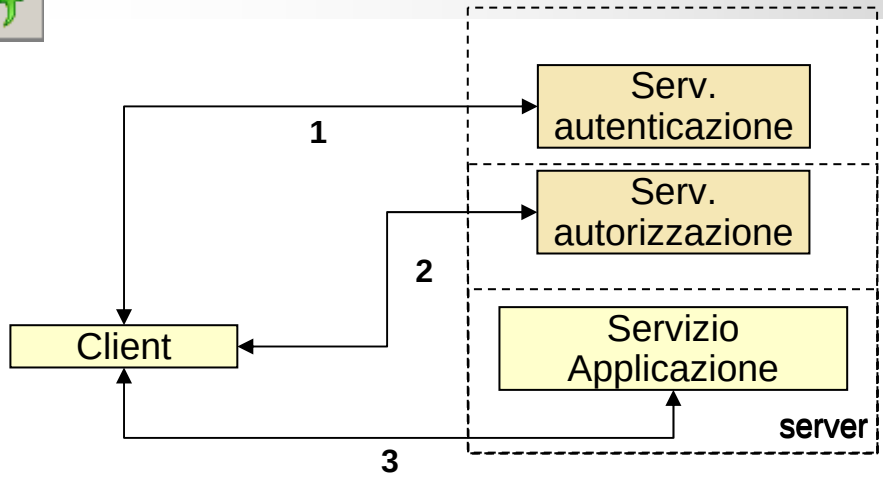
INFN Computing Service

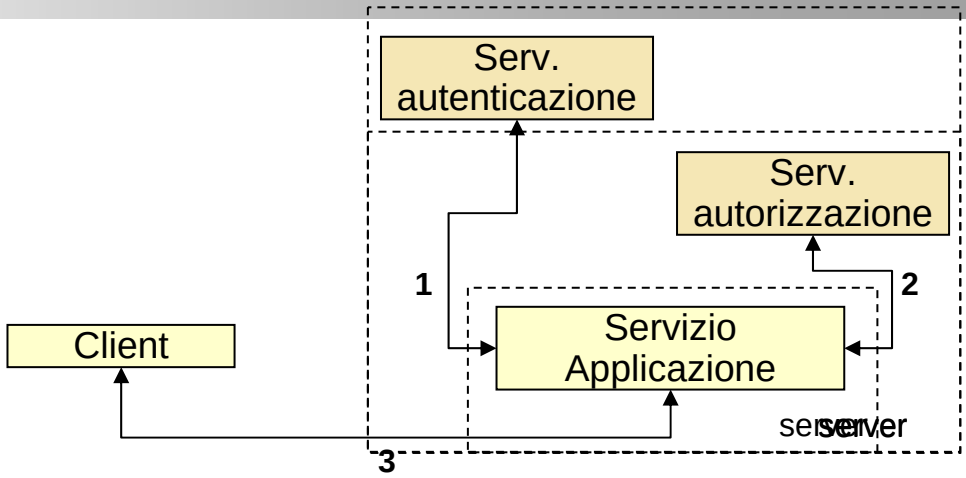
Principi di WinNT Security
Meccaniche di autorizzazione e user profiling per l'accesso alla piattaforma windows

Nunzio AMANZI, LNF – AC - INFN
E-mail: Nunzio.Amanzi@lnf.infn.it
www: http://www.lnf.infn.it/~amanzi
Phone: +39 6 94 03 2446-8225

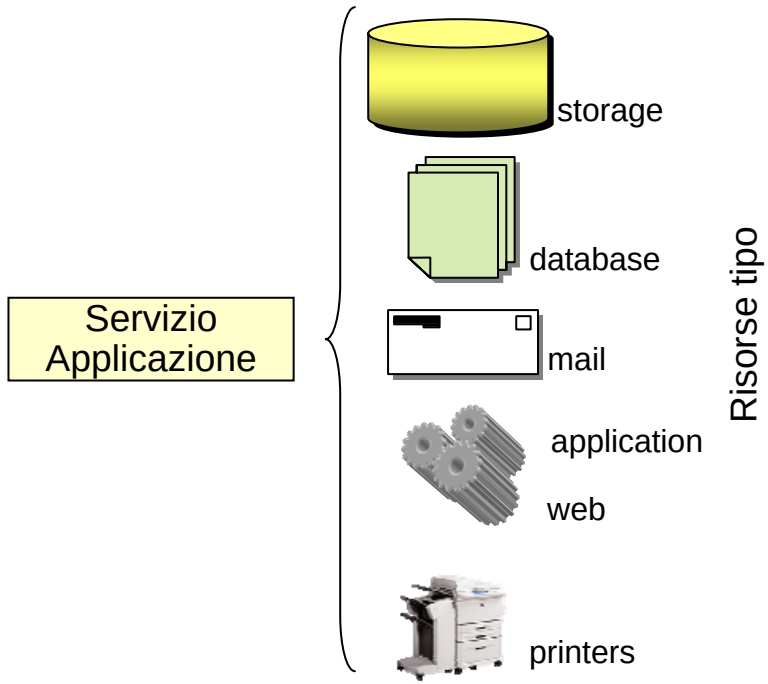
Autenticazione e Autorizzazione

Meccaniche di accesso ai servizi di rete





1. **Autenticazione**: processo di convalida delle credenziali utente (username – password - dominio) presso un *Account DB*
2. **Identificazione-Autorizzazione**: rilascio di un pacchetto cifrato di informazioni che identifica l'utente durante tutta la sessione
3. **Autorizzazione-Accesso**: confronto/convalida delle informazioni contenute nel pacchetto di identificazione, presentato dal client, con le autorizzazioni ammesse per la risorsa richiesta



Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

Autenticazione e Autorizzazione

Livello di autenticazione

E’ generalmente il livello della pila OSI-ISO al quale intervengono i processi di autenticazione per l’accesso ai servizi di rete.
Indica anche il livello e/o il complesso delle risorse dell’host a cui e’ possibile accedere presentando il pacchetto di identificazione emesso a seguito dell’autenticazione.

- Livello 2: per connettere la piattaforma in rete ed ottenere un indirizzo IP
- Livello 3: per accedere agli oggetti serviti dal S.O. (es. file system, stampanti, ecc.)
- Livello 5: per accedere ai servizi di rete (es. www, mail, ecc.)
- Livello 7: per accedere alle applicazioni e servizi di alto livello

Le infrastrutture e i processi di autenticazione ai livelli inferiori possono essere a servizio delle procedure di accesso ai livelli superiori.
L’accesso ai livelli superiori puo’/deve presupporre l’autenticazione/autorizzazione ai livelli inferiori.

Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

Autenticazione e Autorizzazione

Ambito di autenticazione e Single-Sign-On

Ambito di Autenticazione

Complesso degli host, risorse, servizi che condividono, ad un determinato livello, lo stesso sistema di autenticazione in corrispondenza del quale essi rilasciano di volta in volta le autorizzazioni di accesso.

- Autent. locale: ogni postazione alla quale si accede utilizza un proprio *Account DB*
- Autent. centralizzata: tutte le postazioni di accesso utilizzano un unico *Account DB*

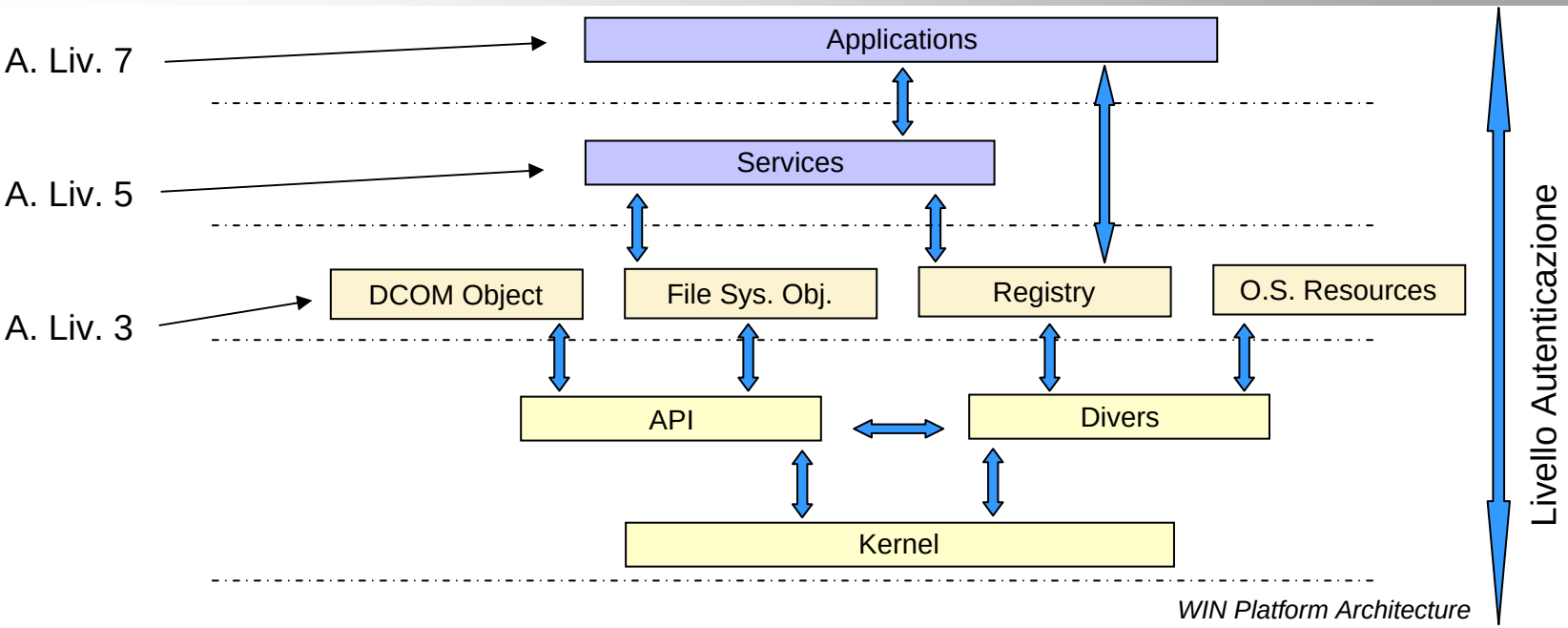
Single Sign On

Caratteristica che circoscrive le piattaforme, i servizi, le applicazioni ai quali e' possibile accedere a seguito di un unico processo di autenticazione, senza che la stessa sia richesta/necessaria ogni volta.

