INFN Windows Group

Windows@INFN – CCR 14/15 Mar. 2006

Windows Activities Planning

Global Scenario Case Study

Nunzio AMANZI, LNF - INFN
E-mail: Nunzio.Amanzi@lnf.infn.it
www: http://www.lnf.infn.it/~amanzi
Phone: +39 6 94 03 2607-8225

Subjects Menu

1 - OVERVIEWS

- Current Windows Infrastucture
- Desiderata

2 - LNF PRINT SERVICE

- Common Interesting Subjects
- Security Policies
- Deploy & Management Proc.
- Rem. Access & Collabor. Tools
- Other Activities
- Global Windows Scenario
- Global Integration Model
- Local Windows Scenario
- Priority
- Collaboration Strategies

3 - IN DEPTH SUBJECTS

- Management Related Activities
- GPO Overviews
- Windows Dom. Structure Tips

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

1 - Overviews

Current Windows Infrastructure

LO STATO ATTUALE

- Le strutture windows si sono evolute in forma eterogenea
- Esiste un insieme di infrastrutture locali in genere basate su domini windows del tipo win.x.infn.it
- Non tutte le Sezioni hanno domini windows in produzione
- I diversi domini non sono correlati in termini implementativi/sistemistici
- Solo in alcuni casi i domini includono la maggior parte dei nodi
- La gestione non coordinata dei client (soprattutto quelli fuori dominio) determina un evidente dispendio globale di energie

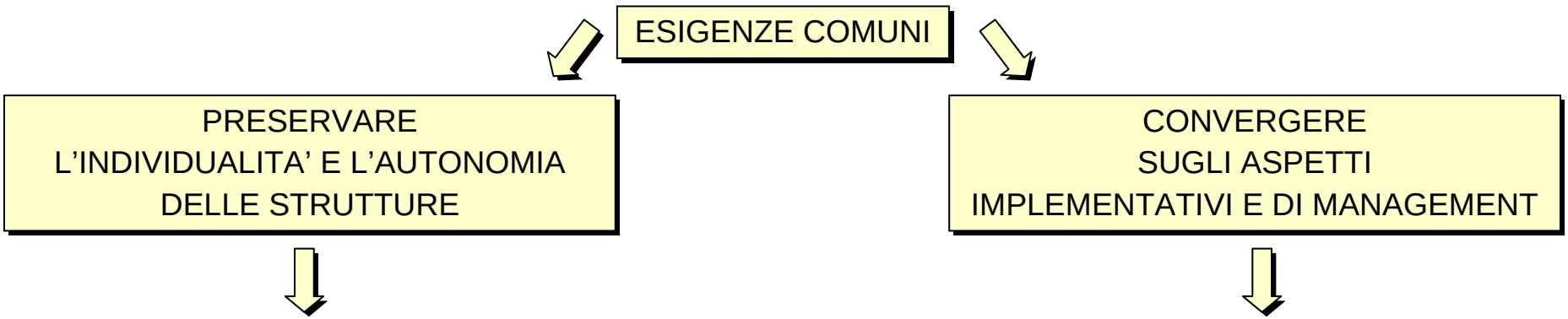
MOTIVAZIONI DI FONDO

- L'INFN e' basato su varie realta' locali
- Le unita' che costituiscono l'Ente hanno un assetto intrinsecamente autonomo
- L'utenza esprime esigenze specifiche e distinte che impattano sul *local computing*

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

1 - Overviews

Desiderata



PRESUPPOSTI PER L'ATTIVITA' DI COORDINAMENTO

- Sensibilizzare la collaborazione tra le Sedi nell'ambito del *Gruppo Windows INFN*
- Delineare i contesti di interesse comune
- Incentivare la comunicazione e l'interazione tra le Sezioni
- Promuovere attivita' proficue in un contesto globale definendo le relative strategie
- Sfruttare eventuali sinergie esistenti

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

2 - Activities Planning

Common Interesting Subjects

AREE TEMATICHE DI RILIEVO IN UN CONTESTO GLOBALE

- Politiche di Sicurezza
- Procedure di Deploy e Management
- Accesso Remoto
- Collaborative Tools
- Attivita' trasversali di sviluppo, test, supporto

