INDICE

INTRODUZIONE

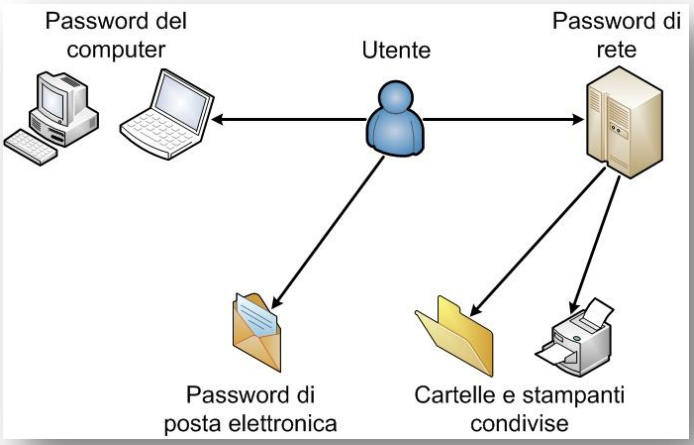
La continua evoluzione dei sistemi informativi, lo sviluppo delle reti, la diffusione del personal computer e l'accresciuta informatizzazione di base, hanno favorito la crescita del bacino d'utenza che fruisce di servizi in via telematica. Questi ultimi sono erogati sempre più frequentemente tramite applicazioni web-based spesso eterogenee e gestite da molteplici unità organizzative all'interno della stessa realtà aziendale. In questa ottica i problemi di autenticazione e autorizzazione dell'utente devono essere centralizzati per semplificarne la gestione, normalizzare ed integrare le informazioni con sistemi legacy ed attuare policy di sicurezza omogenee. Le directory services costituiscono la soluzione ideale e standardizzata al problema assumendo quindi un ruolo chiave nella infrastruttura IT aziendale.

La tecnologia delle Directory Services è diventata una componente preziosa in ogni importate infrastruttura IT. Le Directory Services sono richieste per gestire risorse, controllo degli accessi e aumentare la sicurezza internamente e esternamente alla rete. La scelta di una soluzione di Directory Services è un passo critico per le infrastrutture IT, in quanto inciderà sul futuro di tutte le relazioni tra le risorse e i relativi accessi. Infatti questa tecnologia è già il

cervello della rete in molte aziende, e lo sarà sempre più nel futuro in quanto conferisce un unico punto di amministrazione per una vasta gamma di servizi internet e intranet e permette di gestire in modo integrato utenti, server, stampanti, sistemi di file, controllo di accesso, norme di rete, sistemi desktop e impiego di applicazioni a livello aziendale.

Alle necessità di alta affidabilità e continuità si associa l'esigenza di livelli di scalabilità della infrastruttura che rispondano alle dinamiche di evoluzione dei volumi di servizi erogati.

Prima dell'avvento delle Directory Services, spesso un'utente che si trovava a lavorare in una rete aziendale, veniva fornito di diverse password per poter usufriure dei servizi messi a sua disposizione, di conseguenza durante il lavoro giornaliero si trovava a dover ricordare più password, con ovvi problemi di memorizzazione. Un esempio e l'immagine successiva.



Oppure poteva capitare il caso in cui un'utente doveva comunicare con un altro utente, all'interno di una stessa rete aziendale e non era possibile utilizzare soltanto il nome della persona, ma occorreva necessariamente la sua e-mail.

Un'altra situazione che poteva capitare, riguarda la semplice stampa di un documento. Se non si disponeva di una stampante connessa al proprio computer,

occorreva utilizzare una stampante di rete. Per poterne usufruire, occorreva procurarsi tutte le informazioni necessarie per una corretta stampa, che spesso invece non avveniva a causa di eventuali errori nelle informazioni relative alla stampante.

Per assolvere a questi e ad altri problemi, fu impiegata una singola directory aziendale anziché gestire dozzine di database sugli utenti e le risorse di rete. Una singola directory gerarchica che centralizzasse tutte le informazioni. Con il suo impiego è possibile effettuare richieste nella directory da ciascun punto di connessione sulla rete. E inoltre può essere facilmente replicata in pochi minuti e distribuita ai server nei più lontani punti della rete.

In questo tesi vengono riportati vari approci, per una corretta gestione delle utenze all'interno di una rete più o meno estesa, presentando un'architettura realizzata mediante software opensource e proprietario per i servizi di directory.

