Programma di attività del gruppo Windows

N.Amanzi (LNF), S.Arezzini (PI), E.M.V.Fasanelli (LE), G.P.Siroli (BO)
CCR, Roma 14-15.3.2006

Introduzione

Il 16 febbraio 2006 si e' tenuta a Bologna una riunione del Gruppo Windows alla quale hanno partecipato 18 colleghi in rappresentanza di 12 Sezioni. Sulla base di alcune presentazioni, ha avuto luogo un'attiva discussione su vari aspetti relativi alla gestione delle infrastrutture Windows in ambito INFN.
Lo stato attuale di dette infrastrutture e' il risultato di un'evoluzione abbastanza eterogenea che si e' andata delineando negli ultimi anni per le varie realtà locali. In alcuni casi sono stati costruiti dei domini che raccolgono la grande maggioranza dei nodi presenti, permettendo in questo modo una gestione centralizzata sicuramente efficace, mentre in altri casi il numero di nodi gestiti in modo coordinato e' molto più limitato e ci si trova a dover amministrare molte macchine standalone con un evidente dispendio globale di energie. Questa realtà e' indubbiamente anche il frutto della struttura intrinsecamente autonoma delle varie Unità di cui e' costituito l'Ente, struttura che va tenuta in considerazione in qualsiasi progetto di lavoro comune.

L'Ente si trova attualmente a dover fronteggiare lo sviluppo di nuove attività di cui i servizi calcolo, già oberati di lavoro, devono farsi carico, contemporaneamente ad una limitazione nell'accrescimento delle risorse umane a disposizione. Si ritiene opportuna una razionalizzazione delle risorse, al fine di migliorarne la qualità, facendo leva sulla collaborazione tra sedi diverse nell'ambito di argomenti di interesse comune; lo scopo e' anche di limitare il dispendio globale di energie e sfruttare eventuali sinergie esistenti, ad esempio con i centri di calcolo delle

Università o i dipartimenti di Informatica. A questo proposito e' altresì importante migliorare la comunicazione tra le varie Sezioni sull'approccio e la soluzione a problematiche condivise.

Argomenti di interesse

In questa ottica il gruppo ha delineato una serie di aree tematiche sulle quali sarebbe opportuno sviluppare delle attività che siano proficue in un contesto globale; ciascuna di queste aree omogenee include una serie di argomenti specifici correlati, alcuni dei quali con valenza su più aree, sui quali potrebbero aggregarsi gruppi di lavoro distinti.
Segue la lista delle aree tematiche, con una sintetica descrizione del contesto, e gli argomenti specifici relativi a ciascuna area:

- **Procedure di deploy e management**

  L'importanza di definire procedure verificate e funzionanti cui fare riferimento in questo campo è particolarmente avvertita. Si tratta, infatti, di un settore caratterizzato da attività anche di routine che beneficiano particolarmente dell'adozione di sistemi standard e agevolmente implementabili. Pensiamo ad esempio alla gestione delle patch tramite WSUS. Oltre agli ovvi vantaggi derivanti dal meccanismo centralizzato per le installazioni, si ha anche un beneficio immediato legato alla sicurezza generale dell'ambiente di rete.
  In tal senso, nell'ottica di limitare l'impatto in termini di manpower e in generale di risorse, ai vari livelli, e' esigenza diffusa far riferimento ad un sistema di cloning. All'uopo dovrebbero essere valutate soluzioni applicative caratterizzate sia dal serving di immagini statiche (per macchine appartenenti a gruppi omogenei in termini hardware) sia dall'implementazione di *unattended procedures* relative all'installazione da scratch del S.O. Le procedure di clonazione e/o installazione non assistita consentirebbero, tra l'altro, il *deploy* di un sub-set minimale di impostazioni aderenti alle politiche di sezione e la definizione di opportuni meccanismi attraverso i quali i nodi, e soprattutto i client 'fuori dominio', possano recepire le GPO (*Group Policies Objects*), consentendo un approccio coordinato delle attività di

management/monitoring, nonché alla installazione e configurazione di applicativi comuni (quali server X11, ecc.).

- **Politiche di security**

Anche in questo settore è assai avvertita la necessità di implementare soluzioni agili e in grado di mettere al sicuro da gravi problemi. Pensiamo ad esempio alla problematica AntiVirus, solo parzialmente risolta tramite l'adozione di un unico software per l'ente. Il Servizio Calcolo di una sezione deve comunque definire le modalità di scaricamento del software in modo che tutti gli aventi diritto siano in grado di provvedere.
Pensiamo poi a quanto sarebbe importante una modalità di controllo per accertarsi dell'avvenuta installazione dell'antivirus e di patch di sicurezza al momento della registrazione in rete.
In un'ottica di distribuzione delle politiche di sicurezza ai client e' opportuno focalizzare l'attenzione sulle GPO.
Le GPO sono criteri di alto livello relativi ai diritti e privilegi di accesso, ai settings degli applicativi/servizi, alle preferences dell'environment utente. Poiché essi possono essere definiti localmente e globalmente, nell'ambito di un dominio windows, sarebbe proficuo indirizzare l'attività del gruppo verso lo studio delle relative meccaniche di propagazione nel contesto di scenari centralizzati e/o geografici. In tal senso l'obiettivo da perseguire dovrebbe essere contraddistinto dalla riduzione drastica degli interventi di configurazione da attuare sulle singole piattaforme, a beneficio del management centralizzato e del minimo impatto sul dispendio di risorse.
Queste tematiche vanno a collocarsi in una più generale problematica sulla sicurezza dell'ente, per la quale sarebbe opportuna una politica generale definita tramite linee guida cui ispirarsi al momento dell'implementazione delle specifiche politiche di sicurezza di ogni sede.