GOALS

- Portabilita' delle implementazioni e delle procedure di gestione nei distinti scenari
- Propagazione delle impostazioni, definite ai vari livelli, anche ai client fuori dominio
- Fornire alle infrastrutture windows un'impronta globale volta a:
  - esportare servizi/risorse *intra* e *inter* domini
  - uniformare e snellire le procedure di gestione e controllo
  - fronteggiare la carenza di *manpower*

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

2 - Activities Planning

Security Policies

- Politiche di sicurezza in ambito comune e linee guida per le implementazioni locali, in particolare:
  - esame delle vulnerabilita' e definizione di filtri IP locali
  - elaborazione di un modello di diritti/permessi layer macchina (GPO), servizio, risorsa
  - individuazione dei settings di rilievo a livello di GPO
- Meccaniche di propagazione delle GPO in ambito geografico/dominio/locale e modalita' di serving ai client intra/extra dominio
- Procedure per download e la distribuzione del software antivirus (Sophos)
- Meccaniche di aggiornamento per le definizioni delle impronte virali

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

2 - Activities Planning

Deploy & Management Procedures

- Procedure di installazione e cloning:
  - definizione di un workflow di installazione
  - rilascio di specifiche di configurazione per servizi/kits comuni (es. Printing,X-Server)
  - serving statico di immagini per nodi HAL compatibili (es. Rembo)
  - implementazione di *unattended procedures* per installazione da scratch del S.O.
- Uso delle GPO per la configurazione dei nodi e la predisposizione al monitoraggio coordinato
- Rilascio degli aggiornamenti windows (WSUS)
- Strumenti di monitoraggio dei nodi in termini di aderenza alle politiche di sicurezza (verifica settings, inst. antivirus, livello di patching…)

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

2 - Activities Planning

Remote Access & Collaborative Tools

- Difinizione di procedure per l'accesso remoto mediante RDP/WTS
  - impostazioni per TS de definire layer domain/client in ambito GPO
  - metodi di connessione RDP tramite port-forwanding su connessioni cifrate
- Serving e condivisione delle risorse di storage mediante:
  - implementazione di una infrastruttura DFS nella lan
  - definizione di front-end interfaccia/proxy per l'accesso DFS nella wan
  - procedure di autenticazione e accesso per il serving tramite WebDav
- Indivuazione degli strumenti ottimali per la collaborazione *on-fly*

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

2 - Activities Planning

Other Development & Support Activities

Attivita' trasversali orientate

- alla mobilita' degli utenti
- all'interoperabilita' tra le sedi
- ai test e al supporto per le valutazioni di fattibilita'

- X-Authentication
  - Modello comune di architettura di AD orientato al re-mapping degli utenti trusted
  - Meccaniche di acquisizione degli utenti che si autenticano in regni K5 (non windows)
  - Strategie di definizione delle memberships locali
- Scenari di test mediante macchine virtuali nell'ottica di:
  - Limitare l'impegno delle risorse
  - Produrre un impatto minimo sulle infrastrutture
  - Beneficiare di roll-back facilities, mobilita' e portabilita'

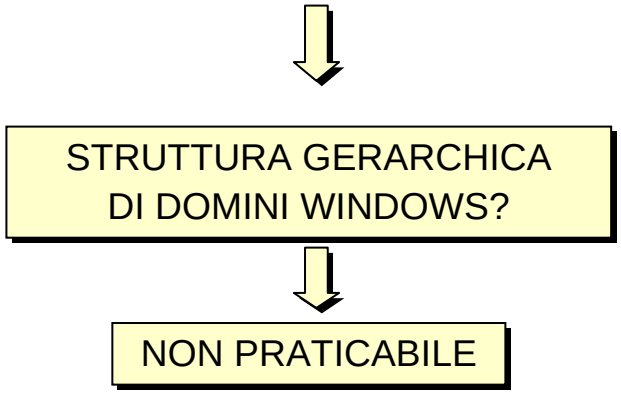
Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

2 - Activities Planning

Global Windows Scenario

LA PROBLEMATICA SULL'IMPLEMENTAZIONE DI UN'INFRASTRUTTURA GLOBALE

- Uniformare e globalizzare i processi di autenticazione per l'accesso alle risorse windows
- Collocare in un superlayer le GPO piu' comuni
- Individuare una strategia per la propagazione delle politiche/updates in ambito geografico