Spesso all'interno di una rete ci si trova a gestire richieste di autenticazioni e autorizzazione provenienti da computer basati su sistemi operativi differenti. Per ovviare a tale problema, e quindi fare in modo che tutti gli utenti siano correttamente autenticati e autorizzati, ho analizzato e configurato due diversi servizi di directory, uno nel mondo Linux e l'altro in quello Windows, in modo tale che si sincronizzino tra di loro per poter gestire contemporaneamente richieste di autenticazione e autorizzazione provenienti da computer con sistemi operativi differenti.

CAPITOLO 1

DIRECTORY SERVICE

1.1 Definizione di Directory

Una directory è un contenitore di dati. Ad esempio, una directory è una guida TV, la quale elenca i programmi televisivi e gli orari di programmazione. Queste directory tradizionali sono stampate e distribuite a intervalli regolari e non sono modificate, ma sostituite da nuove emissioni; pertanto possono essere considerate *directory non in linea*. Tali directory sono utilizzate generalmente per la pubblicazioni di informazioni di sola lettura.

Una *directory in linea* è una directory a cui è possibile accedere e che è possibile aggiornare elettronicamente su una rete di computer, una LAN (local area network), una WAN (wide area network) o anche Internet. Molte directory non in linea dispongono di una corrispettiva directory in linea o elettronica. Le compagnie telefoniche pubblicano i propri elenchi e le pagine gialle sul Web e forniscono un'interfaccia di semplice utilizzo.

Altri tipi di directory in linea includono directory di applicazioni e directory destinate a un determinato scopo. *Una directory di applicazione* è relativa a un'applicazione software, ad esempio Lotus Notes o Novell GroupWise. Entrambe utilizzano directory proprietarie adatte alle esigenze specifiche dell'applicazione.

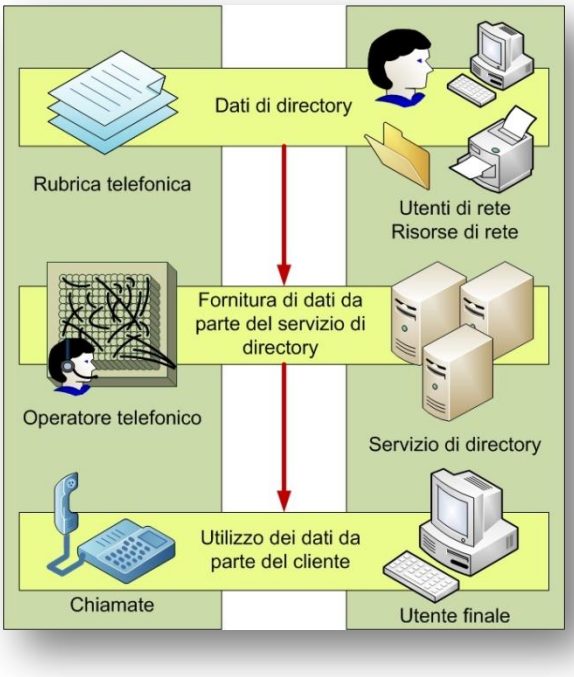
Una *directory destinata a un determinato scopo* può essere utilizzata da qualsiasi applicazione, ma è legata alla gestione dei dati per un obiettivo limitato. Un esempio di questo tipo di directory è rappresentato dal DNS (Domain Name System) utilizzato da Internet. Anche se differenti applicazioni utilizzano DNS, le

informazioni in esso contenute sono utili solo per specifiche attività, quali la risoluzione dei nomi e degli indirizzi IP.

Le *directory di rete* sono directory in linea che memorizzano informazioni relative ai servizi e alle risorse di rete. In genere, includono informazioni sull'utente, dati di protezione e un elenco di servizi disponibili come i servizi di pubblicazione e di stampa.

1.2 Definizione di un Servizio di Directory

Spesso, alla domanda relativa a cosa è un servizio di directory, la maggior parte delle persone risponde riferendosi all'operatore telefonico che ricerca i numeri telefonici per l'utente. In effetti la risposta è corretta. Se la directory rappresenta i dati effettivi, cioè l'elenco di persone e i numeri telefonici, gli operatori e il metodo mediante cui sono chiamati, rappresenta il servizio di directory. Nel mondo elettronico le cose non stanno diversamente. La figura sottostante illustra un confronto tra un servizio di directory telefonico tradizionale e un servizio di directory elettronico.



Un servizio di directory fornisce l'archiviazione e il recupero di informazioni di directory per utenti e applicazioni. Le aree interessate dal servizio di directory riguardano le prestazioni, la protezione, l'affidabilità, la disponibilità e la semplicità di utilizzo. Quest'ultima comporta che gli sviluppatori possono scrivere applicazioni per accedere alle informazioni di directory senza eccessive difficoltà di programmazione.