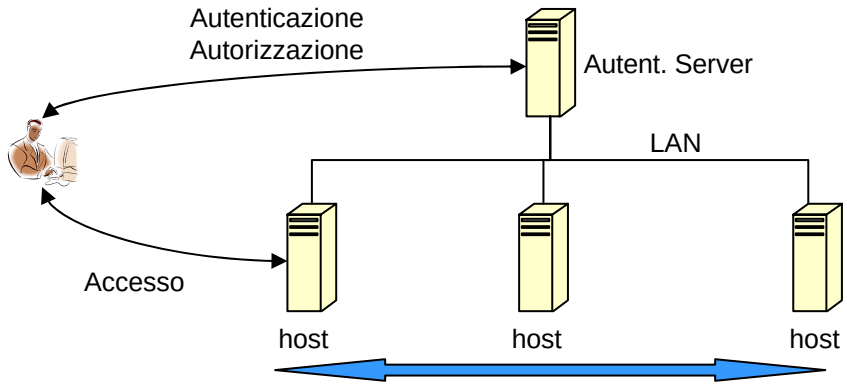
Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

Autenticazione e Autorizzazione

Schematizzazione degli ambiti



WIN Platform Architecture

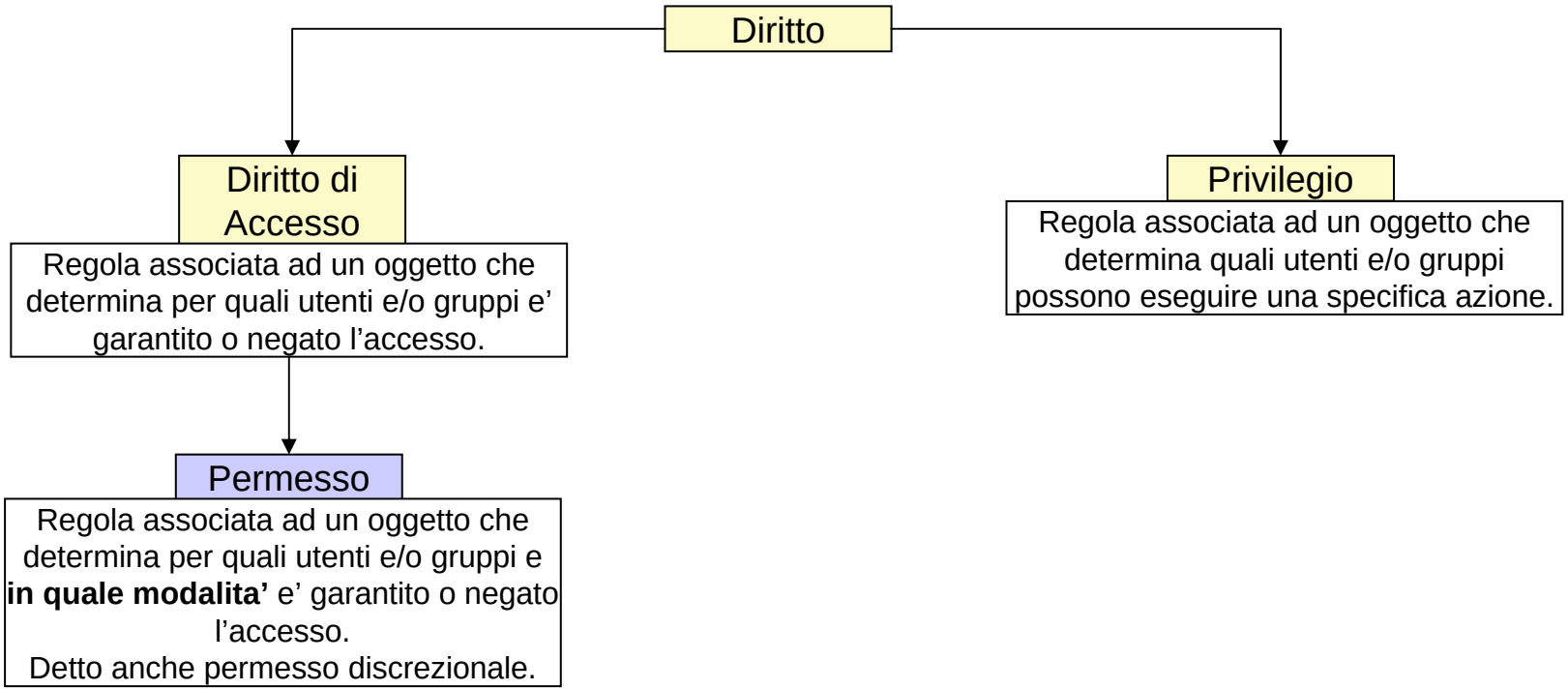


WIN Platform Architecture

Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

Autenticazione e Autorizzazione

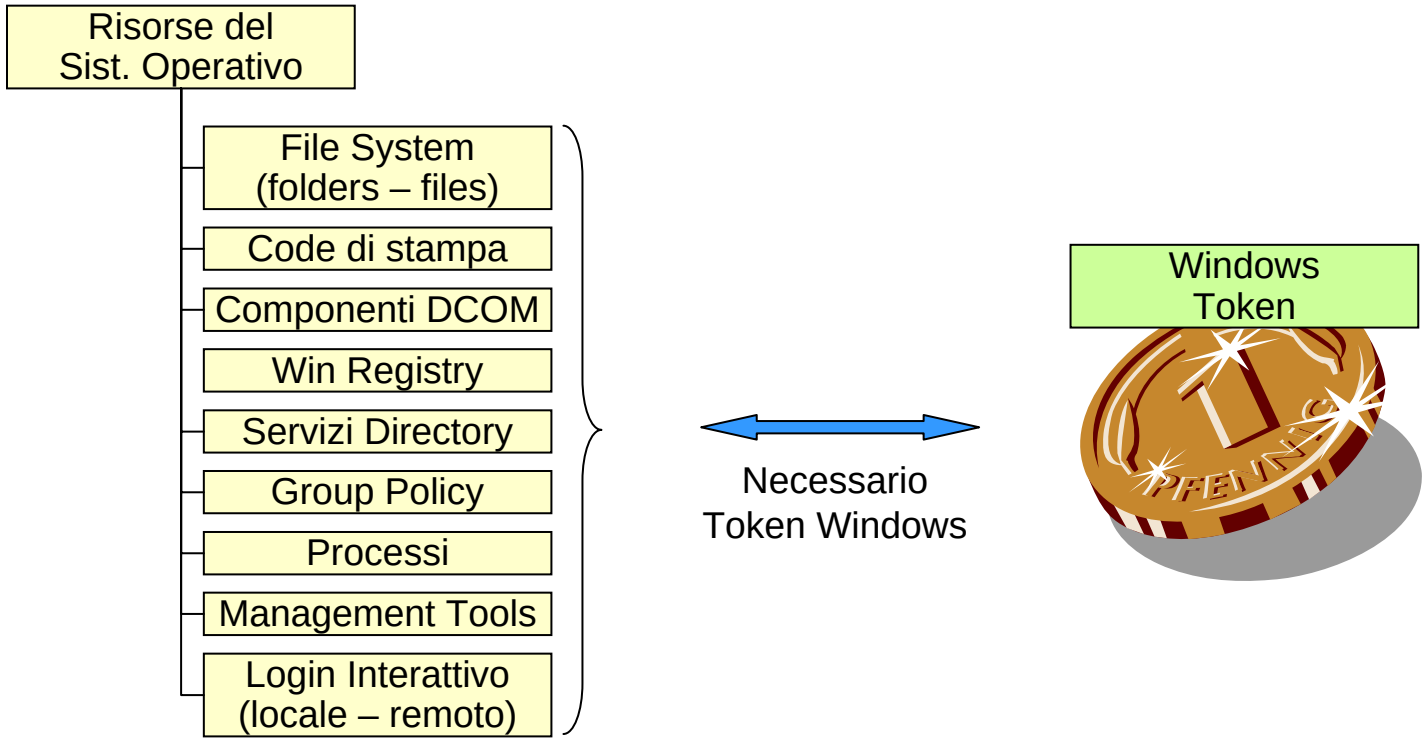
Regole di accesso



Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

Principi di WNT-Security

Accesso alle risorse e oggetti di sistema



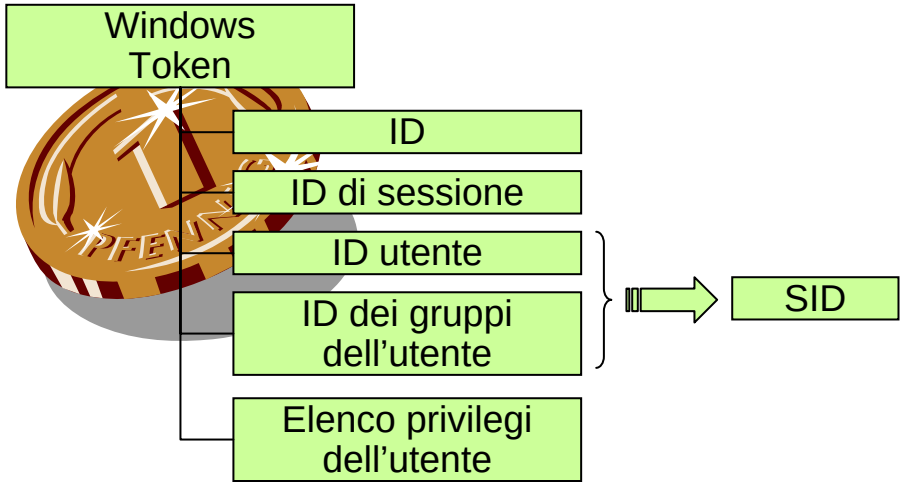
Token

Particolare pacchetto cifrato di identificazione, rilasciato dall'infrastruttura di autorizzazione, che contiene *informazioni di protezione* costituite dagli *ID* dell'utente, dai gruppi di appartenenza e dall'elenco dei privilegi associati.

Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

Principi di WNT-Security

Token Windows



SID: Identificatori di protezione

- Identificano univocamente un utente o un gruppo
- Sono memorizzati come dati binari
- Sono rappresentati come stringhe
- Per un host windows, che non e' controller di dominio, sono definiti nel SAM DB e mappati nel *Registro di Configurazione*

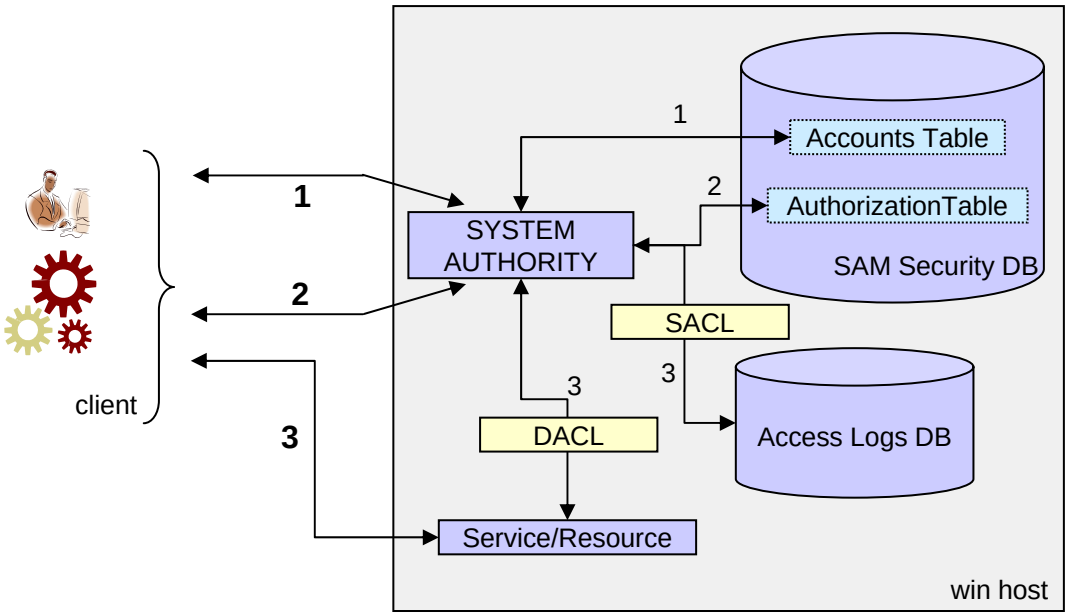
Privilegi

- Definiscono permessi speciali
- Concedono facolta' di azione (es.: eseguire lo shutdown locale e/o remoto)
- Non interessano necessariamente l'accesso agli aggetti di sistema
- Sono attribuiti ad utenti e/o gruppi
- La maggior parte sono inizialmente disabilitati per sicurezza

Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

Principi di WNT-Security

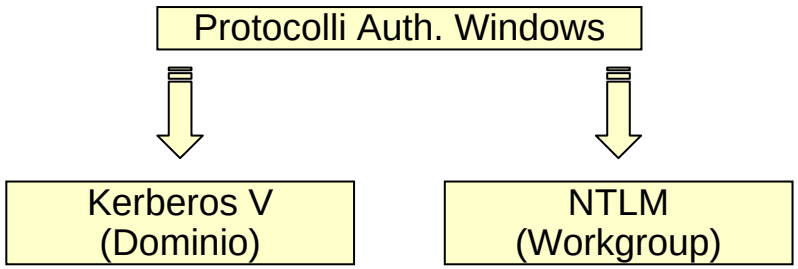
Autenticazione e Autorizzazione Locale



1. **Autenticazione**: la LSA convalida delle credenziali utente (username – password) presso un *Account DB (SAM)* residente/esportato dal Registro Windows
2. **Identificazione-Autorizzazione**: la LSA rilascia un informazioni di protezione in un *token* che definiscono l'utente, i relativi gruppi di appartenenza, i diritti/privilegi
3. **Autorizzazione-Accesso**: le informazioni contenute nel *token* sono confrontate/convalidate mediante la lista di autorizzazioni definite per la risorsa richiesta al fine di:
   - Autorizzare e disciplinare l'accesso
   - Generare logs per gli eventi di accesso che si intente monitorare

I processi di autenticazione e autorizzazione sono definiti da un complesso di regole

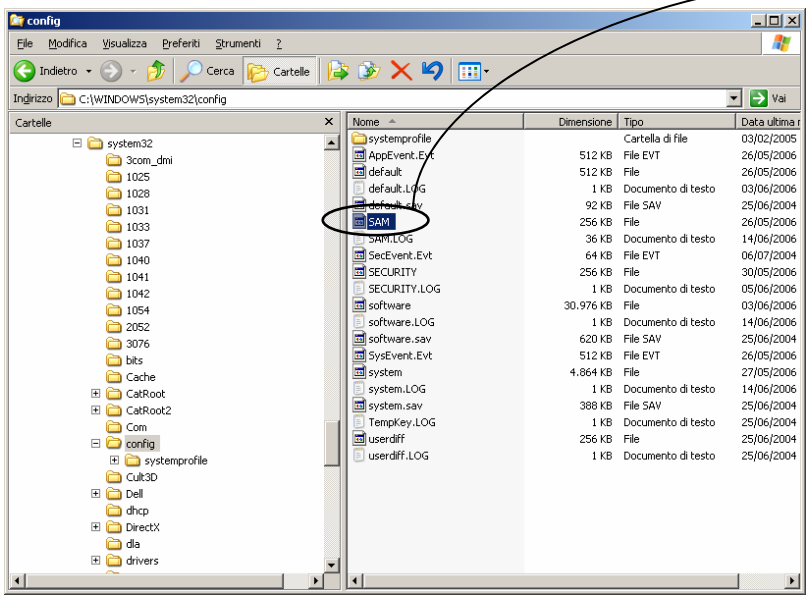
che contraddistingue un Protocollo di Autenticazione



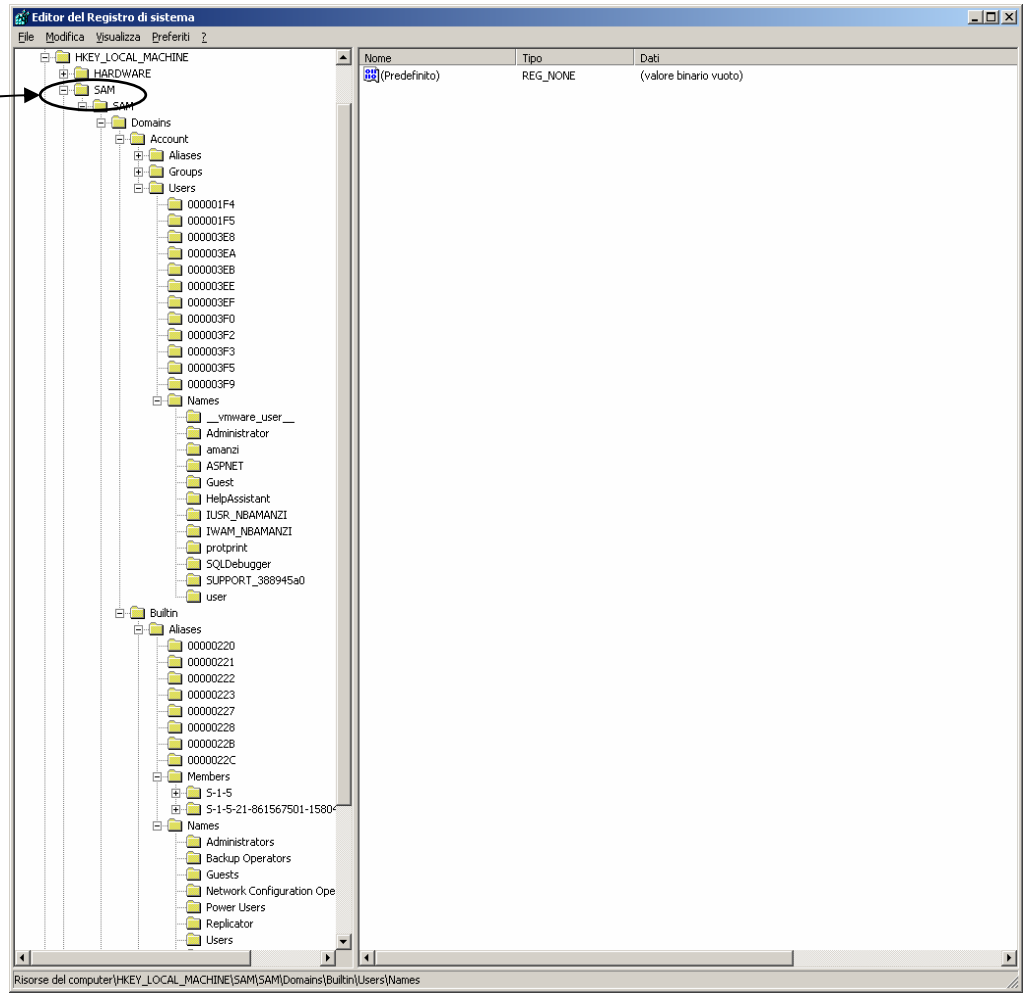
Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