LA STRADA DA INTRAPRENDERE

- Proiettare le infrastrutture locali nell'ambito di un tree di autenticazione K5 in fase di consolidamento
- Definire opportune relazioni di trust tra il dominio win.x.infn.it e il *K5 Unix Realm* x.infn.it
- Creare opportuni *Windows Domain Local Groups* relativi ai singoli servizi da esportare
- Attribuire una membership locale agli utenti che si autenticano nel *K5 Unix Realm* locale e in quelli remoti
- Implementare un sistema globale/distribuito per il *serving* asincrono delle GPO in ambito geografico

STUDIO DI
FATTIBILITA'

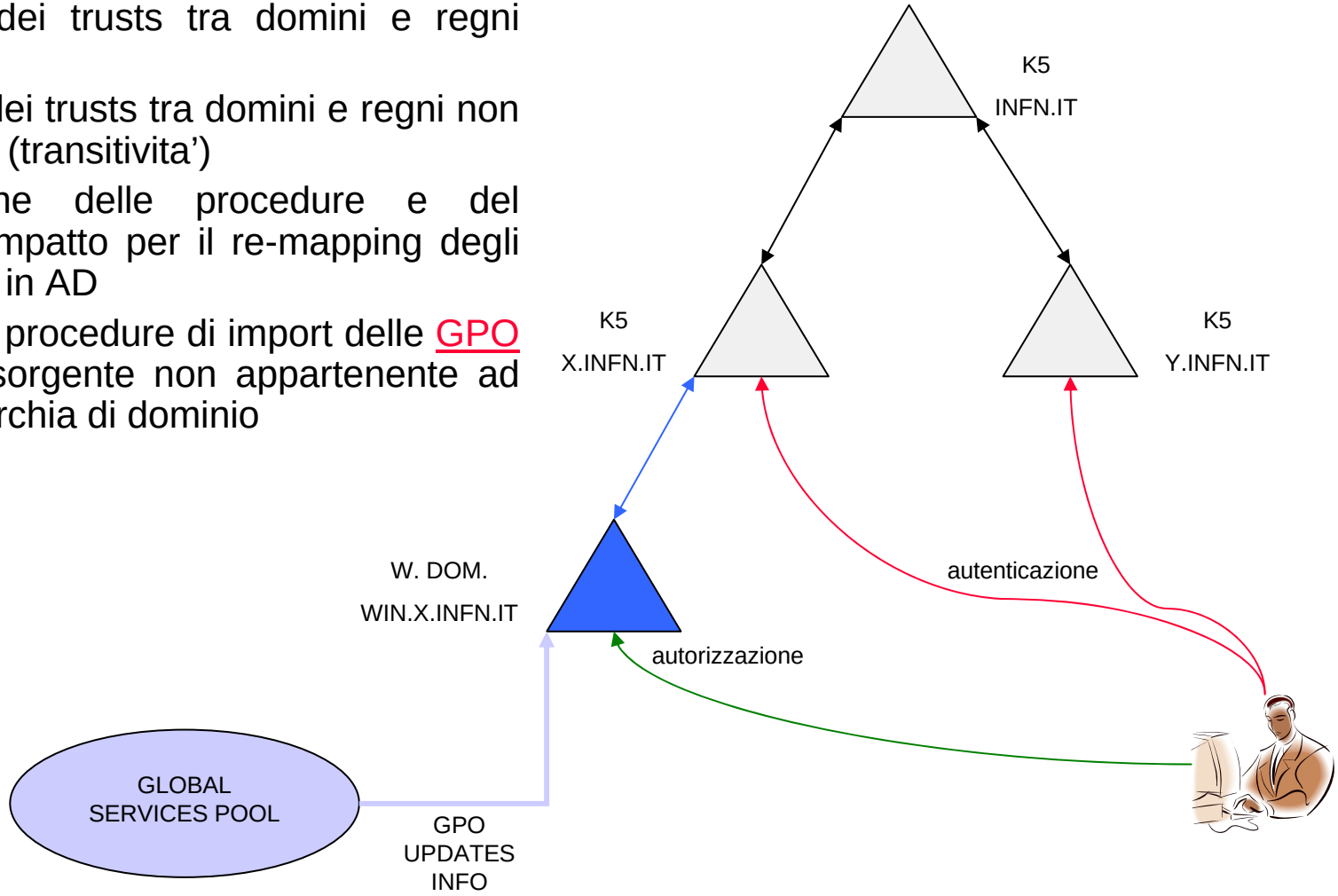
Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