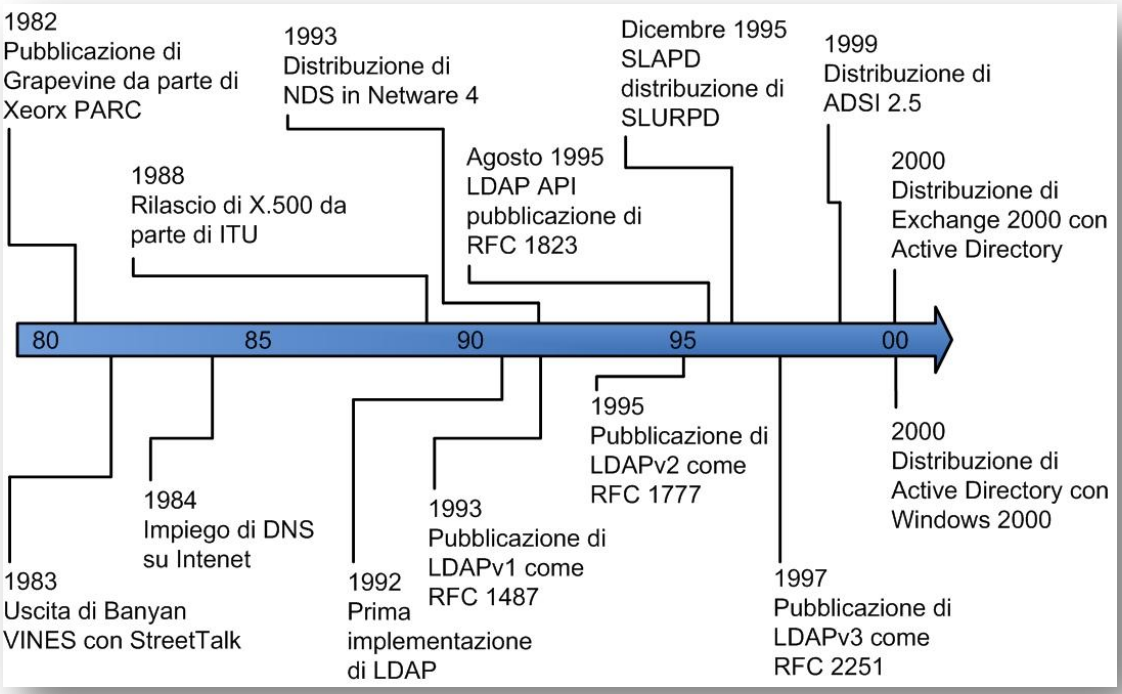
Le directory di rete forniscono soluzioni adatte. Per assicurare elevata disponibilità, le informazioni di directory sono replicate a molti server. I computer che accedono alle informazioni nella directory possono effettuare la stessa operazione dal server più vicino, con conseguente miglioramento delle prestazioni. Poiché è possibile raccogliere e presentare le informazioni di directory in diversi modi, ne risulta una più semplice accessibilità per l'utente finale.

I servizi di directory facilitano le attività per gli sviluppatori, gli amministratori e gli utenti finali. Per uno sviluppatore, i servizi di directory facilitano la memorizzazione e la ricerca di informazioni relative alle risorse di rete. Le applicazioni possono pubblicare informazioni da memorizzare nella directory di rete che possono essere utilizzate da altre applicazioni; gli amministratori di rete ottengono vantaggi rappresentati da un miglioramento della protezione e dalla semplicità di amministrazione. Gli utenti beneficiano di un modello di protezione comune (senza la necessità di diverse password); essi usufruiscono della condivisione di dati tra applicazioni e non devono più ricordare elementi specifici di una risorsa nella directory, come ad esempio il percorso di rete alla stampante.

1.3 Cenni Storici sulle Directory

Le directory di rete comportano grandi vantaggi per gli utenti, per i professionisti IT e gli sviluppatori. Il modo in cui tali vantaggi si sviluppano, è determinato dalla storia delle directory di rete, specialmente dallo sviluppo e

dall'evoluzione di DNS, X.500 e LDAP, tre servizi di directory. La figura sottostante illustra i periodi di alcuni degli eventi significativi nella storia delle directory.