Principi di WNT-Security

SAM Account DB



%systemroot%\system32\config

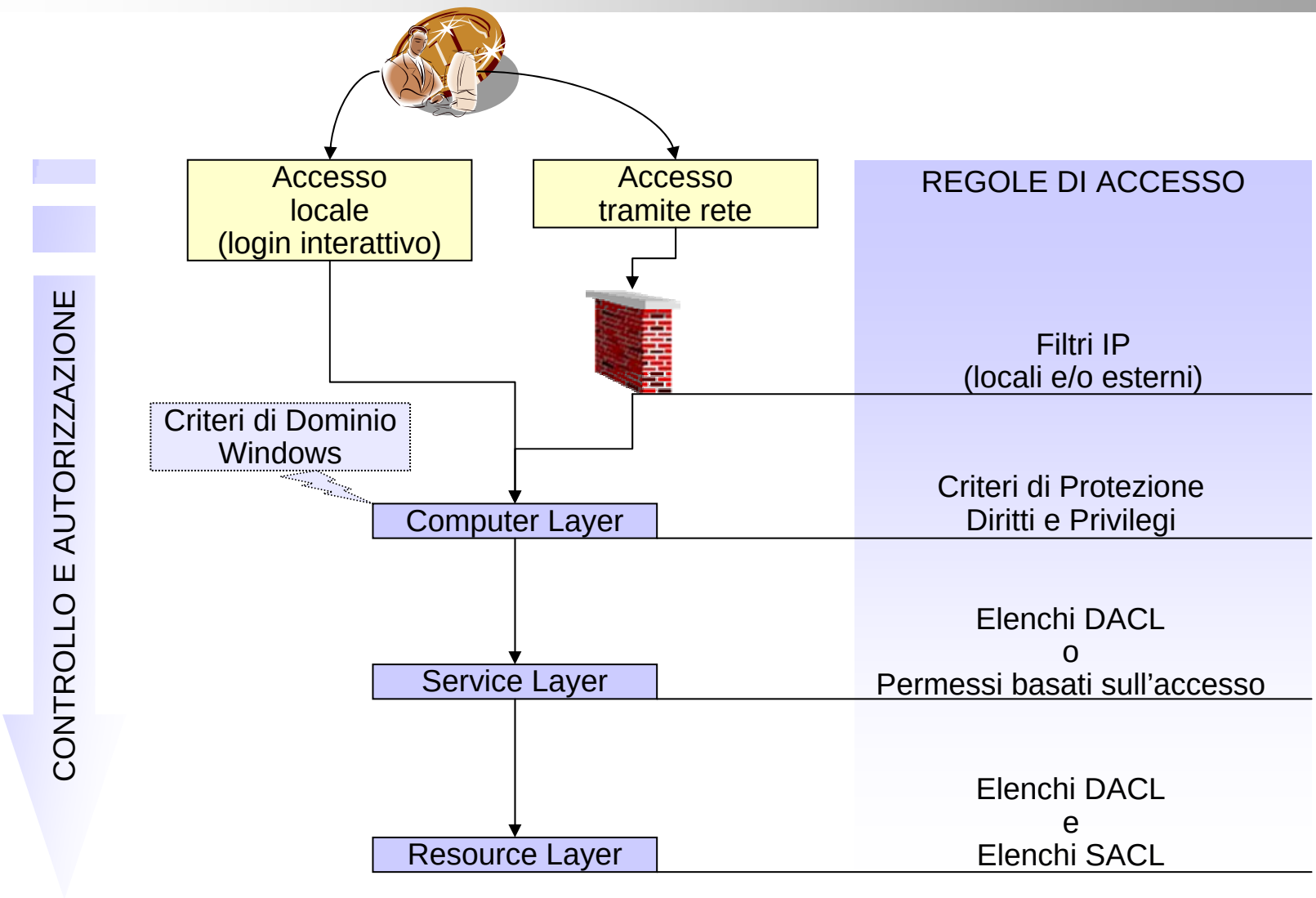


HKEY_LOCAL_MACHINE\SAM

Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

Principi di WNT-Security

Livelli di autorizzazione

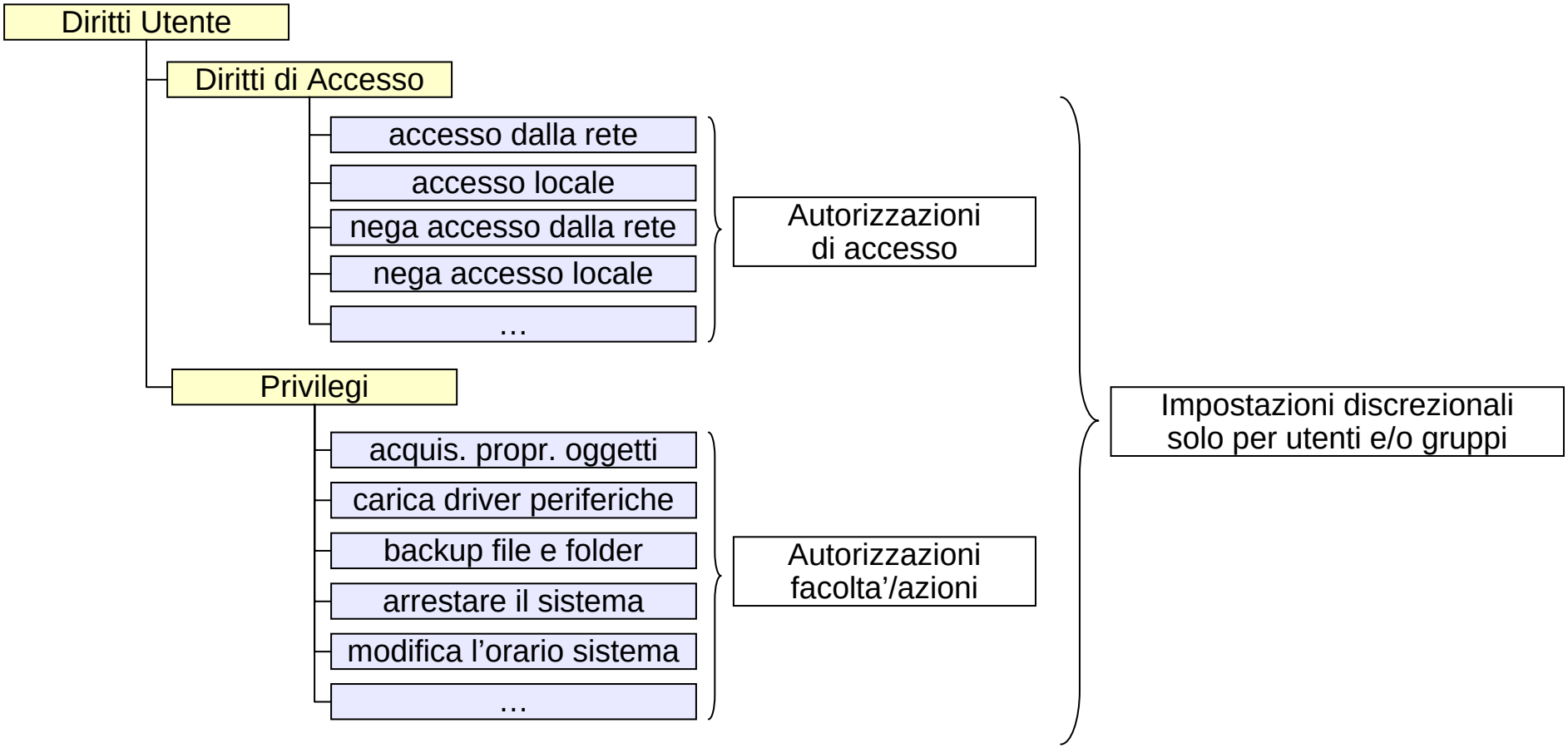


Per l'accesso vengono confrontati le informazioni di protezione contenute nel token con le autorizzazioni definite ai vari livelli

Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

Principi di WNT-Security

Computer Layer



Le impostazioni locali

- possono essere modificate tramite il comando secpol.msc (Windows XP/Server 2003)
- possono essere sovrascritte/ereditate se il pc e' membro di un dominio

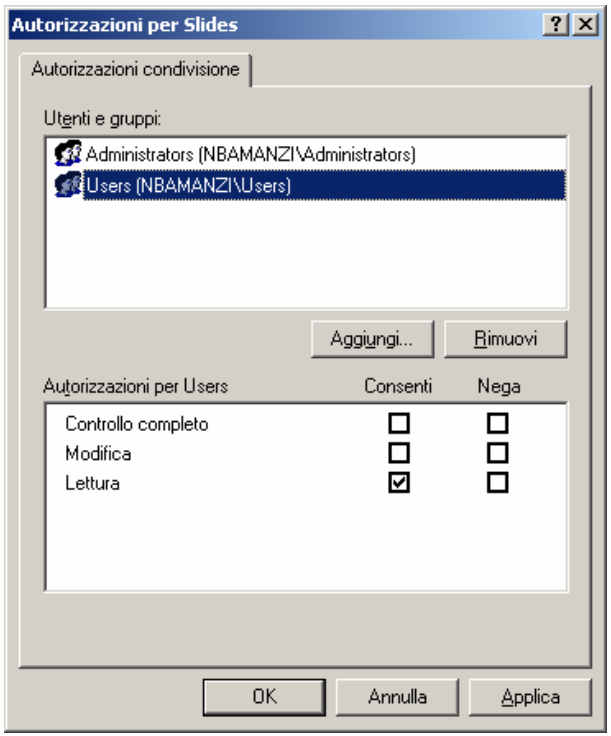
Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

Principi di WNT-Security

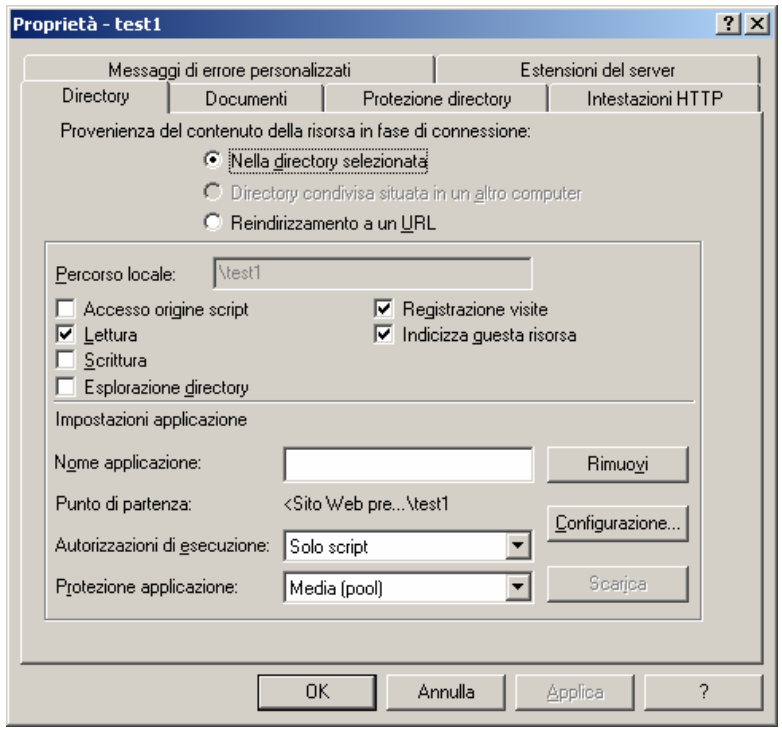
Service Layer

Le autorizzazioni:

1. possono essere definite nell'ambito di elenchi di controllo discrezionali sia in base ai SIDs (utenti e/o gruppi) che in base alla modalita' di accesso
2. Possono contemplare solo specifiche modalita' di accesso per le quali l'autorizzazione e concessa o negata senza discrezionalita' sull'utente o sui gruppi



