ISTITUTO NAZIONALE DI FISICA NUCLEARE

Centro Nazionale CNAF

INFN/TC-00/003
28 Febbraio 2001

PROPOSTA DI IMPLEMENTAZIONE DI WINDOWS 2000 NELL'INFN

Gian Piero Siroli[1], Stefano Zani[2]
Andrea Baldini [3], Rosario Esposito[4], Enrico M.V. Fasanelli[5], Roberto Giacomelli[1], Gianluca Peco[1], Francesco Taurino[4], Alessandro Tirel[6]

[1] Istituto Nazionale di Fisica Nucleare Sezione di Bologna
[2] Istituto Nazionale di Fisica Nucleare C.N.A.F.
[3] Istituto Nazionale di Fisica Nucleare Sezione di Milano
[4] Istituto Nazionale di Fisica Nucleare Sezione di Napoli
[5] Istituto Nazionale di Fisica Nucleare Sezione di Lecce
[6] Istituto Nazionale di Fisica Nucleare Sezione di Trieste

Abstract

Questo documento si prefigge lo scopo di descrivere in modo molto conciso le caratteristiche principali del sistema operativo che possano essere di particolare interesse per l'INFN e delineare due possibili modelli di implementazione di Windows 2000. In estrema sintesi l'infrastruttura potrebbe essere organizzata in un unico dominio nazionale oppure in modo completamente separato in ogni singola Unità INFN; i due modelli sono messi a confronto in modo da poter analizzare vantaggi e svantaggi.

Published by ***SIS–Pubblicazioni***
Laboratori Nazionali di Frascati

Introduzione

Nel Maggio 2000 la Commissione Calcolo ha istituito un gruppo di lavoro su Windows 2000: scopo del gruppo e' quello di analizzare una possibile implementazione di tale sistema operativo in ambito INFN attraverso una fase iniziale di sperimentazione sul sistema e sulla gestione degli applicativi, oltre a coordinare l'attività dell'INFN in questo settore.
Da Maggio a Dicembre 2000 il gruppo di lavoro ha tenuto cinque riunioni risultate molto proficue sia dal punto di vista dello scambio di informazioni che per compiere attività di sperimentazione e test. Ad una di queste riunioni hanno partecipato anche tre rappresentanti tecnici di Microsoft, offertisi per una consulenza gratuita, in modo da permettere di approfondire ulteriormente alcuni punti giudicati particolarmente importanti. Durante questo periodo, a scopo di sperimentazione, e' stato installato e configurato un dominio temporaneo (w2k.infn.it) su scala geografica con nodi in cinque differenti siti INFN (Bologna, CNAF, Milano, Lecce, Trieste).
Da un recente sondaggio condotto (Ottobre 2000), risulta che attualmente circa il 30% dei sistemi installati nell'INFN utilizzano una qualche versione del sistema operativo Windows/9x e circa un altro 15% aggiuntivo Windows/NT; Windows 2000, attualmente installato su un numero di computer dell'Ente stimabile tra le 100 e le 200 unita', rappresenterebbe la naturale evoluzione dei sistemi Windows/NT e potrebbe sostituire buona parte dei sistemi Windows/9x che diverranno obsoleti, sia dal punto di vista hardware che software, nel prossimo futuro. Anche i maggiori laboratori di Fisica delle Alte Energie si stanno dotando di una infrastruttura basata su questo sistema operativo dopo la attuale fase di apprendimento e sperimentazione.
Questo documento si prefigge lo scopo di descrivere in modo molto conciso le caratteristiche principali del sistema operativo che possano essere di particolare interesse per l'INFN e delineare due possibili modelli di implementazione di Windows 2000. In estrema sintesi l'infrastruttura potrebbe essere organizzata in un unico dominio nazionale oppure in modo completamente separato in ogni singola Unità INFN; i due modelli sono messi a confronto in modo da poter analizzare vantaggi e svantaggi.

Descrizione del sistema operativo

Windows 2000 rappresenta l'evoluzione di Windows/NT e ne supera alcune mancanze soprattutto per quanto riguarda la gestione in ambienti di organizzazioni estese. Il suo design permette di assegnare e/o delegare la gestione di funzioni specifiche o estese di amministrazione dell'infrastruttura attraverso l'uso di strutture gerarchiche (ad esempio a livello di Unità Organizzativa o OU). E' possibile controllare con grande flessibilità la granularità dell'architettura (sottodomini, OU) in modo da poter meglio coprire le necessità specifiche. L'Active Directory (AD) e' lo strumento principale di Windows 2000 per gestire tutti gli oggetti esistenti in un dominio (ad es. utenti o computer) in una struttura gerarchica e replicata.

Caratteristiche architetturali

I due componenti principali dell'Active Directory sono la sua struttura logica e quella fisica, che riguardano rispettivamente l'organizzazione e la comunicazione tra gli oggetti. Una terza componente fondamentale e` lo *schema* che definisce le classi di oggetti e gli attributi.

Dominio

Un dominio e` un insieme di computer e risorse di rete delimitate da un comune spazio logico di sicurezza. L'amministratore di un dominio ha i permessi di amministrazione solo all'interno del dominio stesso, a meno che non sia stato esplicitamente autorizzato ad amministrare altri domini. Ogni dominio ha le proprie *policies* di sicurezza e può avere relazioni di "trust" con altri domini. Lo schema e` memorizzato nell'Active Directory.
Ogni dominio deve avere almeno un Domain Controller. I domain controller sono computer con sistema operativo Windows 2000 Server che contengono una copia completa della directory. AD utilizza la replicazione multi-master per scambiare informazioni tra i domini.
Si possono avere domini misti e nativi. I domini misti possono avere domain controller con sistema operativo Windows 2000 o NT. Nei domini nativi tutti i domain controller hanno sistema operativo Windows 2000. Alcune funzionalità di AD richiedono che il dominio sia nativo.