1.4 DNS (Domain Name System)

Una delle principali directory elettroniche, il sistema DNS (Domain Name System) prevede la corrispondenza dei nomi di dominio su Internet con i rispettivi indirizzi IP (Internet Protocol) difficili da ricordare. Come le persone dispongono di numeri telefonici, i computer su una rete TCP/IP dispongono di indirizzi IP. Affinché un computer comunichi con un altro computer sulla rete, è necessario che conosca l'indirizzo IP dell'altro computer. Le informazioni utilizzate da DNS sono create localmente e distribuite globalmente. È possibile aggiungere un nuovo computer alla rete, assegnare il nome *copper1* e indicare al server DNS il nuovo nome del computer e l'indirizzo IP.

Data la presenza su Internet di migliaia di computer, sarebbe dispendioso replicare tutte le informazioni a tutti i server DNS. Invece, quando un server DNS non riconosce un nome che gli viene fornito, invia la richiesta a un altro server DNS nella catena. Infine, il sistema rileva il server responsabile del dominio *coppersoftware.com*, richiede la ricerca di *copper1* e restituisce l'indirizzo IP. Poiché DNS è un sistema notevolmente solido, tutti i computer connessi a Internet sono in grado di comunicare con *copper1*, specificando il nome *copper1.coppersoftware.com*; il nome di dominio completo per il DNS di rete rappresenta un eloquente esempio di directory destinata a un determinato scopo.

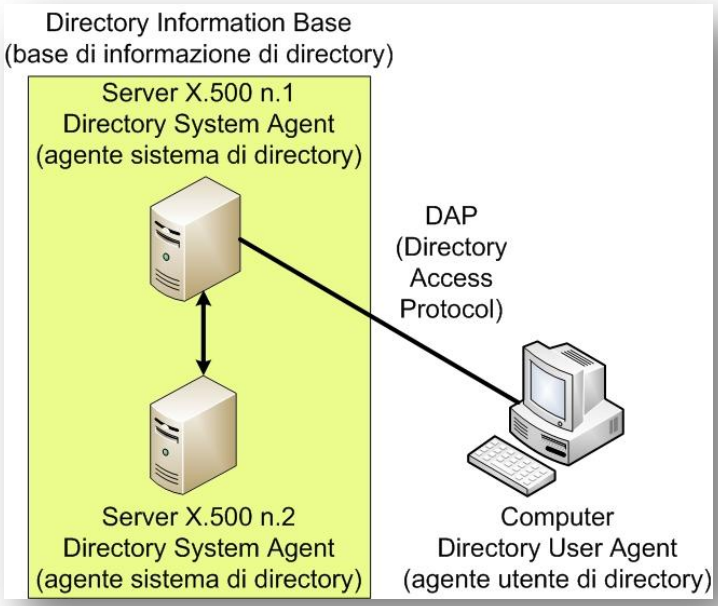
1.5 Servizio di Directory X.500

Il proliferare di applicazioni in rete ha comportato la necessità di directory standardizzate che implementassero interfacce di programmazione comuni, in modo che più applicazioni potessero accedere alle stesse informazioni. Questo periodo ha avuto inizio nel corso degli anni '80 con diverse organizzazioni aziendali e accademiche volte alla ricerca di una soluzione comune di directory. Nel 1988, l'International Telecommunications Union ha pubblicato i servizi di directory X.500 e definito il protocollo DAP (Directory Access Protocol). Questo standard rappresentava il culmine dello sforzo compiuto da CCITT (International Telephone and Telegraph Consultative Committee), ora nota come ITU-T, e dell'organizzazione ISO (International Standards Organization) per produrre uno standard globale dei servizi di directory. Lo standard X.500 è stato aggiornato nel 1993 e in seguito nel 1997.

Sviluppati dall'inizio per essere un servizio di directory globale omnicomprensivo, X.500 e DAP furono considerati difficili da implementare e non ebbero ampia diffusione commerciale. Un altro limite fu rappresentato dal fatto che X.500 dipendeva dai protocolli di rete OSI (Open Systems Interconnect) anziché dai modelli Internet attualmente prevalenti, basati su TCP/IP. Sebbene

X.500 presentasse una natura distribuita ed efficaci funzionalità di ricerca nelle directory, tali caratteristiche richiedevano un'elevata quantità di risorse di elaborazione.

Quando i fornitori di software esaminarono X.500, rilevarono che la complessità dell'interfaccia era preoccupante e non si resero contro delle potenzialità di questo standard efficace e aperto. Essi non intuirono l'importanza di un servizio di directory globale, e le directory proprietarie ebbero un'evoluzione analoga al software utilizzato. La figura successiva illustra i componenti di un sistema X.500.