2 - Activities Planning

Global Integration Model

VALUTAZIONI DI FATTIBILITA'

- Verifica dei trusts tra domini e regni adiacenti
- Verifica dei trusts tra domini e regni non adiacenti (transitivita')
- Definizione delle procedure e del relativo impatto per il re-mapping degli utenti K5 in AD
- Studio di procedure di import delle GPO da una sorgente non appartenente ad una gerarchia di dominio



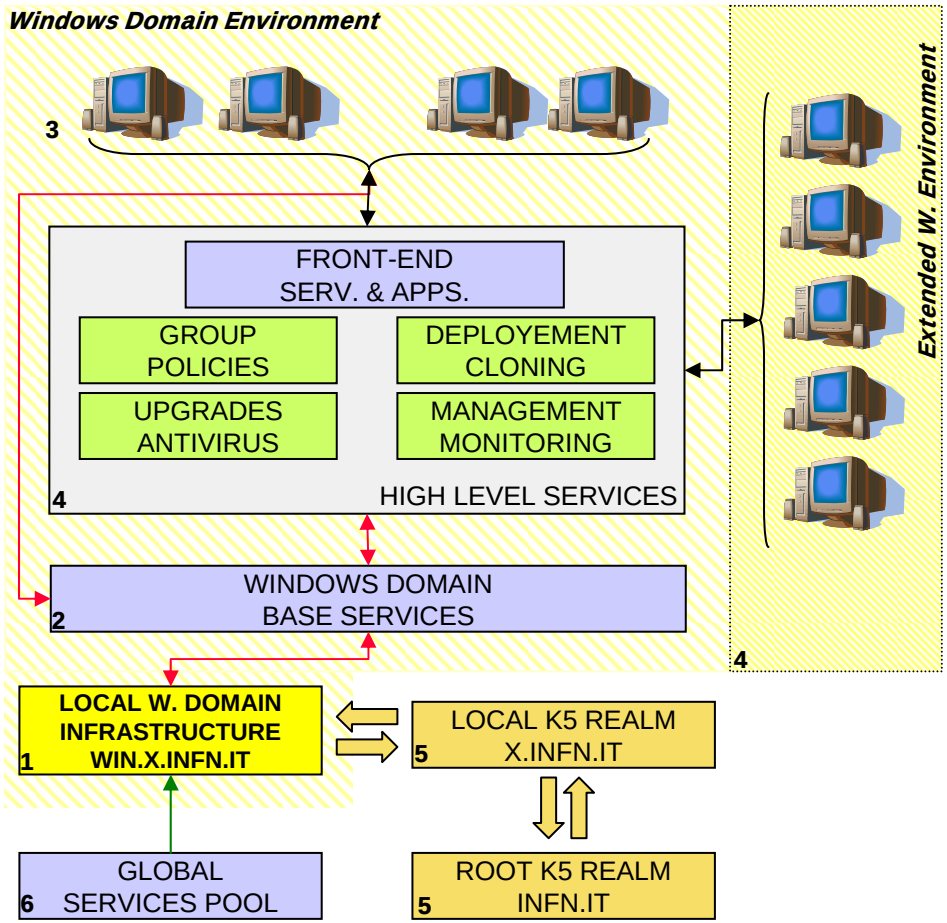
Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

2 - Activities Planning

Local Windows Scenario

APPROCCIO IMPLEMENTATIVO BASATO SU:

- Strutture di base di dominio windows definite in ambito locale
- Definizione di moduli di servizio/funzionalita' compatibili con le infrastrutture esistenti