Organizational Unit

Una Organizational Unit (OU) e` un contenitore logico di oggetti (massimo 10 milioni) usato per organizzare gli oggetti all'interno di un dominio. In una OU si possono raggruppare oggetti in una logica gerarchica. Per esempio si può creare una OU per gli utenti ed una per i computer e delegare l'amministrazione degli account degli utenti alla prima OU e quella dei computer alla seconda OU. Si possono nidificare OU all'interno di altre OU. La gerarchia delle OU all'interno di un dominio e` indipendente da quella degli altri domini (ogni dominio può implementare la propria gerarchie di OU). Si possono delegare funzioni amministrative sugli oggetti di una OU assegnando specifici permessi a uno o più utenti o gruppi. Si può assegnare un controllo amministrativo completo o limitato (gestione stampanti, utenti, ...).

Albero

Il primo dominio Windows 2000 che viene creato e` il root domain della foresta, e contiene la configurazione e lo schema della foresta; i domini aggiuntivi formano la struttura ad albero o a foresta.
Un albero e` un ordinamento gerarchico di domini Windows 2000 che hanno namespace comuni e contigui, uno schema comune e una relazione di sicurezza. Quando si aggiunge un dominio ad un albero preesistente, il nuovo dominio e` un "figlio" (*child* domain) del dominio "genitore" (parent domain). Il nome del child domain viene aggiunto al nome del parent domain in modo da formare il suo nome DNS. Ad esempio se il parent domain si chiama w2k.infn.it e si vogliono aggiungere i child domain bo e mi (Sezioni di Bologna e Milano), questi si chiameranno bo.w2k.infn.it e mi.w2k.infn.it in modo da formare un namespace contiguo, la cui root e` w2k.infn.it.

Foresta

Una foresta e` un gruppo di alberi che non hanno namespace contigui. Gli alberi di una foresta condividono una comune configurazione, schema e Global Catalog. Il nome alla foresta viene dato dal root domain.

Active Directory

L'Active Directory e` il directory service in una rete Windows 2000. Una directory service e` un servizio di rete che memorizza le informazioni riguardanti le risorse di rete e le rende accessibili alle applicazioni ed agli utenti e gruppi autorizzati. Ogni cosa in Active Directory viene considerata un oggetto (utenti, server, workstation, stampanti, documenti e devices).

Sito

Un sito e` l'insieme di una o più sottoreti IP connesse tra di loro ad alta velocità ed in modo affidabile. Si può dire che la velocità di connessione minima per reti "piccole" e` di 128 kbps, mentre per reti "grandi" e` di 3 Mbps. Una sottorete IP non può appartenere a più siti. I siti sono creati allo scopo di ottimizzare il traffico di replica e per permettere agli utenti di collegarsi ad un domain controller con connessioni veloci e sicure.

Funzionalità e servizi del sistema operativo

DHCP

Il Dynamic Host Configuration Protocol (DHCP) e` parte integrante del sistema operativo. La funzione principale svolta e` quella di fornire all'amministratore del sistema gli strumenti per una gestione centralizzata dell'indirizzamento IP. Questo protocollo non e` nuovo, la sua introduzione risale ormai ad alcuni anni fa (RFC 1541), tuttavia l'integrazione con il DNS e l'Active Directory concorre alla semplificazione delle operazioni di configurazione dei client.
Di seguito sono riportate alcune delle principali caratteristiche del protocollo:

- Fornisce ai client in modo automatico l'indirizzo IP, l'hostname, il domain name, ed altri parametri come gli indirizzi dei name server.
- Quando assegna un indirizzo IP ad una macchina, il DHCP e` in grado, tramite l'integrazione con il DNS dinamico, di registrare anche il nome a dominio permettendo di ridurre i compiti demandati all'amministratore del sistema.
- Solo i DHCP server autorizzati tramite l'Active Directory possono fornire gli indirizzi IP ai client; questo accorgimento e` necessario al fine di scongiurare pericolose sovrapposizioni di ruoli.
- Funzioni di statistica e monitor delle risorse assegnate.

RIS

L'installazione di un nuovo sistema operativo generalmente consiste in una fase di pianificazione ed una successiva fase di attuazione. Questo processo può durare molto tempo ed impiegare molte persone. Infatti si rende necessario spostarsi fisicamente su ogni singolo computer. Tutte queste operazioni comportano un incremento del TCO (Total Cost of Ownership). Per semplificare ed accelerare soprattutto la fase di attuazione sono stati creati i Remote Installation Services che sono:

- Boot Information Negotiation Layer (BINL)
- Trivial File Transfer Protocol (TFTP)
- Single Instance Storage Groveler (SIS)

Al fine di ottenere il massimo delle funzionalità di questi servizi e` importante che il computer client sia dotato di una scheda di rete di recente fabbricazione che supporti il funzionalità PXE (Pre-Boot Execution Enviroment). In alternativa e` possibile usare un dischetto di boot per simulare tale funzionalità.
Dopo aver configurato il RIS server ed i servizi di cui abbisogna (DNS, Active Directory e DHCP), si passa all'installazione del sistema operativo sui client. Nella forma più semplice la procedura e` la seguente:

- Boot del client via rete tramite l'ambiente PXE, richiesta tramite protocollo DHCP di un indirizzo IP
- Il DHCP server assegna il indirizzo IP
- Richiesta del client di accedere al servizio BINL
- Se il client e` autorizzato viene fornito dal servizio BINL il nome del programma di bootstrap via rete da eseguire.
- Il client tramite il protocollo TFTP fa il download del programma e lo esegue
- Inizia l'installazione del sistema operativo.

L'amministratore può definire delle configurazioni ad hoc in base a molti parametri oppure creare una procedura a menu` che indirizzi l'utente verso una corretta installazione. Deve risultare chiaro che il livello di libertà nell'installazione del sistema operativo e` sotto il completo controllo dell'amministratore del sistema.