1.6 L'avvento di LDAP

Le versioni precedenti di applicazioni utilizzavano directory, che però erano proprietarie, nel senso che l'interoperabilità con altri client era disponibile solo in determinati casi. La flessibilità, la protezione e la replica erano minime o addirittura inesistenti. I sistemi operativi di rete come Banyan VINES, Microsoft Windows NT e Novell NetWare iniziarono l'implementazione di moduli di

directory per gestire utenti e risorse di rete. NetWare disponeva di Bindery, mentre Windows NT disponeva del database SAM (Security Account Manager). Banyan iniziò con un servizio di directory integrato denominato StreetTalk, innovativo ma che non ottenne mai un successo commerciale. Ciascuna directory memorizzava informazioni sugli utenti e le risorse di rete, ma ciascuna era orientata verso l'autenticazione e la protezione, le esigenze principali dei sistemi operativi di rete in quel periodo.

Dal 1993, con la seconda revisione di X.500 che generò un lieve interesse commerciale, un gruppo di ricercatori dell'Università del Michigan svilupparono un'alternativa alla complessa interfaccia DAP in X.500. L'obiettivo era quello di creare un protocollo di accesso più semplice alle directory X.500. Il gruppo creò un protocollo che rimuove-va molti elementi di X.500 di intralcio agli sviluppatori, particolarmente il modello di rete OSI, e che eliminava molte delle funzioni non utilizzate di DAP. Questa versione di DAP partì come DIXIE (RFC 1249) e divenne nota come LDAP (Lightweight Directory Access Protocol). Anche se questa prima versione di LDAP costituiva un notevole miglioramento rispetto al complesso DAP di X.500, non fu immediatamente presa in considerazione dai fornitori, almeno fino alla pubblicazione di LDAPv2 (nella forma proposta in RFC 1487 e come standard in RFC 1777).

Inizialmente, LDAP era una semplice alternativa al protocollo DAP di X.500. Tuttavia, poiché LDAP definiva il protocollo, gli sviluppatori erano liberi di effettuare le implementazioni di un servizio di directory che si conformava semplicemente ai requisiti di LDAP e non richiedeva X.500. La prima implementazione fu effettuata presso l'Università del Michigan, dove nel 1995 furono sviluppati SLAPD (stand-alone LDAP daemon) e il relativo partner di replica SLURPD (stand-alone LDAP update replication daemon). SLAPD era un semplice server LDAP in grado di comunicare con diversi database differenti che fungevano da directory. SLURPD era il programma che replicava le modifiche

apportate nel database di directory, agli altri computer che fungevano da server di directory.

Importante per il successo di LDAP fu inoltre lo sviluppo dell'interfaccia API (Application Programming Interface) per il linguaggio C. Definita in RFC 1823, questa API include un insieme di funzioni che gli sviluppatori possono utilizzare per accedere ai servizi di directory. Windows NT e Windows 2000 supportano questa API come parte del sistema operativo per consentire alle applicazioni in esecuzione su queste piattaforme l'accesso alle directory basate su LDAP.

Alcune parti di LDAP sono state sviluppate nel corso degli anni, con uno sforzo maggiore indirizzato a fornire estensibilità. L'ultima versione, pubblicata nel 1997 come RFC 2251, è nota come LDAPv3. Questa versione è un superset di LDAPv2 e include nuove funzioni, quali controlli estesi e la capacità di esporre la definizione o lo schema dei dati di directory. Una funzione principale di LDAPv3 consiste nella capacità delle directory LDAP di esporre informazioni relative ai servizi forniti [1].

1.7 Lightweight Directory Access Protocol

Per LDAP, acronimo di *Lightweight Directory Access Protocol,* intendiamo un protocollo leggero per accedere ai servizi di directory, basati sul protocollo X.500 dal quale trae le sue origini. X.500 risalente al 1988 (raccomandazione CCITT X.500 / ISO IS9594) e adottato per rispondere alle esigenze di accesso e condivisione di directory (o Directory Service, Servizio di Directory).

Sviluppato originariamente presso l'Università del Michigan, LDAP fu impiegato inizialmente proprio come front-end a sistemi X.500.