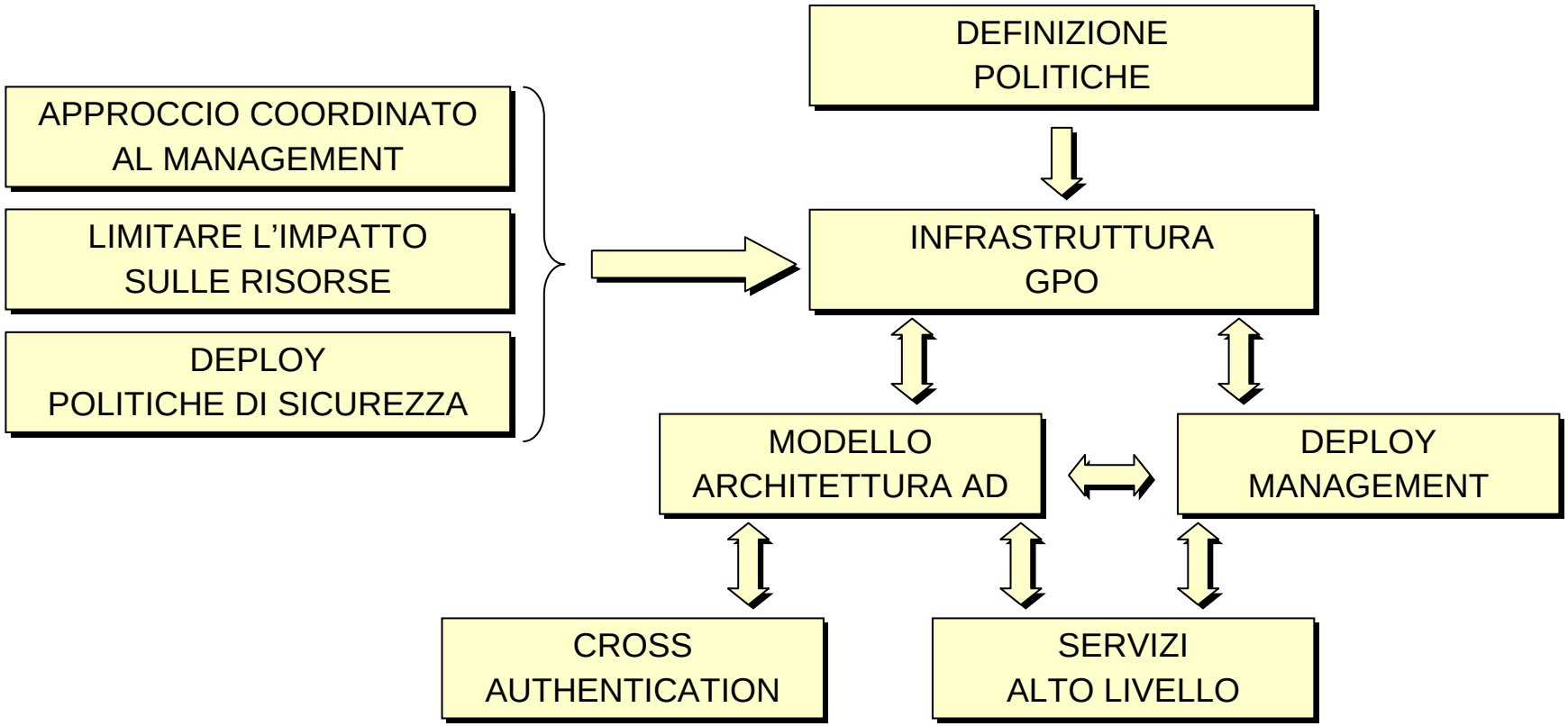


1. Infrastruttura di dominio windows locale carattarizzata da controllers e server membri.
2. Servizi di base quali l'accesso alle shares, le stampanti, il DFS.
3. I client nel dominio recepiscono automaticamente le politiche mediante meccanismi gerarchici. Gli utenti autenticati possono accedere alle risorse e ai servizi di base.
4. Moduli applicativi, agent e tools di alto livello che riesportano i servizi di base e le politiche rendendoli disponibili anche ai client fuori dominio.
5. Le relazioni di trusts consentono l'accesso alle risorse locali agli utenti che si autenticano nel *K5 Unix Realm* locale e in quelli remoti.
6. Pool di servizi distribuiti su area geografica per il *get asincrono* delle politiche globali, degli aggiornamenti e delle informazioni.