1 – DACL per condivisione folder

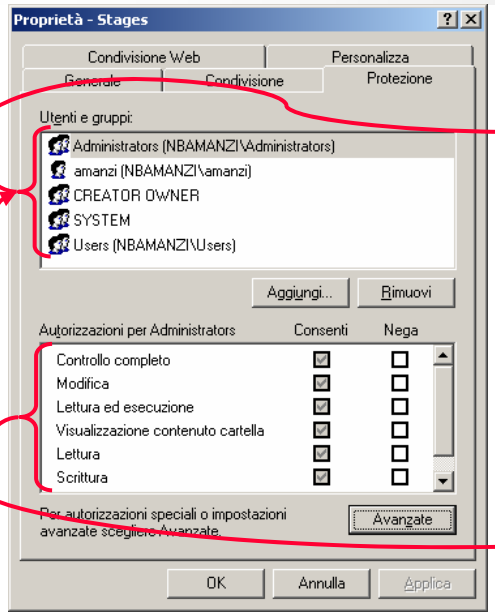


2 – Autorizzazioni di accesso per web-folder

Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

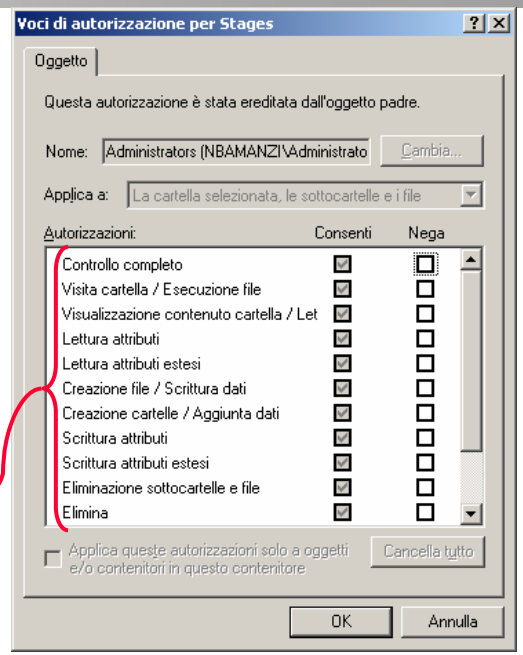
Principi di WNT-Security

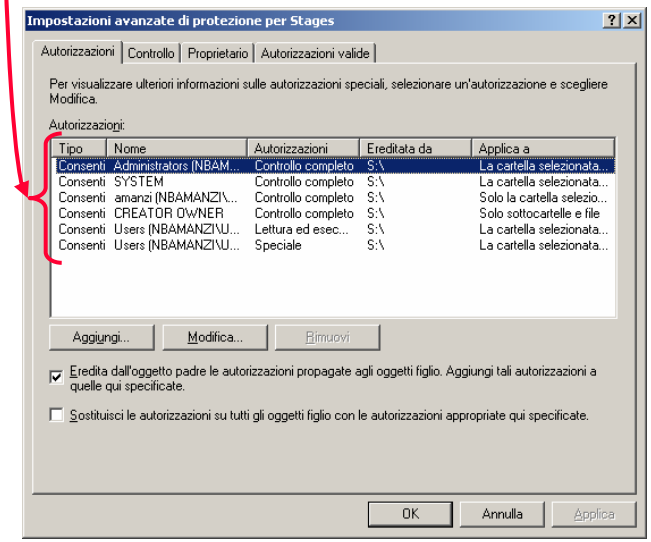
Resource Layer: DACL



DACL
(Elenchi discrezionali controllo accesso)
Elenco relativo agli utenti e/o gruppi ai quali sono attribuite le autorizzazioni

ACE (Access Control Entries)
elenco permessi di accesso relativi all'oggetto, assegnati/negati all'utente e/o al gruppo





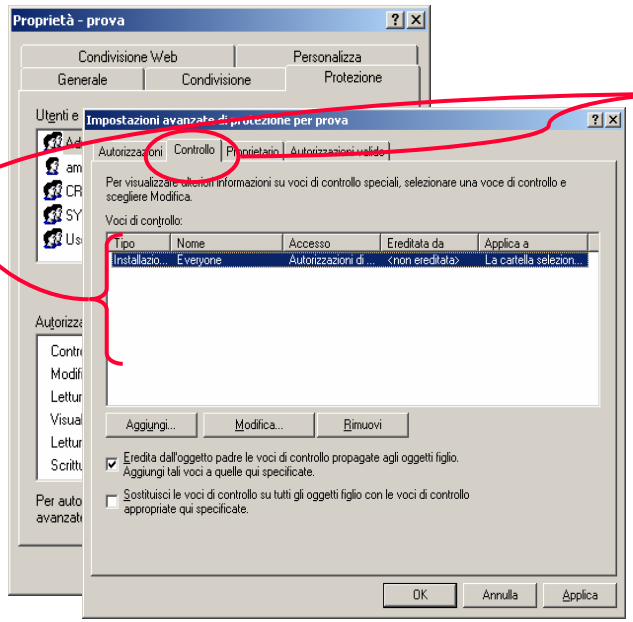
Le autorizzazioni:

- Sono discrezionali rispetto all'utente/gruppo e alla modalita' di accesso
- Sono definite dal proprietario dell'oggetto e da utente autorizzato
- A livello di container padre (es. folder) sono definite le politiche di propagazione per ereditarieta'
- Possono essere ereditate o no da un oggetto figlio
- Possono essere applicate/ripristinate dal padre a tutti gli oggetti subordinati

Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

Principi di WNT-Security

Resource Layer: SACL



2

SACL

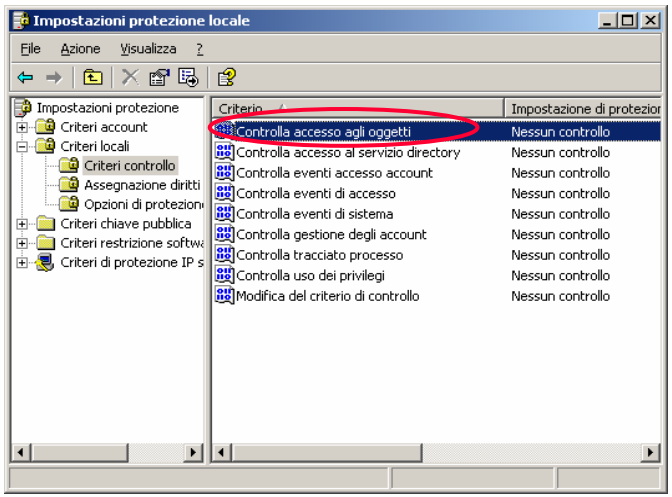
(Elenchi discrezionali controllo del sistema)

Elenco relativo agli utenti e/o gruppi dei quali si intende monitorare dichiarati eventi di accesso (riusciti/falliti)

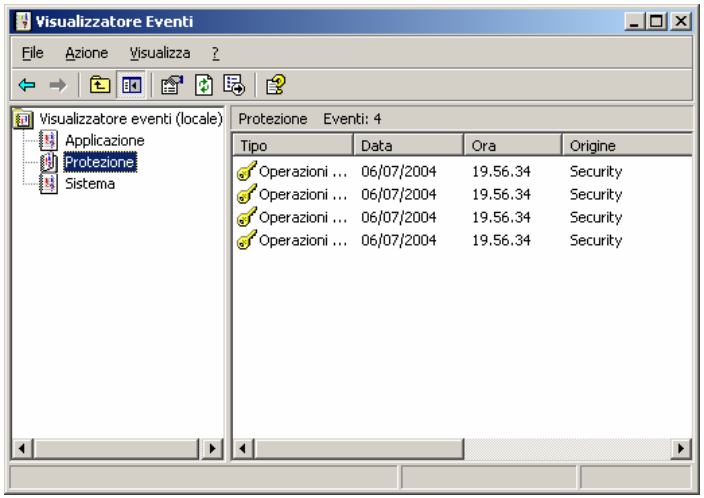
Monitoraggio eventi accesso oggetti ⟺ Audit

Procedure

1. Abilitazione dell'Audit a livello di sistema mediante secpol.msc
2. Definizione delle autorizzazioni associate agli accessi da intercettare/loggare
3. Gli eventi sono letti tramite eventvwr.msc



1

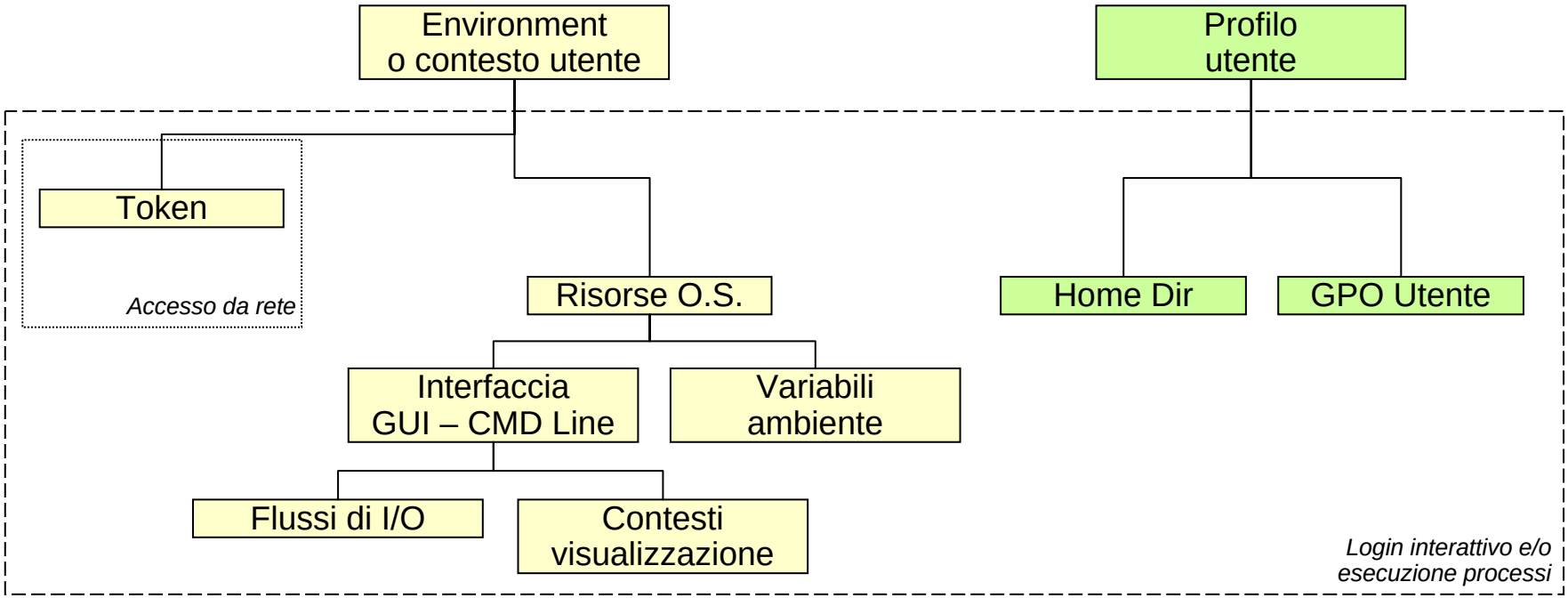


3

Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

Identificazione utente.

All'utente autenticato sono associate informazioni e risorse relative di autorizzazione, configurazione, preferenze e politiche per l'accesso e l'uso del sistema.