RIPrep

Nel caso in cui si debbano installare un numero consistente di client dalle medesime caratteristiche hardware (Hardware Abstraction Level) si può utilizzare il programma chiamato Remote Installation Preparation. In sostanza si tratta di installare su uno dei computer il sistema operativo e tutti gli applicativi, quindi "fotografarlo" con RIPrep e copiare sul server RIS questa immagine, la quale verrà replicata sugli altri client. Sebbene questa tecnica possa risultare utile nel velocizzare le operazioni di installazione del software in realtà ne compromette la gestibilità come si vedrà nel seguente paragrafo. Tale tecnica può comunque trovare un utile impiego nella preparazione di computing room in caso di workshop, corsi di istruzione ed altre attività similari che non richiedono aggiornamenti del software installato.

Deployment di applicazioni

Uno dei principali problemi del personale che si occupa dei PC e` la gestione degli applicativi che può essere suddivisa in tre fasi:

- Installazione
- Aggiornamento
- Rimozione

Con l'introduzione di Windows 2000 questo problema e` stato sviluppato al fine di diminuire in modo notevole l'impegno del personale. Sono state infatti introdotte delle tecnologie chiamate Software Installation and Maintenance che in collaborazione con altri servizi quali Active Directory, RIS e le Group Policy (GPO) consentono una gestione centralizzata delle fasi di ogni singolo applicativo. Gli applicativi che meglio si adattano a questo tipo di utilizzo sono quelli che impiegano il Windows Installer, quindi le ultime versioni dei prodotti Microsoft e quelli certificati Windows 2000. E` possibile, tuttavia, tramite un operazione chiamata di re-packaging utilizzare anche i programmi più datati che pero` non potranno beneficiare di tutte le facility. I benefici offerti da questa nuova tecnologia sono:

- Installazioni personalizzate: alcune delle funzioni non vengono installate sul disco locale (ad es. clip-art, librerie,...), ma rimangono comunque accessibili da programma e, quando richieste, vengono installate in modo trasparente all'utente.
- Consistenza dell'installazione: nel caso in cui un file appartenente all'applicazione venga corrotto o cancellato inavvertitamente, tale file viene immediatamente sostituito senza richiedere alcun intervento da parte dell'utente.

- Rimozione totale: quando l'applicazione viene rimossa vengono tolti tutti i file mantenendo pero` quelli in comune con altre applicazioni ancora attive.

La distribuzione delle applicazioni avviene esclusivamente via rete, non c'e' alcun bisogno di effettuare copie dei media (CD-ROM o dischetti). Viene creato sul server un distribution point nel quale vengono copiati i vari pacchetti.
Come detto in precedenza questo servizio si basa sulle Group Policy che possiamo definire come un insieme di regole che definiscono gli attributi di un computer o di un utente. Quindi una volta creato il pacchetto nel distribution point, si possono utilizzare le GPO per installare l'applicazione sul computer dell'utente oppure aggiornare l'applicazione tramite patches o Service Pack oppure per rimuovere l'applicazione. Queste operazioni vengono effettuate automaticamente senza che vi sia bisogno di accedere ai vari computer. Le GPO permettono inoltre di assegnare i pacchetti software ai computer o agli utenti; nel primo caso il software viene installato automaticamente all'accensione del computer mentre nel secondo vengono predisposti i riferimenti all'applicazione che verrà installata solo se richiamata dall'utente.
Un ulteriore modalità nella gestione del software e` quella della pubblicazione, ovvero viene messo a disposizione il pacchetto software e sarà l'utente a decidere se installarlo. Quest'ultima modalità pero` non controlla la consistenza dell'installazione quindi in caso di malfunzionamenti sarà l'utente a dover reinstallare l'applicazione.

Nota: I test effettuati hanno dato risultati molto positivi e si confida che una maggior conoscenza del sistema possa migliorarli ulteriormente

RAS

Windows2000 Server fornisce numerosi miglioramenti al servizio di accesso remoto rispetto alla precedente implementazione su Windows/NT 4.0. Questi miglioramenti possono essere organizzati in tre categorie:

- Migliore integrazione dei client
- Servizi e tools di management più efficienti
- Piattaforma client-server maggiormente integrata

Il RAS di Windows 2000 fornisce una serie completa di servizi di autenticazione e di protocolli che semplificano la connessione dei client con sistemi operativi Microsoft, Apple e Unix. Bisogna tenere presente che soltanto i client Windows2000 Professional possono usufruire pienamente di tutte le caratteristiche offerte dal nuovo RAS, come l'utilizzo di particolari tecniche di autenticazione (es. smart card), il Quality of Service (QoS) e le reti private virtuali (VPN). Sui client non-Windows2000 è quasi sempre necessario installare pacchetti aggiuntivi.
Windows2000 Server migliora lo stack TCP/IP di NT 4, supporta un maggior numero di dispositivi di comunicazione e implementa molti servizi innovativi, tra cui:

- Supporto integrato per i DSP per la riduzione del carico durante alcune operazioni (es. criptazione delle trasmissioni)
- Network-traffic data compression
- Aggregazione multipla di canali a bassa capacità di comunicazione
- Servizi di clustering e load balancing
- Supporto per i principali protocolli di Quality of Service (QoS)

I tool di management del RAS sono più semplici da usare e sono perfettamente integrati con i sistemi di directory service e di assegnazione di user-rights di Windows2000.
Windows 2000 Server semplifica il setup del RAS attraverso l'utilizzo di wizard e di file di help abbastanza dettagliati. Una volta configurato il RAS, è possibile creare gli account per i client e specificare i permessi di dial-up usando il servizio di Active Directory.
Tra i numerosi protocolli di autenticazione, il RAS di Windows2000 supporta RADIUS (Remote Access Dial-Up User Service). Uno dei vantaggi nell'utilizzo di RADIUS in combinazione con Active Directory è la possibilità di stabilire delle policy di accesso remoto basate su:

- Gruppo dell'utente
- Servizio richiesto
- Protocollo usato
- Numero di telefono composto dall'utente
- Numero di telefono del chiamante
- Porta fisica utilizzata
- Giorno e ora
- Indirizzo IP di origine

Inoltre la configurazione dei client e' stata semplificata dal Connection Manager Administration Kit, che permette di creare pacchetti per la connessione automatica in base a specifiche richieste, come la presenza o meno di una VPN. Il QoS garantisce la priorità di determinati servizi rispetto ad altri su una rete.
Windows 2000 supporta:

- Resorce Reservation Protocol (RSVP)
- Subnet Bandwidth Manager/Designated Subnet Bandwidth Manager (SBM/DSBM), una estensione di RSVP per reti condivise
- Common Open Protocol Services (COPS)

Il supporto per questi standard permette alle reti basate su Windows 2000 di gestire in maniera più efficiente il traffico di rete, consentendo di assegnare più banda a servizi ritenuti più importanti.

VPN

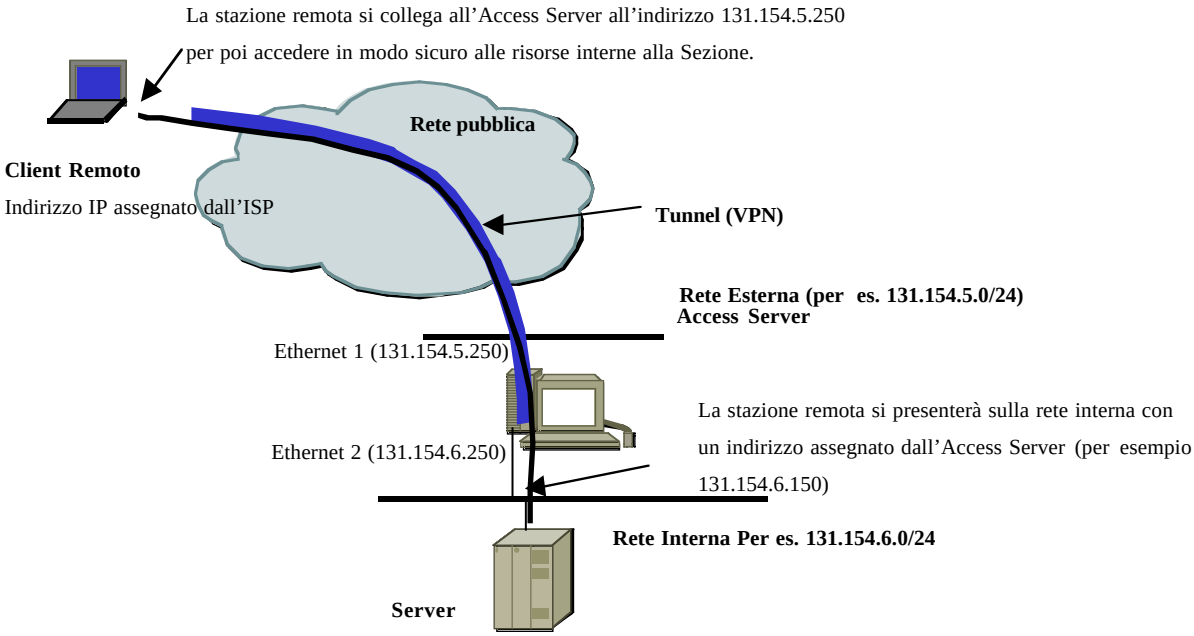
Una Virtual Private Network è una connessione privata (sicura) tra due macchine (o due reti) che trasporta dati privati utilizzando come supporto una rete pubblica (insicura), tramite l'incapsulamento e la codifica del contenuto informativo (encryption). La connessione logica realizza, attraverso un "tunnel" sul protocollo di trasporto e la associata cifratura del contenuto, un canale virtuale privato attraverso la rete. I protocolli utilizzati sono:

- Point to Point Tunnelling Protocol con Microsoft Point to Point Encryption come protocollo di cifratura (RSA RC4 con chiave a 40 o 128 bit)
- Protocolli a chiavi asimmetriche IPSec e L2PT (sviluppato da Cisco in draft alla IETF) . - Standard

Windows 2000 rende disponibili sia VPN host-to-host che, tramite un Tunnel Server, host-to-rete e rete-to-rete , realizzando una piattaforma di instradamento sicuro tra la rete pubblica e quella privata per i client remoti e VPN tra sottoreti completamente trasparenti ai client. L'integrazione del VPN con il Remote Access and Routing Server garantisce anche la possibilità

di realizzare sottoreti per uso privato indipendentemente dalla posizione geografica e l'utilizzo di spazi di indirizzamento privati nel collegamento virtuale (NAT).

Segue un esempio di configurazione che potrebbe essere applicato alla realtà dell'INFN.



Nell'esempio sopra indicato oltre a realizzare una connessione "Sicura" , si ottiene anche di "presentarsi" con un indirizzo interno alla rete della sezione.

Distributed File System (A Logical View of Physical Storage)

Il prodotto Dfs di Microsoft (da non confondere con il DFS/DCE dell'OSF) permette di raggruppare file e directory sparsi su differenti computer in un singolo name space.

Con questo prodotto, che è disponibile nella versione server sia su piattaforma Windows2000 che Windows NT (anche se nella versione presente su quest'ultimo mancano tutte le funzionalità collegate all'integrazione con Active Directory) è possibile:

- Definire una singola struttura logica, organizzata gerarchicamente, dei vari file server e share presenti all'interno di una organizzazione, in modo da rendere trasparente all'utente finale la locazione fisica di un sotto albero; tutto ciò mantenendo inalterata, quindi distribuita, la gestione amministrativa dei vari file server e share.
- Definire in tale struttura insiemi di file e/o directory read-only da rendere altamente disponibili (attraverso definizione di repliche che vengono sincronizzate in modo automatico)
- Provvedere funzionalità di load balancing tra file server per la distribuzione di share (sempre per mezzo della definizione di repliche) frequentemente acceduti.