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

2 - Activities Planning

Priority



Implementazione di una infrastruttura di politiche e impostazioni mediante GPO

Studio e implementazione dei layers di correlazione con gli altri contesti

Tempi Previsti: ~ 2 – 3 mesi

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

2 - Activities Planning

Collaboration Strategies

Possono essere prese in considerazione le seguenti forme di collaborazione

- Progetti assegnati a piccoli gruppi per i quali sono ben definiti:
  - tempi di produzione
  - mezzi di divulgazione (pubblicazioni, report…)
- Workshop periodici indirizzati allo scambio di informazioni tra le infrastrutture

Per la divulgazione delle informazioni e l'interoperabilita' tra i gruppi sarebbe proficuo un *Repository Documentale Globale* per il quale siano definite:

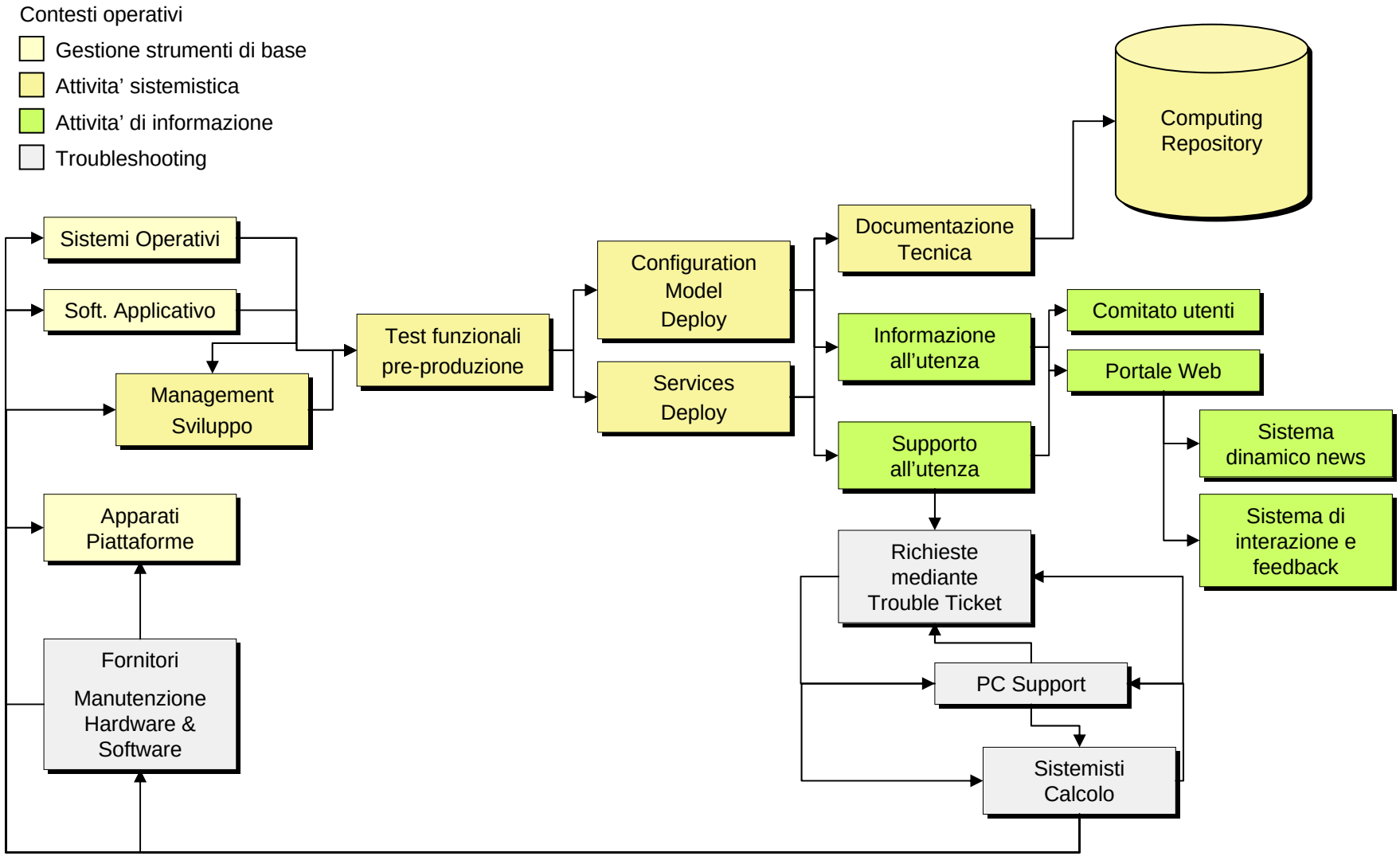
- opportune procedure di accesso/autorizzazione
- specifiche per la pubblicazione dei links nell'ambito delle pagine web di sezione

Tale repository potrebbe essere inquadrato nell'ambito del *Global Services Pool* utilizzato per il supporto alle infrastrutture locali.