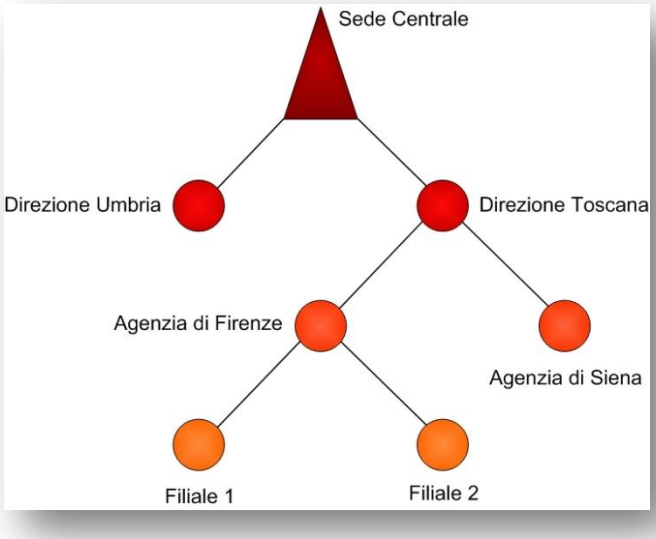
La raccomandazione X.500, alla quale si devono riferire tutti i servizi di directory, include numerose caratteristiche interessanti, la maggior parte

inutilizzate; l'implementazione della stessa è molto complessa, richede grandi risorse e necessita inoltre di uno stack OSI completo: tutti i motivi che spinsero a svilupparne un'implementazione semplificata, *Lightweight Directory Access Prococol* appunto o anche X.500 Light, che funzionasse correttamente su architetture PC e fosse basata sulla più snella suite TCP/IP.

Proposto nel 1993, LDAP è stato successivamente adottato dalla IETF e reso standard nel 1995 con RFC1777 e successivamente con RFC2251 per il rilascio della relase LDAPv3.

Per *Directory* intendiamo un servizio che offre la possibilità di consolidare informazioni eterogenee all'interno di elenchi gerarchicamente strutturati, consentendo l'accesso su rete, insieme a uno o più metodi per individuarle, insomma una sorta di rubrica virtuale, un servizio con accesso globale del tipo *white pages*.

Tanto per chiarire, il concetto di *spanning* delle informazioni che sta alla base del funzionamento del DNS si avvicina, e di molto, a quello relativo ad una Directory.



Usiamo comunemente i servizi di directory, magari pervasivamente o chiamandoli in un altro modo: un esempio è la rubrica telefonica del cellulare, ma non è necessario l'imprimatur elettroico-informatico: la guida telefonica è pur

sempre una directory così come lo è l'organigramma di un'azienda o l'inventario dei libri disponibili in una biblioteca, nelle varie forme in cui questi elenchi sono rappresentati e i loro contenuti referenziati. Bene, LDAP è insieme un metodo e un protocollo che descrive e consente l'accesso alle directory e ai loro dati.

Come X.500 LDAP organizza i dati in strutture gerarchiche che sono in grado di immagazzinare variegate e numerose informazioni. Anche se originariamente, e in molti casi tuttora, veniva utilizzato semplicemente come rubrica virtuale, LDAP è molto di più: se non altro perché può propagare le proprie informazioni ad altri server LDAP in tutto il mondo.

Ma quello che lo rende particolarmente appetibile e interessante è la possibilità di essere utilizzato come repository di userid-password per servizi di autenticazione centralizzata. Tramite moduli *pam_ldap* gli utenti potranno disporre di un login unificato che comprende i login di console, i server POP e IMAP, le macchine connesse a una rete tramite Samba e perfino calcolatori Windows NT/2000, semplificando notevolmente l'amministrazione.

Per capire l'utilità di un servizio generico di questo tipo consideriamo come in un sistema GNU/Linux siano già presenti molteplici elenchi di informazioni: la lista degli utenti, quella dei gruppi, quella delle porte TCP e UDP, etc. In generale si tende a distinguere fra quelli che sono i servizi di elenco *locali*, come la lista degli utenti di `/etc/passwd`, e quelli che invece sono globali, come la lista delle corrispondente fra nomi a dominio e numeri IP fornite dal DNS.

La presenza di un servizio che permetta di mantenere diversi tipi di informazione e di recuperarli in maniera efficiente sulla base di criteri di ricerca generici viene allora a costituire uno strumento fondamentale in tutti quei casi in cui si debbano integrare fra loro sistemi diversi che necessitano di accedere a informazioni comuni, che a questo punto possono essere mantenute in maniera centralizzata all'interno di questo servizio.

Ma non solo LDAP può essere efficacemente impiegato in altri ambiti quali:

- Back end di autenticazione per servizi Internet (Apache, SQUID, FTP ecc);
- Profiling degli utenti;
- Repository di configurazioni per server DHCP;
- Name server;
- Routing di posta elettronica, mailing-list.

1.8 Perché utilizzare LDAP

Il vantaggio principale nell'uso di LDAP, trattandosi di un protocollo aperto e configurabile, e la possibilità di considerare in maniera strutturata quasi ogni tipo di informazione, consentendone anche la replica (ridondanza del servizio) e la distribuzione *(bilanciamento del carico)* su server distinti. Dal momento poi che sono supportati i protocolli SSL *(Secure Sockets Layer)* e TSL (Transport Layer Security), è possibile proteggere i dati importanti da occhi indiscreti.