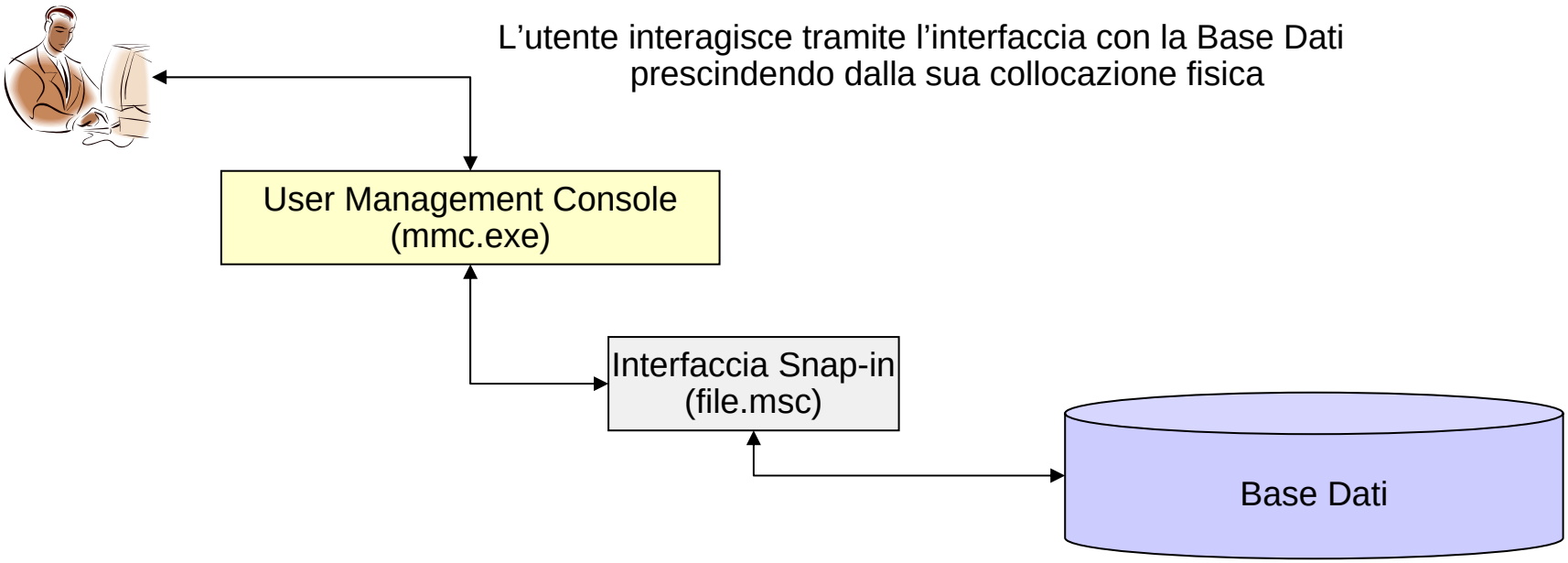


Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

Win Management & Profiling

Management Tools

- Una piattaforma windows puo' essere amministrata mediante un unico strumento GUI denominato Microsoft Management Console
- La console e' attivabile in Start/Run mediante il comando mmc.exe
- La gestione si esplica mediante particolari file .msc denominati *snap-in*
- Gli *snap-in* predefiniti risiedono in %systemroot%\system32
- Ogni *snap.in* costituisce un'interfaccia di gestione e definisce le regole, i metodi di accesso alla specifica base dei dati con la quale si intente interagire
- Distinti *snap-in* possono essere aggregati in un unico file .msc tramite MMC



Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

Win Management & Profiling

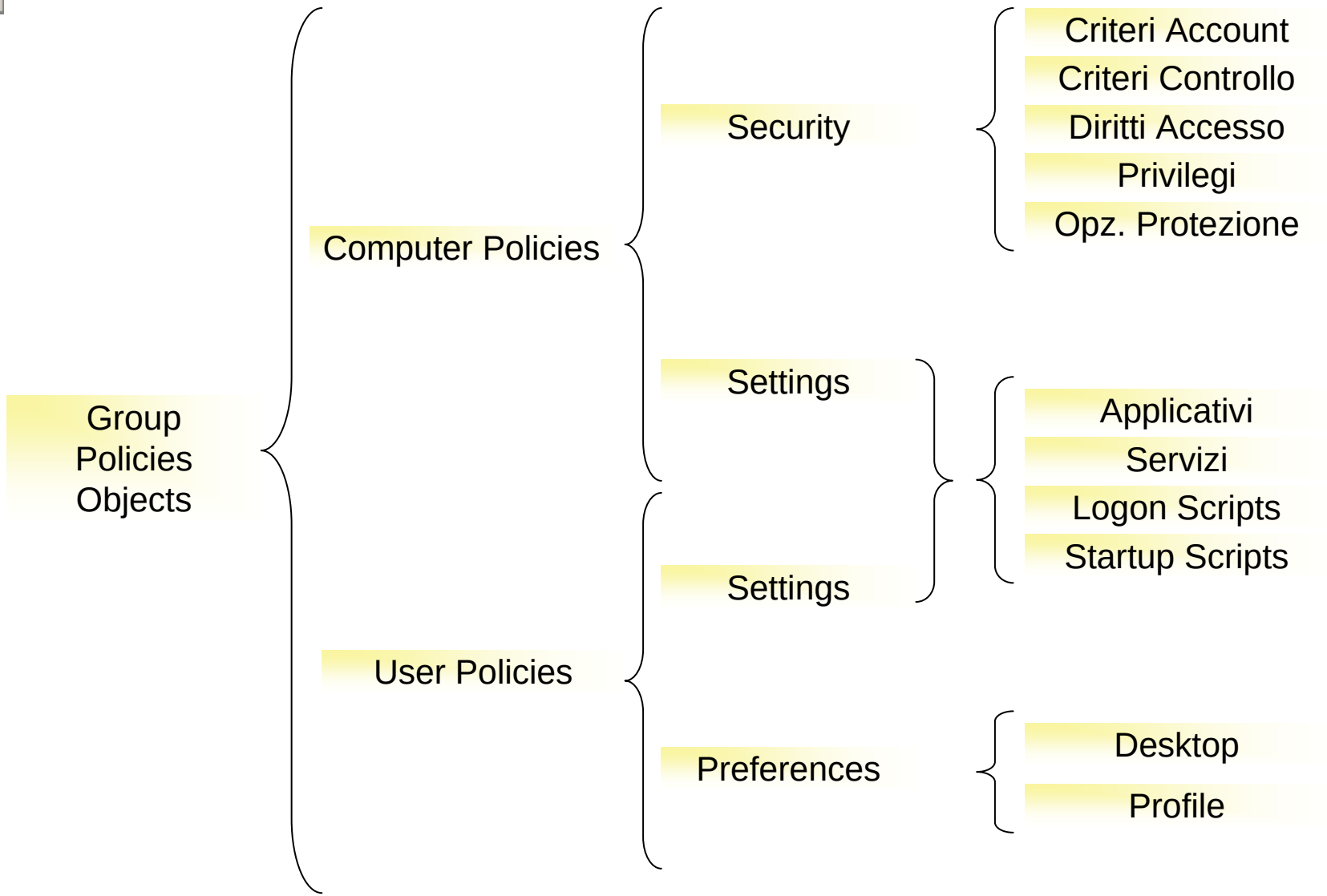
Snap-In locali predefiniti

certmgr.msc	Gestione Certificati Host/Utenti
ciadv.msc	Sistema indicizzazione file (ottimizza le ricerche)
compmgmt.msc	Servizi componenti
devmgmt.msc	Gestione periferiche
dfrg.msc	Deframmentazione file system
diskmgmt.msc	Amministrazione dischi – volumi - partizioni
eventvwr.msc	Visualizzazione eventi di sistema
fsmgmt.msc	Gestione oggetti condivisi
gpedit.msc	Amministrazione Group Policies locali (GPO)
lusrmgr.msc	Gestione account utenti e gruppi
ntmsmgr.msc	Archivi e supporti rimovibili
perfmon.msc	Monitoraggio prestazioni – Gestione Alert
rsop.msc	Elaborazione Criteri di Gruppo Risultante
secpol.msc	Criteri di protezione locali
services.msc	Servizi
wmimgmt.msc	Gestione console e servizi WMI
comexp.msc	Servizi e moduli componenti (DCOM – ActiveX)
iis.msc	Internet Information Services – Servizio Web, FTP, SMTP

Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

Win Management & Profiling

GPO: generalita' sullo snap-in



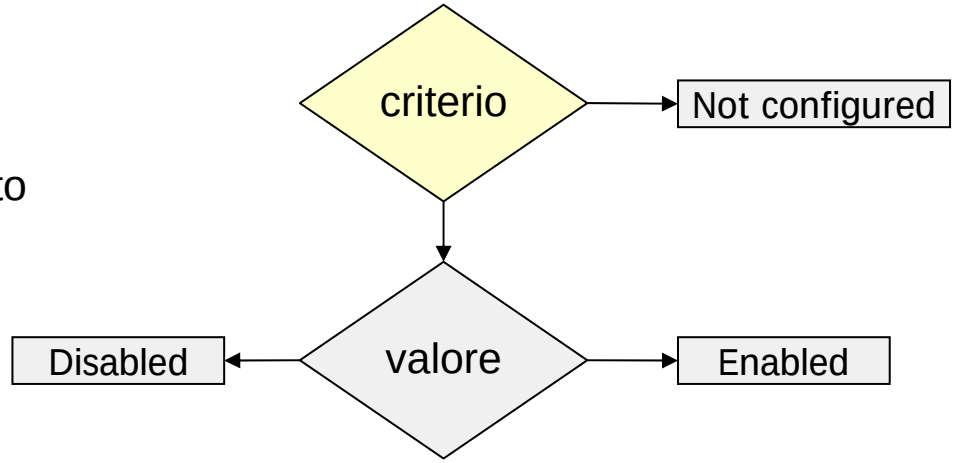
Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

Win Management & Profiling

GPO: struttura e composizione

I CRITERI DI GRUPPO

- costituiscono politiche o regole di alto livello
- sono strutturati in categorie
- possono avere impostazioni associate



Impostazioni tipiche di un criterio di GPO

Definizione di un criterio

- Caratterizzare la policy, la regola espressa dal criterio
- Fornire una descrizione esplicativa
- Definire l'elenco delle impostazioni di alto livello ammesse
- Definire un riferimento ovvero una procedera di accesso alla base di dati associata che contiene le impostazioni di basso livello

Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

Win Management & Profiling

GPO: caratteristiche di applicazione

GENERALITA' SULL'APPLICAZIONE DELLE GPO

- I criteri di *Configurazione Computer* sono applicati al computer indipendentemente dall'utente che esegue l'accesso
- I criteri di *Configurazione Utente* sono applicati agli utenti, che eseguono la sessione di login interattivo, indipendentemente dal computer al quale essi accedono
- Sono definiti a livello locale
- Sono definiti a livello di contenitori di Active Directory
- Nel dominio sono trasmessi agli oggetti utente e computer secondo meccanismi gerarchici e di ereditarieta'
- L'applicazione nel dominio windows e' discrezionale (DACL)