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

3 - In Depth Subjects

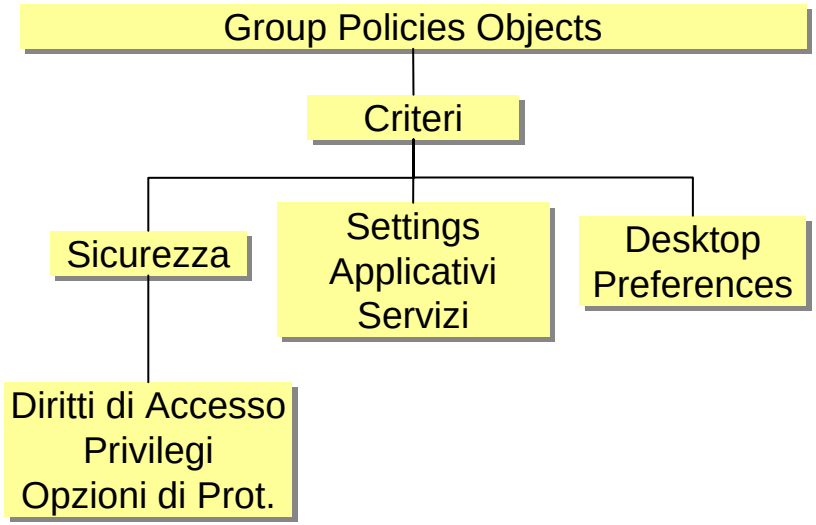
Management Related Activities



Typical Computing Management Scenario

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

3 - In Depth Subjects
GPO Overviews

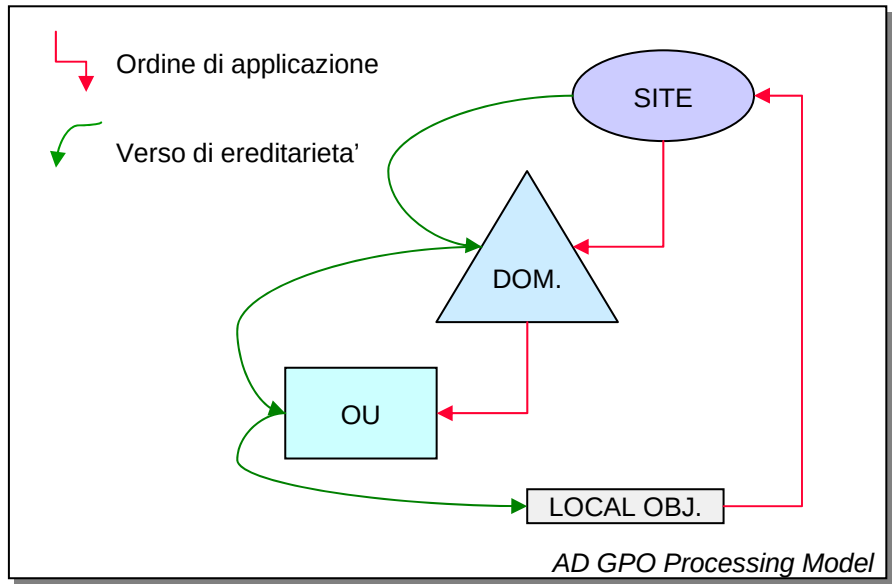


ASPETTI SUI CRITERI DI GRUPPO

- Puntano chiavi di *registro di configurazione*
- Interessano gli oggetti *Utente* e *Computer*
- Sono definiti a livello locale
- Sono definiti a livello di contenitori di AD
- Nel dominio sono trasmessi agli oggetti locali secondo meccanismi gerarchici e di ereditarieta'
- L'applicazione in ambito non locale e' discrezionale (DACL)