Inoltre il protocollo è costituito da una parte che definisce l'organizzazione dei dati (chiamata *Data model*) che permette di stabilire come viene rappresentata l'informazione, uno schema di assegnazione dei nomi (detto *Naming model*) che identifica il singolo dato mantenuto nel sistema, ed infine una modalità di accesso ai dati con tanto di meccanismi molto dettagliati per il controllo degli accessi. Il protocollo invece non dice niente rispetto alle modalità specifiche in cui i dati vengono memorizzati, tratta solo la loro strutturazione astratta, e le modalità con cui possono essere compiute le operazioni previste dal protocollo (ricerca, lettura o scrittura) sugli stessi; l'implementazione è lasciata al funzionamento del singolo server. LDAP supporta numerosi database backend in cui immagazzinare le directory, ciascuno dei quali ottimizzato per operazioni di lettura rapide e per grandi volumi: questo accorda agli amministratori la flessibilità di scegliere il database più indicato per il tipo di informazione che il server deve mantenere.

Inoltre, poiché LDAP ha un'API chiara e ben definita, in numero di applicazioni e gateway che sfruttano LDAP è elevato e sta ancora crescendo in termini di quantità e qualità: fra l'altro molte applicazioni Netscape, incluso il Netscape Roaming Access, sono di default abilitate al protocollo LDAP.

Gli svantaggi consistono principalmente nel fatto che LDAP richiede client abilitati e che, a volte, può essere abbastanza complesso da configurare.

1.9 Caratteristiche

LDAP è un sistema client-server con protocollo di tipo message-oriented (vengono spedite richieste ed ottenute risposte). Quando un'applicazione client si cinnette a un server LDAP, può interrogare una directory oppure caricare informazioni al suo interno. Nel caso dell'interrogazione il server risponde oppure, se non può farlo a livello locale, può delegare il flusso dell'interrogazione a un server LDAP di livello superiore che sia in grado di rispondere. Se l'applicazione client cerca di caricare informazioni all'interno di una directory LDAP, il server verifica che l'utente abbia il permesso di attuare la modifica, poi aggiunge o aggiorna le informazioni. E' del tutto evidente la similitudine fra directory LDAP e database, potendo sicuramente definire le prime come un database specializzato ed ottimizzato per ricerche e consultazioni. In particolare, una directory LDAP:

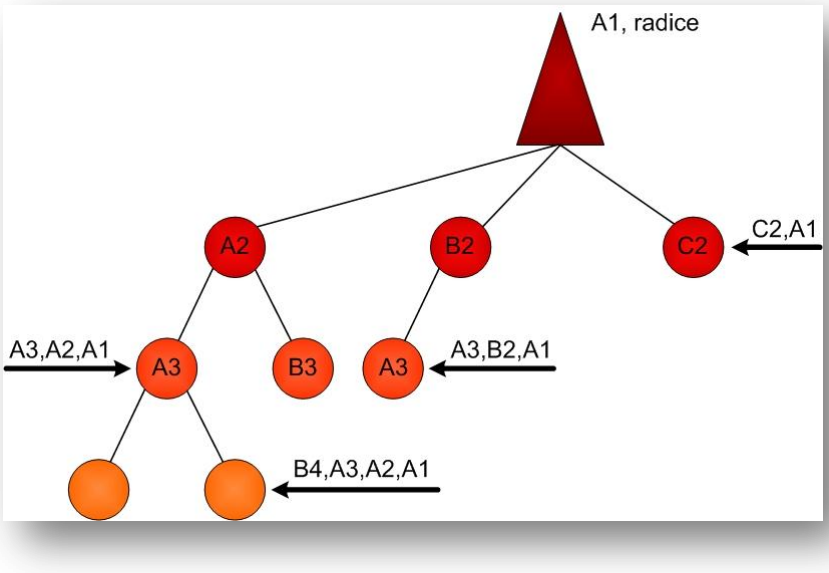
- Supporta in maniera nativa strutture gerarchiche (dette anche alberi) che permettono di modulare a piacere la profondità dell'esplorazione, a partire dal livello di ingresso nella struttura;

- Accetta per ogni entry un numero arbitrario di attributi, ciascuno con un arbitrario numero di valori (si parla strettamente di *entry* e non di *row*, termine tipico e più appropriato ai db);

- Ha sempre un bassissimo rateo di aggiornamenti;

- E' object oriented, pensato per contenere informazioni basate su coppie attributi-valori;
- Non ha meccanismi di roll-back;
- E' ottimizzato per fornire una più elevata performance alle richieste di browsing;
- Può essere facilmente replicato in strutture master-slave;
- Supporta la distribuzione del carico far più servizi correlati;
- In casi di directory replicate su più server, valuta come accettabili anche inconsistenze temporanee delle informazioni, dovute alle non istantaneità degli aggiornamenti.