La struttura logica dello spazio Dfs con i puntatori ai vari file servers, può essere pubblicata in Active Directory e quindi essere disponibile (via global catalog) a tutti i sistemi che hanno accesso all'Active Directory (in particolare ai Domain Controllers); è quindi possibile definire strutture Dfs in cui l'intero albero sia visibile anche in presenza di network breakdown.

Altra caratteristica del Dfs è il fatto che non vengono assolutamente gestiti i lock, e quindi accessi multipli a file presenti in Dfs NON vengono assolutamente gestiti a livello di Dfs. Ciononostante, rimane un utile strumento per la distribuzione (con caratteristiche di elevata disponibilità, fault-tolerance e load balancing) di sotto alberi read-only, oltre che per la definizione e la gestione di un albero logico di file shares che rende l'accesso ai file e directory indipendente dalla loro locazione fisica. Ciò può risultare particolarmente utile nel caso di home folder degli utenti che non necessitano obbligatoriamente di meccanismi di locking.

Encrypted File System

Windows 2000 con l'implementazione dell'encrypted file system fornisce uno strumento integrato nel sistema operativo per aumentare la riservatezza dei propri file.
Ogni utente può crittografare i propri file avendo la garanzia che solo lui ed eventualmente il "Recovery Agent" (utente designato alla gestione della encryption) avrà la possibilità di accedere ai dati .
L'accesso da parte del proprietario ai file crittografati è trasparente, mentre un eventuale intruso si vedrebbe negato l'accesso.
Un aspetto interessante è che il "Recovery Agent" del file system criptato può non essere l'amministratore di dominio ma un altro utente designato allo scopo, ad esempio il direttore di Sezione.
Ogni file ha una unica "*file encryption key*" che verrà successivamente utilizzata per la "decryption".
La *file encryption key* è criptata a sua volta ed è protetta dalla chiave pubblica dell'utente.
La *file encryption key* è anche protetta dalla chiave pubblica del *Recovery Agent.*

Terminal Services

Windows Terminal Server può essere utilizzato per due scopi distinti:
Gestione remota:
Windows2000 Server, tramite la funzionalità di Terminal Server, permette agli utenti con privilegi di Administrator di gestire remotamente la macchina da una qualsiasi macchina Windows purché abbia il WTS client installato. Sono consentite al massimo due connessioni contemporanee di questo tipo.
Server Applicativo:
Tutte le macchine con sistemi operativi Microsoft (Windows 3.11/95/98/NT/2000) possono eseguire programmi residenti sul server Windows 2000 (previa installazione del WTS client), che provvede ad esportare un desktop verso la macchina client.
La macchina client si occupa solamente della visualizzazione del desktop e non dell'esecuzione dei programmi. L'occupazione della cpu del client è minima.
La connessione è crittografata, avviene tramite TCP/IP e usa circa 23Kbit/secondo (uso di Office).
L'eventuale acquisto dell'add-on "Metaframe" di Citrix estende l'uso del Terminal Server anche a client Unix/XTerminal/Mac.

Clustering

Per cluster si intende un gruppo di computer che suddividono un determinato workload e permettono un funzionalità di "redundant faul tolerance". I "Cluster Services" di Windows 2000 sono disponibili solo nelle versioni Advanced Server e Data Center Server. Se un membro del cluster cessa l'attività, i suoi processi sono trasferiti ad un altro membro che ne assume il workload, con un tipico meccanismo di failover (e failback quando il nodo ritorna attivo). I cluster possono eseguire funzioni generiche o specifiche ma sono tipicamente utilizzati per funzioni di server di file, server di stampa o di applicativi e Web server che necessitano di elevata disponibilità; è possibile configurare dei server virtuali che agiscono come un unico nodo (un determinato nome ed indirizzo IP) con capacità di failover che rendono le risorse disponibili anche in caso di system failure.

Applicativi multimediali

Nella distribuzione di Windows 2000 viene fornito “di default” anche Netmeeting che permette di effettuare videoconferenze punto-punto.

In Windows 2000 Server è disponibile il Windows Media Sever che permette di distribuire filmati (Audio-Video) in formato Advanced Stream Format (ASF).

Il tipo di streaming può avvenire “in diretta”, ossia il feed viene prodotto in tempo reale utilizzando il Windows Media Encoder e “Servito” dal Windows Media Server, oppure si può accedere a filmati già salvati in formato ASF sul server (Video on Demand).

Si possono visualizzare i filmati utilizzando il WindowsMediaPlayer oppure semplicemente da un browser utilizzando Activex.

Il tipo di trasmissione del feed può essere *unicast* o *multicast* in base alla infrastruttura di rete che si ha a disposizione.

Il server fornisce varie possibilità di configurazione, sia a livello di banda massima utilizzata per ogni feed che a livello di accounting e controllo di accesso alle informazioni.

Questo Servizio può rappresentare una alternativa al server della RealNetworks attualmente in produzione.

Interoperabilità con Unix

Windows e UNIX/LINUX non devono necessariamente essere visti in alternativa uno all'altro ed in particolare sarebbe utile individuare le possibilità di interoperabilità ed integrazione dei due sistemi, anche allo scopo di evitare una estesa polarizzazione delle risorse di calcolo su uno dei due sistemi ed utilizzare al meglio entrambi nelle loro competenze specifiche. In particolare un applicativo X-server (quale ad esempio Exceed) su piattaforma Windows permette l'accesso contemporaneo ai due mondi, poiché permette ad un desktop Windows un accesso attraverso il protocollo X ad un nodo UNIX qualsivoglia, includendo anche un client NFS. VMware, un applicativo che permette di avere una macchina virtuale Windows dentro un sistema LINUX (o viceversa) può, in determinati casi, assolvere questa doppia funzionalità. Per quanto riguarda i file system, SAMBA permette una condivisione di risorse, quali home directory di utenti e stampanti, tra UNIX e Windows, cosa in parte possibile anche attraverso il client AFS per Windows quando sarà disponibile.