VANTAGGI PER I CLIENT NEL DOMINIO

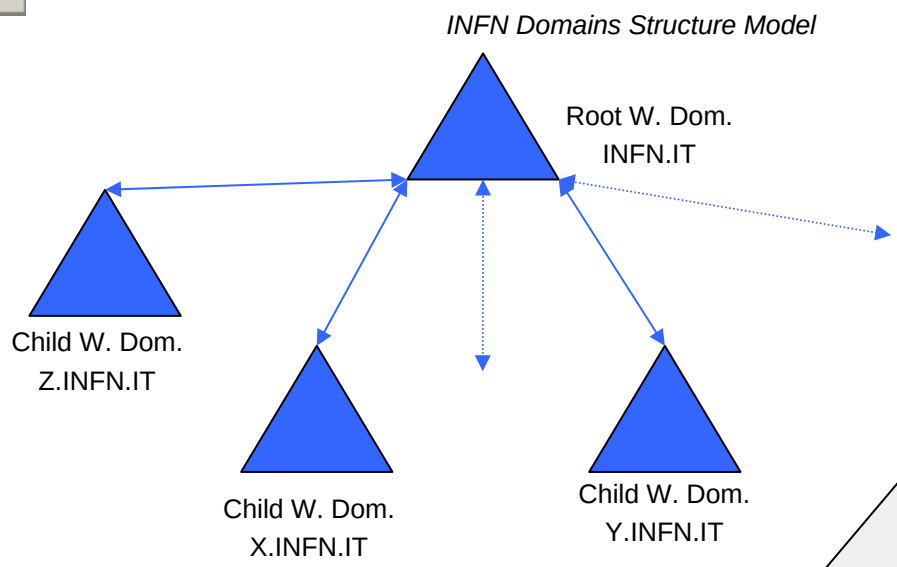
- Approccio centralizzato alle impostazioni
- Configurazione locale drasticamente ridotta
- Impatto minimo sulle risorse di gestione
- Management coordinato

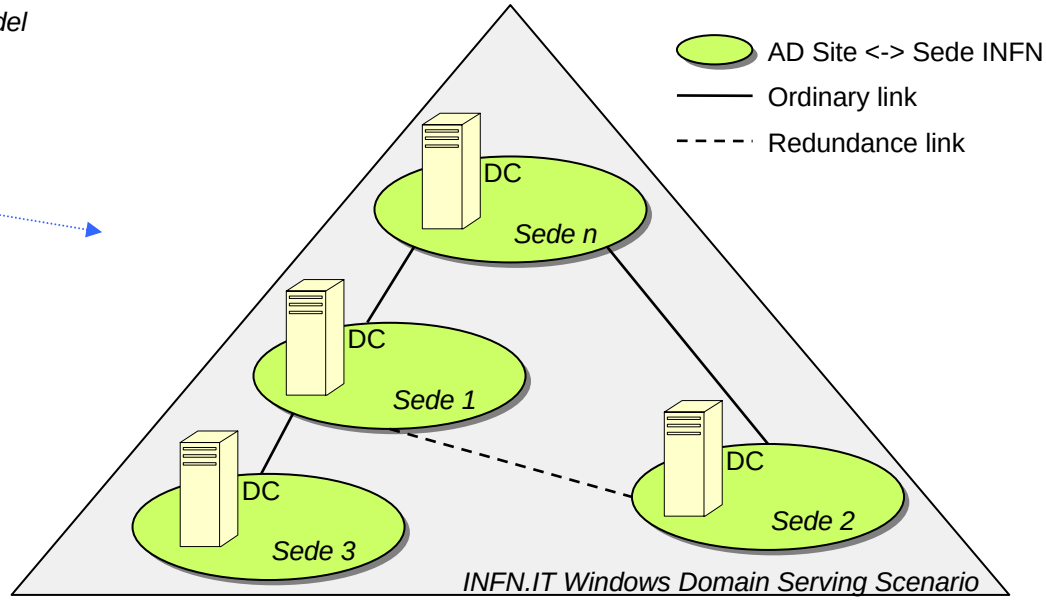


Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

3 - In Depth Subjects

Windows Domains Structure Tips





PROBLEMATICHE IMPLEMENTATIVE

- Integrazione di AD con uno spazio di nomi dns preesistente non servito da windows
- Scratch dei domini esistenti e re-implementazione come domini figli
- Ereditarieta' nei domini figli di memberships e permissions relativi ai gruppi globali predefiniti nel dominio INFN.IT
- Impatto del management centralizzato sull'individualita' delle sedi
- Attuazione di uno scenario geografico di serving e replica basato su AD Sites e distribuzione dei DC per il dominio root
- Necessita' di ridefinire nei domini figli le GPO comuni impostate *root layer*

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 SisInfo Management Team

LNF Computing Service