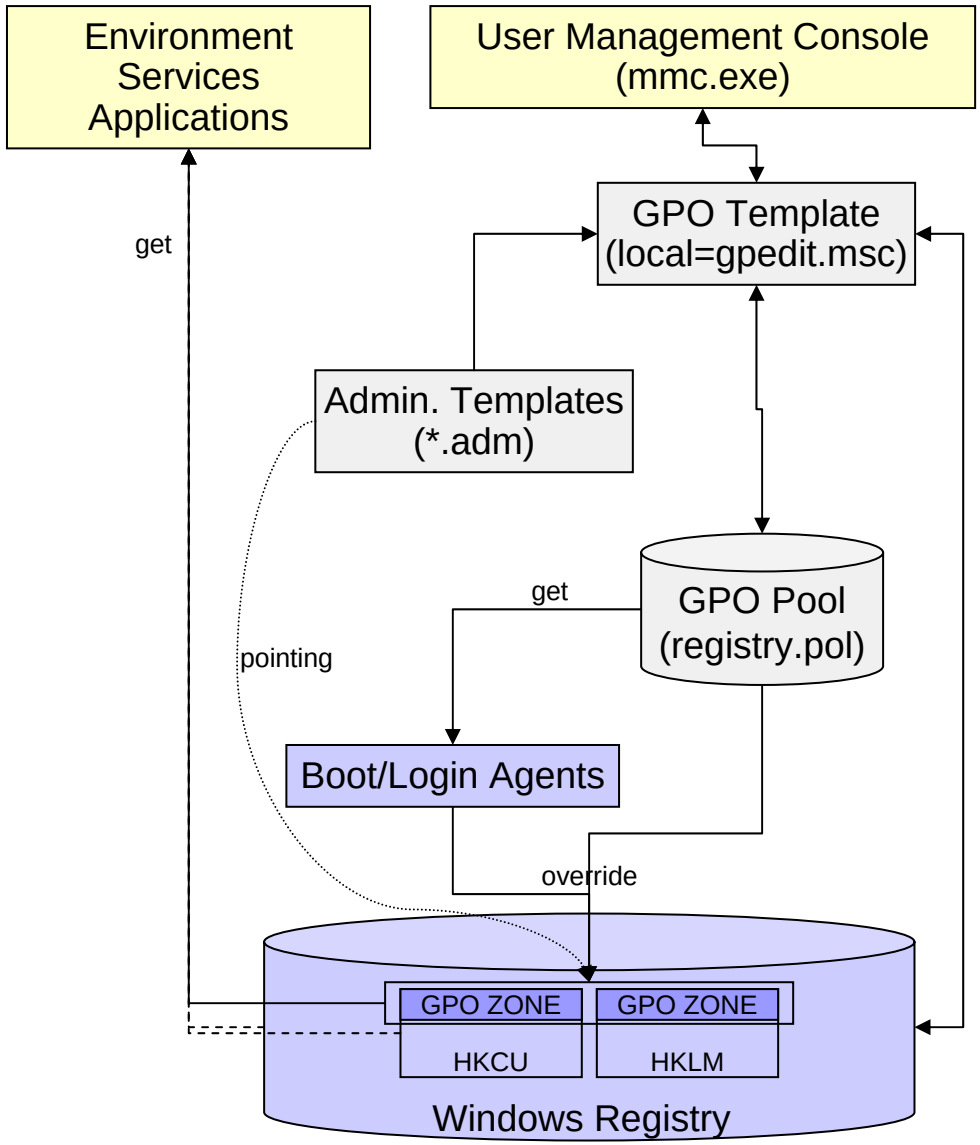
SCOPI DELLE GPO

- Gestire i criteri basati sul Registro di Sistema , generando files di impostazioni che interessano e sovrascrivono specifiche chiavi/valori nelle sezioni *HKEY_CURRENT_USER* e *HKEY_LOCAL_MACHINE*
- Assegnare scripts
- Reindirizzare cartelle (criteri di gruppo di dominio)
- Gestire applicazioni
- Specificare opzioni di protezione

Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

Win Management & Profiling

GPO: modello locale di applicazione



MODELLI AMMINISTRATIVI

- Realizzano un puntamento a chiavi del Registro di Configurazione
- Determinano un metodo di sovrascrittura delle chiavi/valori definite in zone speciali riservate alle GPO all'interno di *HKLM* e *HKCU*

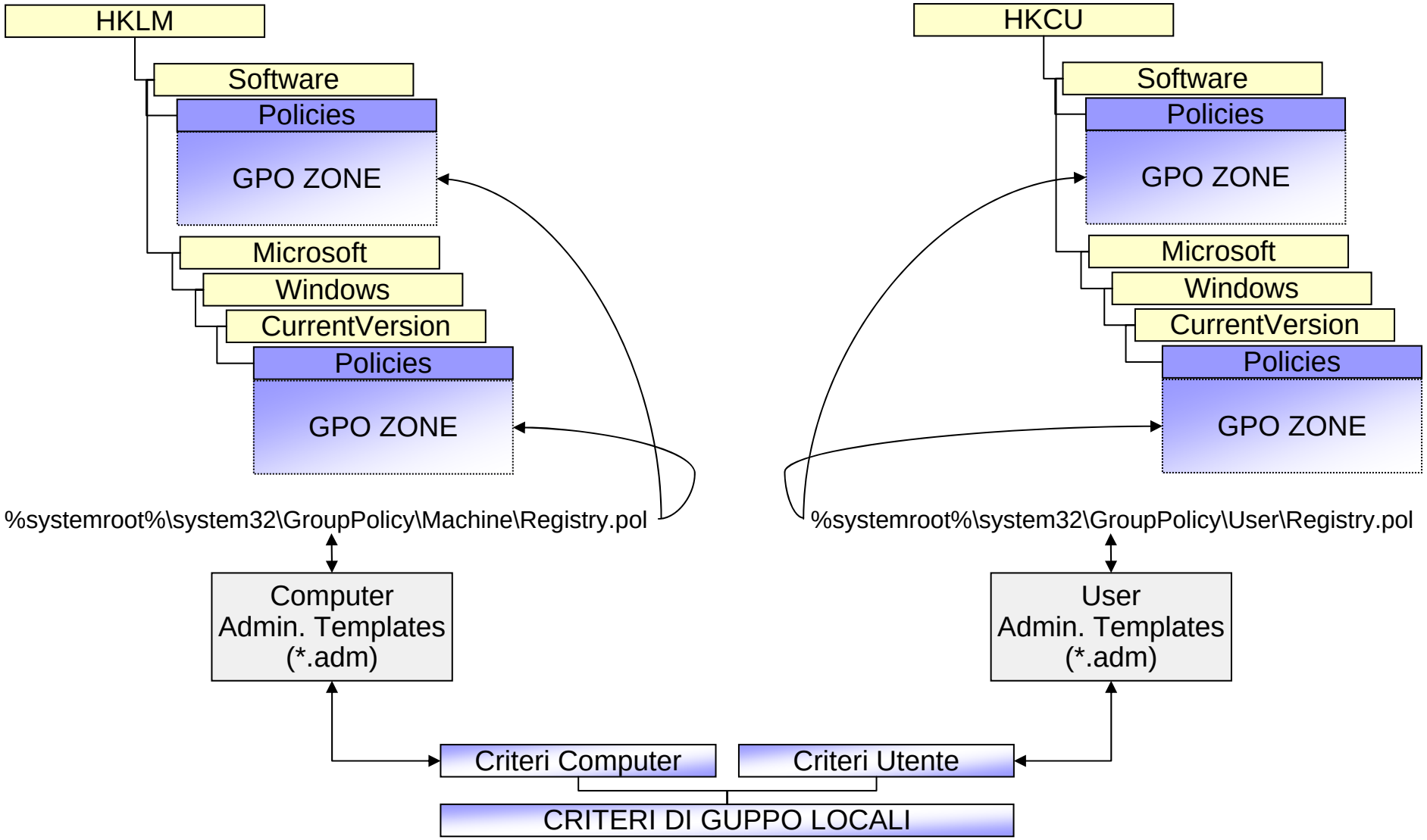
PROCEDURE LOCALI

- Le impostazioni definite mediante *Modelli Amm.vi* sono salvate nei file registry.pol
- I criteri computer e utente interagiscono rispettivamente con file registry.pol distinti
- I file registry.pol contengono un elenco di chiavi/valori/dati associati alle impostazioni definite mediante *Modelli Amm.vi*
- Durante il boot e il login le impostazioni aggiornate in registry.pol sono trasferite nelle zone speciali rispettivamente in *HKLM* e *HKCU*

Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

Win Management & Profiling

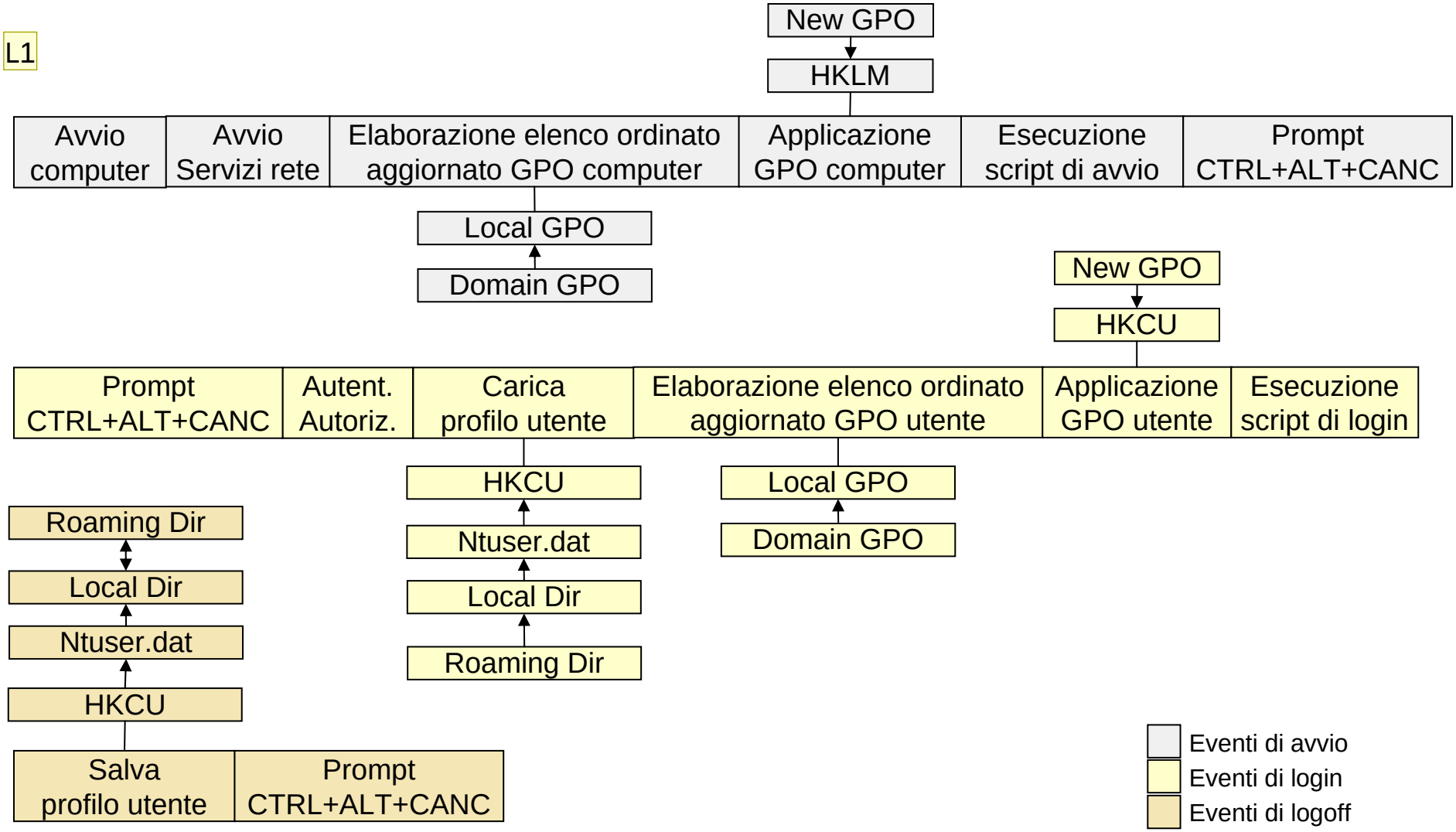
GPO: impatto sul Win Registry



Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

Win Management & Profiling

GPO: sequenza degli eventi di elaborazione



Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

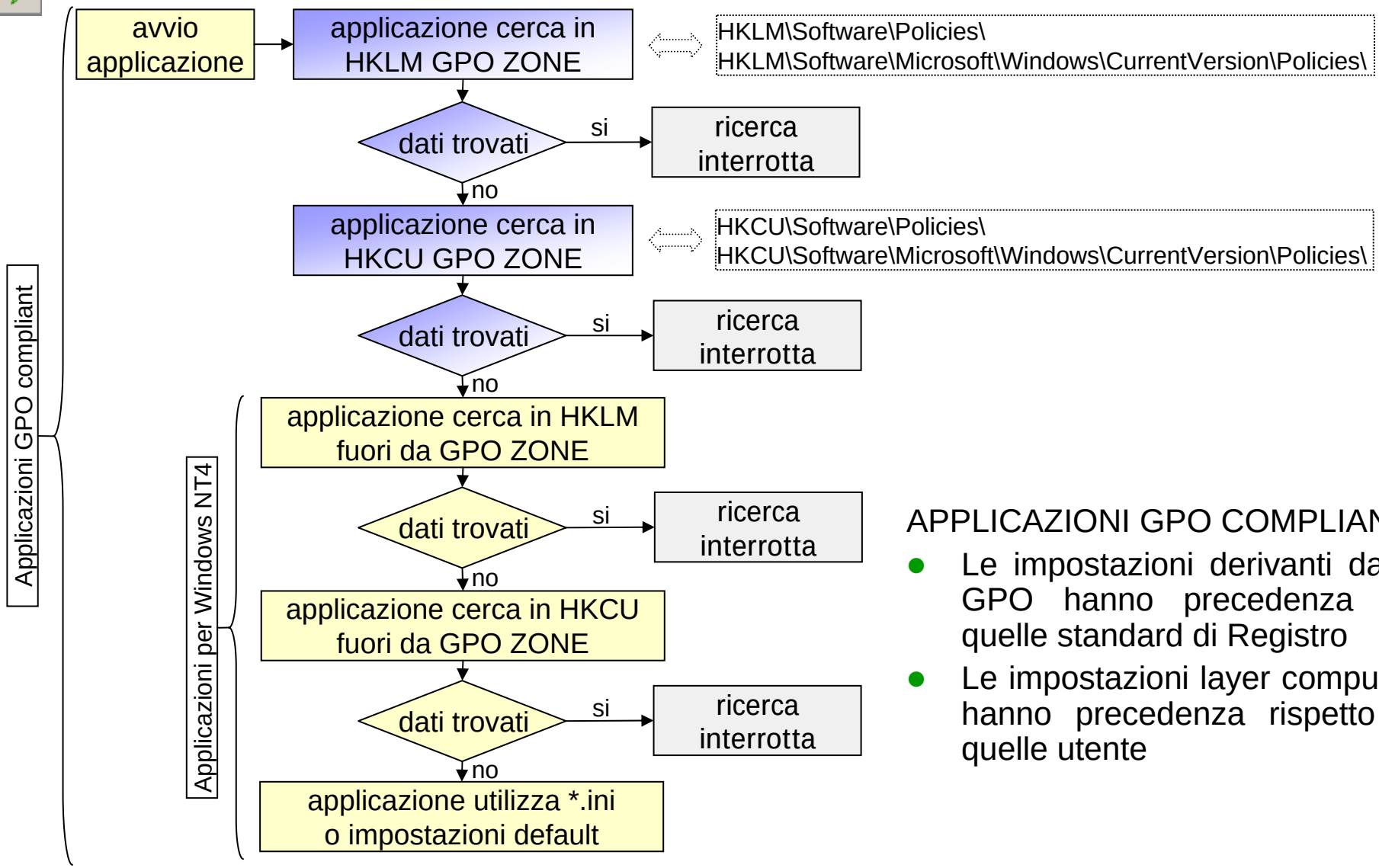
L1

Le GPO sono ritenute nuove se la data di modifica del registry.pol e' piu' recente della data di applicazione delle stesse.
L'applicazione consiste nella scrittura nel registro dei criteri residenti in registry.pol. La data di applicazione presumibilmente e' scritta nel registri o i file di log opportuni (es. ntuser.dat.log).

LNF; 20/06/2007

Win Management & Profiling

GPO: priorita' di esecuzione per le applicazioni



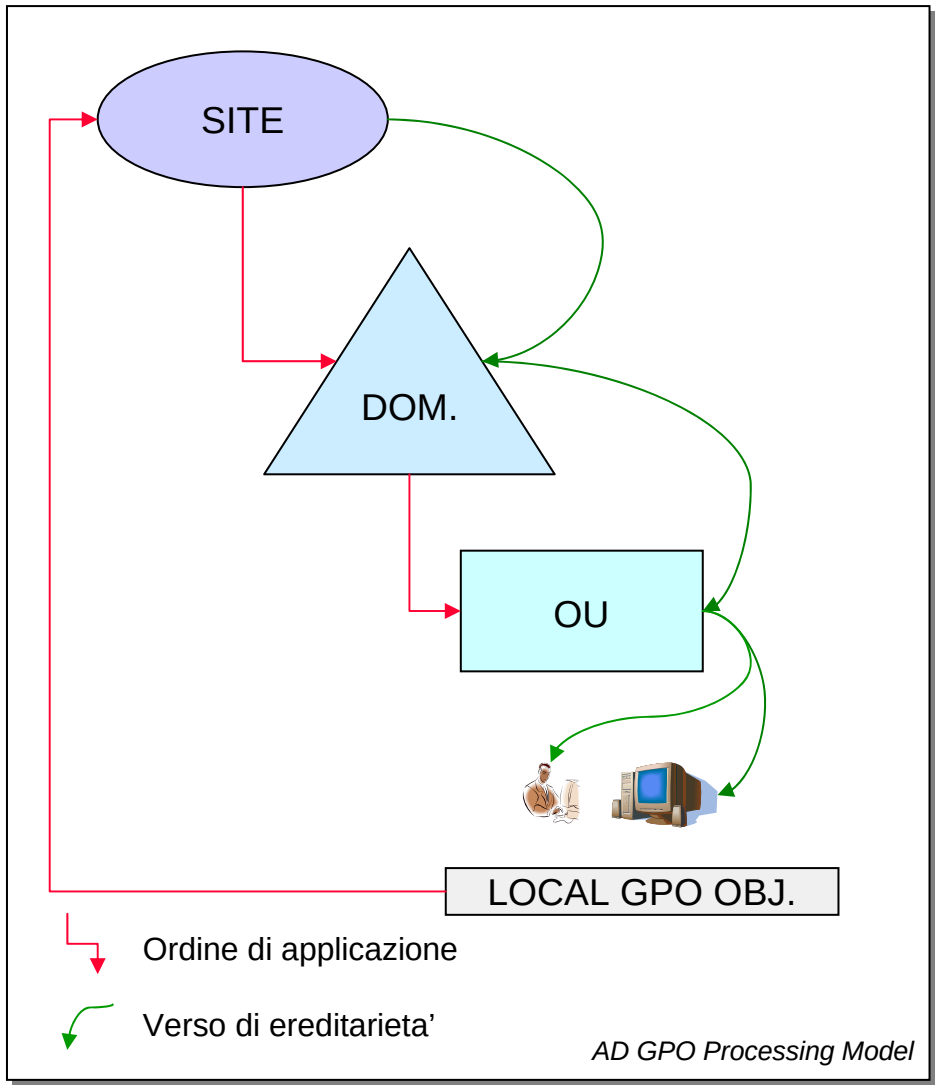
APPLICAZIONI GPO COMPLIANT

- Le impostazioni derivanti dalle GPO hanno precedenza su quelle standard di Registro
- Le impostazioni layer computer hanno precedenza rispetto a quelle utente

Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

Win Management & Profiling

W - Domain GPO Processing Model



EREDITARIETA' DEI CRITERI

- I criteri definiti nei contenitori padri sono trasmessi a tutti i subordinati per ereditarieta', compresi gli oggetti computer ed utente
- I criteri non definiti non vengono ereditati
- Se un contenitore figlio definisce uno stesso criterio presente nel padre, la nuova impostazione ha precedenza
- Se non vi e' conflitto di impostazione tra padre e figlio, il criterio e' ereditato con l'impostazione definita nel figlio

Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

Riferimenti

NT-Security	http://www.microsoft.com/technet/prodtechnol/windowsserver2003/it/library/ServerHelp/fcbc82eb-f896-4be3-85d0-470ac172b50f.mspx
Win Scripting	http://msdn2.microsoft.com/en-us/library/ms950396.aspx
GPO	http://msdn.microsoft.com/library/default.asp?url=/library/en-us/gp/rsrc_gp.asp
DCOM	http://msdn2.microsoft.com/en-us/library/aa139672.aspx
Active Directory	http://www.microsoft.com/technet/prodtechnol/windowsserver2003/it/library/ServerHelp/a9d684f0-90b1-4c67-8dca-7ebf803a003d.mspx

Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

INFN
Istituto Nazionale di Fisica Nucleare
Laboratori Nazionali di Frascati

Cordiali saluti

Nunzio AMANZI

Windows Systems Administrator
INFN Windows Management Team
INFN SisInfo Management Team

INFN Computing Service