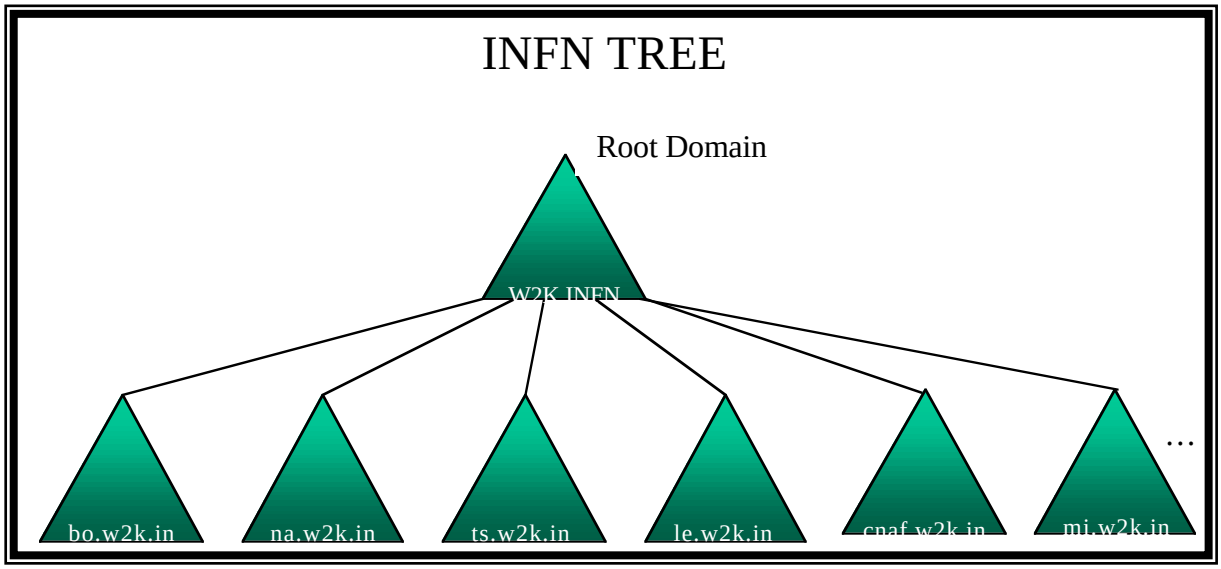
Anche alcuni applicativi usati nell'analisi dati sono disponibili su Windows, quali PAW, ROOT, CONDOR (anche se in modo ancora limitato senza checkpointing). Molto probabilmente, almeno nel prossimo futuro, il workload di calcolo intenso sarà eseguito su macchine UNIX ma in molti casi l'interfaccia utente potrebbe risiedere su desktop Windows.

Inoltre si segnala l’esistenza si due pacchetti orientati alla integrazione dei due mondi, Services For UNIX (Perl, meccanismi di sincronizzazione di password, client e server NFS) ed Interix (ambiente POSIX).

Descrizione dei possibili scenari architetturali e relative infrastrutture: Dominio unico nazionale, Domini indipendenti

Dominio Unico Nazionale

Nel caso si voglia realizzare una installazione di Windows2000 a livello nazionale, la struttura che sembra la più indicata per l'INFN, è l'albero, che permetterebbe di mantenere una struttura gerarchica come quella del DNS.



Per ogni sito può essere creato un sottodominio, configurando almeno un Domain Controller, oppure una semplice OU a seconda delle necessità richieste o del livello di autonomia desiderato.

Per la realizzazione di una struttura gerarchica di questo tipo è necessario che vi sia un forte coordinamento fra le sezioni soprattutto in fase di "startup". In fase di realizzazione, occorre coordinarsi anche come tempistica. Il dominio di livello superiore deve essere creato per primo e solo successivamente tutti i domini di livello inferiore.

La struttura di Windows 2000, come indicato nel paragrafo riguardante le caratteristiche infrastrutturali, si basa su Active Directory. La parte essenziale (contenente la descrizione di tutte le risorse) di tutto l'AD, viene mantenuta in un database chiamato Global Catalog (GC) e risiede su di un server (generalmente il "Root Domain") che diviene quindi una macchina molto "delicata" il cui crash potrebbe provocare gravi problemi rendendo impossibile l'accesso alle risorse sulla rete geografica.
E' quindi consigliato replicare il GC su di un domain controller per ogni "Site" connesso.

Per l'installazione ed il corretto funzionamento di Active Directory, occorre chi i DNS server supportino alcune "features" specifiche come la gestione del record SRV e l'aggiornamento dinamico.
Le ultime versioni del BIND supportano queste funzionalità ed in linea di principio si potrebbero utilizzare anche come DNS per l'albero Windows2000.

Dai primi test effettuati, si ritiene comunque opportuno mantenere separata la struttura di DNS generale da quella di Windows2000 in modo da evitare che eventuali aggiornamenti dinamici vadano eventualmente a danneggiare il contenuto delle tabelle di risoluzione utilizzate per tutti gli altri servizi di rete dell'INFN.
In questo modo si può demandare ai Domain Server Windows2000 di sezione il compito di gestire il DNS utilizzando quello nativo Microsoft.

La proposta che ci sembra più opportuna è quella di utilizzare come per la struttura di test, un domino nativo dedicato w2k.infn.it al quale aggiungere i vari sottodomini (ad es. bo.w2k.infn.it, ct.w2k.infn.it, ecc.) Questa soluzione ci permette di gestire la struttura DNS con i server Microsoft consentendo anche l'update dinamico, ma ci impone di gestire il reverse lookup sui DNS server generali (Normalmente BIND su Unix).