- **Accesso remoto**

Questo campo riguarda due filoni distinti: uno riferito alla condivisione di risorse, in particolare di storage, ed uno riferito invece ad un sistema di autenticazione-autorizzazione in grado di garantire accesso e permessi per precise attività ad una comunità di utenti quanto più vasta possibile.
I benefici derivanti da una programmazione delle attività in grado di garantire una certa esportabilità del proprio ambiente di lavoro sono innegabili, in particolare pensando alla mobility oggi cosi diffusa. Sono

altrettanto evidenti i benefici che tutte le attività di collaborazione tra sedi trarrebbero dall'adozione di sistemi distribuiti.

- **Collaborative tools: condivisione di informazioni e documentazione per utenti ed amministratori**

Anche in questo campo l'idea e' quella di condividere quanto più possibile gli strumenti di lavoro, nell'ottica di una attività fortemente collaborativa. L'analisi e lo studio di specifici strumenti e la proposta di adozione di determinati mezzi al posto di altri (proprio al fine di favorire l'interscambio), andrebbe nella direzione di facilitare le attività comuni e condivise. I mezzi sono molteplici e si passa da quelli più tradizionali a quelli più innovativi. Naturalmente nello specifico vanno attentamente analizzati gli aspetti di sicurezza correlati alle singole attività.

- **Attività trasversali di sviluppo, test, supporto**

Rientrano in questo campo tutta una serie di attività anche già evidenziate in precedenza ma qui raggruppate proprio con riferimento alla loro caratteristica di attività condivise, o prospetticamente condivisibili, in un'ottica di collaborazione più spinta. Esempio principe è la cross autenticazione che dovrebbe permettere di garantire, in ogni sede, accessi e risorse a personale di tutto l'Ente, tramite un'infrastruttura condivisa e opportunamente trustata.
Nell'ottica dell'individuazione degli strumenti di supporto agli studi di fattibilità ed alle conseguenti procedure di deploy, risulta particolarmente agevole poter riprodurre un modello funzionale e implementativo su piccola scala. In tal senso l'utilizzo di scenari virtuali offre indubbi vantaggi in termini di risorse necessarie, di impatto minimo sulle infrastrutture esistenti, di roll-back facilities, di mobilità e portabilità.

Priorità e strategie

L'attività del gruppo di lavoro dovrebbe perseguire lo scopo di coordinamento, ottimizzando le risorse disponibili, e delineando eventualmente alcune linee strategiche di sviluppo.
Fatta salva l'autonomia locale da mantenere nelle varie unità, andrebbero sviluppati degli strati sottili di funzionalità sulle infrastrutture già esistenti, come, ad esempio, l'attuazione di

procedure relative alla condivisione delle GPO e alla distribuzione dei settings di base.

Considerata la realtà disomogenea dei sistemi installati nelle varie sedi, per le attività globali dovrebbero essere, tra l'altro, obiettivi comuni:

- la portabilità delle implementazioni e delle procedure di management tra i distinti scenari di esercizio;
- la propagazione delle impostazioni, definite ai vari livelli, anche ai client fuori dominio (che costituiscono un numero di nodi molto elevato) al fine di uniformare e snellire le procedure di controllo e management;

Gli aspetti relativi alla gestione dei sistemi ed alla sicurezza (infrastrutture di dominio, autenticazione incrociata, definizione delle autorizzazioni e delle relative politiche) sono considerati prioritari rispetto agli altri.
In tal senso, per quanto riguarda per esempio l'accesso remoto alle risorse locali, stabilire sessioni di login interattivo verso il proprio client interno (tecnologia WTS) sarebbe preferibile rispetto all'estensione della LAN via VPN.
Dovendo quindi delineare un contesto iniziale verso il quale il Gruppo Windows dovrebbe indirizzare le proprie attività, si ritiene fondamentale focalizzare l'impegno sulle problematiche relative alla definizione e al serving delle GPO sia in ambito locale che globale. Cio' presuppone, tra l'altro, l'individuazione a priori delle politiche comuni, ai vari livelli, e l'implementazione di uno scenario di distribuzione ai client strettamente correlato con le altre aree di interesse, volte a delineare i presupposti per un'infrastruttura comune e coerente di AD e per un approccio coordinato al deploy/management, anche rivolto ai nodi fuori dominio quando possibile.
In un'ottica di interoperabilità dei contesti e delle risorse, si stima un impegno iniziale di 2-3 mesi per il rilascio di modello implementativo.

Forme di collaborazione

Possono essere prese in considerazione forme diverse di collaborazione in relazione alle diverse attività svolte: progetti per piccoli gruppi con tempistica, e deliverables ben definiti (pubblicazioni, report, raccomandazioni, best practice) oppure workshop periodici indirizzati allo scambio di informazioni nell'ambito della comunità degli amministratori delle infrastrutture.

Per la miglior divulgazione delle informazioni e l'interoperabilità dei gruppi coinvolti sarebbe preferibile fare riferimento ad un *repository documentale globale* per il quale andrebbero definite le opportune procedure inerenti l'accesso e l'eventuale pubblicazione dei links nell'ambito delle pagine web di Sezione.