Per una miglior gestione del sistema sarebbe utile concordare una "politica di naming" a livello globale almeno per i domain controller dei vari sottodomini, in modo che siano documentativi e non duplicati.

La configurazione di eventuali firewall tra i diversi siti INFN deve tenere in considerazione il fatto che il sistema operativo utilizza un certo numero di porte TCP/IP descritte in appendice B.

Valutazione delle risorse necessarie alla gestione

Per realizzare il Root Domain e' necessario utilizzare 2 Server (uno in scorta all'altro) approssimativamente con questa configurazione:
PIII 800 (o superiore), 1 GB di RAM ECC, Controller RAID (Hardware) con almeno 36GB di HD SCSI. Occorre prevedere un regolare e robusto sistema di back-up.

Eventuale acquisto di tool software

A seconda del numero di nodi che si intende supportare in dominio potrebbe essere utile dotarsi di uno strumento di gestione più evoluto che permette maggiori funzionalità rispetto ai meccanismi di Group Policy.
Systems Management Server version 2.0 (SMS, molto più funzionale rispetto alla versione 1.0 considerata molto limitata) è un tool che si compone di una parte server e un pacchetto client.

- Estrae dalla macchina client e inserisce in un database centrale informazioni sul hardware e sul software installati.
- Esegue un check di compatibilità con l'anno 2000 del software e del hardware installato (può eseguire check di compatibilità con parametri arbitrari)
- Tiene traccia dell'uso delle applicazioni (software metering)
- Identifica il sistema operativo e crea una mappa della topologia della rete.
- Genera reports

Il pacchetto SMS server richiede l'installazione di Microsoft SQL server; si consiglia un server dedicato.
Supporto limitato per i terminal server clients (l'installazione del client non può essere eseguita da remoto ma solo localmente; nessun software metering).
Con la prossima release (l'attuale è la 2.0) è prevista l'integrazione del pacchetto con Active Directory.
Per funzionalità differenti possono essere a disponibili altri tool non Microsoft.

Definizione di un gruppo di gestione del root domain

Per la gestione del root Domain nonché per il supporto alla struttura nazionale dovrà essere istituito un gruppo di persone che è stato indicativamente stimato in:

- 4-5 persone al 50% del loro tempo per 3-4 mesi per il BOOT della Struttura
- 3-5 persone equivalenti a 1.5FTE per la gestione dell'albero ed il supporto sulla struttura

Si potrà avere una stima più precisa di questi valori una volta terminata la fase progettuale dell'AD. Il gruppo si dovrà occupare anche della raccolta delle informazioni utili all'installazione di pacchetti (file MSI).

È necessario individuare all'interno di ogni sezione il responsabile per il sottodominio che oltre ad occuparsi della gestione, sarà il punto di contatto per pianificare eventuali operazioni coordinate sulla struttura nazionale.

Descrizione della struttura necessaria alla configurazione di un dominio indipendente per sezione

Questo paragrafo descrive l'architettura nel caso in cui si scelga di non costruire un albero nazionale ma si decida di lasciare la gestione di Windows2000 individualmente alle varie Sezioni in modo completamente scoordinato.
Anche considerando la costruzione di un Dominio Windows2000 "semplice" e non facente parte di un albero, è necessario avere almeno due Domain Controller per dominio (non esiste più il Backup Domain Controller come per Windows NT).
La configurazione dei server sarà legata alla dimensione del dominio da gestire e alle funzionalità che si vorranno implementare.
La gestione del DNS in questo caso sarà completamente a carico della sezione ed anche le soluzioni adottate potranno essere le più diverse in completa autonomia (utilizzo di Domini nascosti ed accesso alla rete geografica tramite NAT o Proxy, utilizzo dei BIND su UNIX, ecc..).

Valutazione delle risorse necessarie alla gestione

In questo caso la gestione del dominio ricade completamente sul centro di calcolo locale sia in termini di carico di lavoro (Configurazione, Supporto per il deployment delle applicazioni, ecc.) che come autonomia decisionale.

Confronto comparato tra le due architetture

Dominio unico: si ricorda che questo modello prevede un unico dominio nazionale (nativo) con un sottodominio per ogni sito INFN, o eventualmente una OU nel caso che un sottodominio non sia necessario; questo ovviamente non impedisce la configurazione di domini locali indipendenti adibiti a scopi specifici se ciò dovesse risultare necessario o auspicabile per determinate ragioni. In questo caso tutte le risorse del dominio sono disponibili e condivisibili a livello nazionale; ad esempio si possono definire gruppi di utenti globali che raggruppano user a livello geografico per i quali possono essere definite delle policy comuni per gestire risorse distribuite. In questa configurazione e' automaticamente disponibile a livello nazionale un database LDAP di tutte le risorse, utenti ed oggetti definiti in AD grazie alla funzionalità nativa del sistema operativo. E' inoltre possibile definire una struttura DFS su WAN che permetterebbe di distribuire shares come ad esempio distribution kit e home folder di utenti (particolarmente utile per l'utenza mobile) in modo trasparente dalla locazione geografica.

Viene assicurata la completa mobilita' di utenti e computer sul territorio nazionale in modo trasparente; la mobilita' e' assicurata anche dall'estero poiché un computer portatile può entrare in dominio utilizzando un ISP locale, eventualmente attraverso opportuni meccanismi (ad esempio VPN) che assicurino la riservatezza dei dati trasmessi. Questa architettura permette anche la distribuzione globale di applicativi, attraverso opportune policy che ne permettono il controllo, la gestione centralizzata di relazioni di trust con eventuali domini esterni (ad esempio altri laboratori HEP) e soprattutto la gestione coordinata di meccanismi e policy di sicurezza sull'intero albero INFN. D'altro lato il gruppo di gestione del Dominio deve essere ben coordinato; la gestione stessa deve essere inquadrata come un Servizio, in modo da assicurare la disponibilità durante i giorni lavorativi e tempi di risposta ragionevolmente limitati per problemi che possono riguardare la struttura globale. Ciò ovviamente si riflette su una maggiore dipendenza dalla disponibilità della rete geografica, pur se in Windows 2000 esistono meccanismi che permettono di limitare fortemente la dipendenza dalla rete geografica stessa.

Domini indipendenti: questo modello prevede che ogni sezione o laboratorio configuri un dominio locale in modo assolutamente scorrelato e non coordinato tra le varie Unita'. In questo caso ovviamente la gestione e' completamente indipendente da qualsiasi altra entità esterna e ricade in toto sul centro di calcolo locale, oltre ad essere indipendente dal funzionamento della rete geografica; il database LDAP di tutte le risorse e gli utenti e' limitato a livello locale. Questa architettura limita le possibilità di sharing di risorse a livello geografico in quanto ogni operazione deve essere esplicitamente concordata con i vari domini esterni coinvolti. Gli utenti sono esclusivamente locali e non mobili tra domini differenti e risulta impossibile, almeno a livello pratico, creare gruppi globali su scala geografica.

Layout di test utilizzato e funzionalità implementate

Per poter provare le varie funzionalità di Windows 2000, in particolare le caratteristiche di auto-aggiornamento del DNS ed i legami con l'Active Directrory, senza interferenza alcuna con il dominio in produzione infn.it, si è definito w2k.infn.it. All'interno di tale dominio si sono definiti alcuni sotto-domini corrispondenti alle Sezioni che hanno partecipato alla sperimentazione: cnaf.w2k.infn.it, bo.w2k.infn.it, le.w2k.infn.it, ts.w2k.infn.it, mi.w2k.infn.it, na.w2k.infn.it. In ogni sotto-dominio è stato installato un domain controller. I test effettuati avevano come scopo la verifica delle funzionalità di Windows 2000 in una struttura ad albero su WAN.

DNS

Il root DNS per il dominio w2k.infn.it è stato definito sulla prima macchina installata, ed è basato sul Software Microsoft. Sono state provate le funzionalità di dynamic update (anche se solo per la risoluzione diretta, in quanto si sono usati indirizzi IP per la risoluzione inversa dei quali erano già autoritativi altri DNS servers). Sono state delegate ai domain controller dei sotto-domini le risoluzioni dirette per le zone corrispondenti.

Installazione automatica

E' stata effettuata una prova di installazione automatica di un pacchetto Microsoft (Office 2000) su WAN usando come application server un Server Windows2000, (in realtà è una macchina virtuale all'interno di una macchina Linux per sopperire alla mancanza di HW dedicato) presso la sezione di Lecce e come client un portatile della sezione di Lecce con a bordo Windows2000 Professional, collegato in rete al CNAF.

L'esito della prova ha dimostrato che il sistema è funzionale ed abbastanza robusto, anche se è necessario un disegno accurato delle politiche di distribuzione ed assegnazione degli applicativi. Non sono stati condotti test di performance, ma é evidente che una automatizzazione delle installazioni, può provocare una saturazione nel server se non disegnata accuratamente: es. installazione di Office2000 SP2 a tutto l'INFN.

Gruppi Geograficamente Distribuiti

E' stato possibile, grazie al fatto che i test si sono svolti in un ambiente ad albero, definire gruppi costituiti da utenti definiti in sotto-domini differenti ed assegnare a tali gruppi privilegi per l'accesso a macchine e a share, anch'essi distribuiti geograficamente.

Conclusioni

Si ritiene che in Windows 2000 si possano identificare varie caratteristiche utili per l' INFN. Si ritiene inoltre che l'implementazione di un unico dominio nazionale offra ulteriori funzionalità di particolare interesse.
Si lascia la decisione sul modello da implementare alla Commissione Calcolo.
Nel caso che si scelga l'implementazione di un unico albero nazionale si consiglia di prevedere una richiesta di consulenza a Microsoft in fase di progettazione.
Indipendentemente dalla scelta e' utile mantenere un livello minimo di collaborazione e coordinamento fra le varie Sezioni per scambio di informazioni ed esperienze, oltre ad avere un punto di contatto più significativo con il gruppo di lavoro Windows 2000 di HTASC.

Repository documentazione tecnica su Windows 2000

http://www.microsoft.com/windows2000/library/default.asp

Altri partecipanti:

Hanno partecipato al set up del layout di test anche Ombretta Pinazza (INFN Bologna) ed Alessandro Italiano (INFN CNAF).

Appendice A

Requirement Hardware in relazione alla versione di Windows 2000 da implementare.

- Windows 2000 Professional
  - Pentium 133 MHz o superiore
  - 64 MB di RAM (Minimo) 128 (Consigliato)
  - 2GB di Disco Rigido (Minimo)

- Windows 2000 Server ed Advanced Server
  - Pentium 133 MHz o superiore
  - 256 MB di RAM o superiore
  - 2GB di Disco Rigido (Minimo)

Appendice B

Porte TCP/IP utilizzate dal sistema
Windows2000 apre i seguenti servizi conosciuti:

```
Port Service
21   ftp
25   smtp
42   nameserver
53   domain
80   http
88   kerberos
119  nntp
135   DCE endpoint resolution (location service, ncs local
location broker)
139  netbios-session service
389  ldap
443  https
445  microsoft-ds (Remote Procedure Call)
464  kpasswd5 (kerberos v5)
563  snews  (nntps)
593  http-rpc-epmap
636  ldapssl
1026 nterm  (remote login network terminal)
3389 msrdp  (MS WBT Server)
```

Inoltre sono aperte le porte 1029 e 3372 per servizi non noti e non documentati. Idem per altre 11 porte maggiori di 1024 aperte in modo casuale ad ogni boot del sistema. Una lista più dettagliata può essere reperita in
http://www.microsoft.com/windows2000/library/resources/reskit/samplechapters/cnfc/cnfc_por_simw.asp