Ogni oggetto o entry di una directory LDAP ha poi la peculiarità di possedere un attributo unico non ambiguo, il *Distinguished Name* o DN, che ha come valore il percorso necessario ad individuarlo, a partire dalla radice dell'albero in cui l'oggetto stesso è posizionato, nella figura i nodi indicati dalle frecce.



Il Distinguished Name riflette la verticalità dell'intera struttura, ed è peraltro un concetto noto, del tutto simile al Domain Name in ambito DNS o al path assoluto usato per recuperare un file.

I Distinguished Name sono stati introdotti con RFC2253, al quale rimando per tutti i dettagli, così come per gli altri RFC menzionati in questo lavoro.

E' abbastanza semplice capire come sia possibile rappresentare un dominio tramite una directory: si potrà usare come radice il proprio FQDN e proseguire verso il basso inserendo gli opportuni contenitori per *hosts,groups,people,* e quant'altro necessario. Da qui ad utilizzare una directory come repository per una autenticazione il passo è breve.

1.10 Terminologia LDAP

Il primo ostacolo che si incontra approcciando una nuova tecnologia è quello dovuto ai suoi termini e acronimi, e come spesso accade, purtroppo, la letteratura, how-to, publicazioni e quant'altro differiscono spesso tra loro utilizzando termini diversi per indicare i medesimi concetti. Per evitare di fossilizzarsi su un "termine" piuttosto che su un concetto, si fa un breve escursus sulla struttura di LDAP, familiarizzando nel contempo con la terminologia impiegata; nel proseguio i termini e acronimi diverranno via via più familiari.

1.10.1 Struttura e entry

LDAP ha un suo namespace costituito da un insieme di oggetti o entry, ciascuna descritta tramite un insieme di coppie:

```
<attributo><valore>
<attributo><valore>
<attributo><valore>
[…]
```

Ogni attributo possiede (RFC2256):

- Un nome (unico e non-sensitive);
- Una sua abbreviazione;
- Un OI o object identifier (una sequenza di interi separati da punti);

ed alcune indicazione come: il tipo di valore che referenzia (stringa, intero, JPEG…), il tipo di operazione di confronto che può sostenere, la possibilita di referenziare più valori, etc.

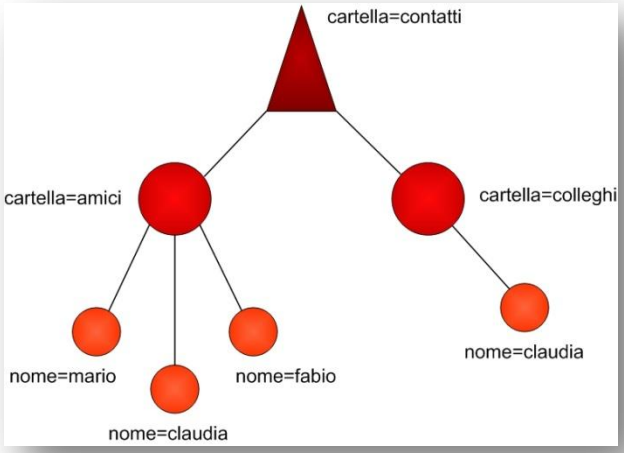
Come oramai noto, le entry poi sono organizzate gerarchicamente in una struttura ad albero che prende il nome di *Directory Information Tree* (DIT, o anche "albero LDAP" o più semplicemente *directory*).

Nell'ambito di una directory ogni entry è identificata in maniera non ambigua tramite il proprio Distinguished Name (DN), mentre la directory è a sua volta identificato da un elemento radice o base, identico anche con il nome *DN-radice*.

Il Directory Information Tree è simile ai file system Unix/Linux, ma mentre in un DIT una entry può essere indifferentemente un contenitore o rappresentare dati, in Unix una entry può essere un file o una directory e non simultaneamente le due cose. Inoltre come già detto, gli identificatori LDAP (i Distinguished Name) sono letti dal basso verso l'alto a differenza di quando avviene nello specificare un file (si parte dalla "/" e si procede verso il basso).

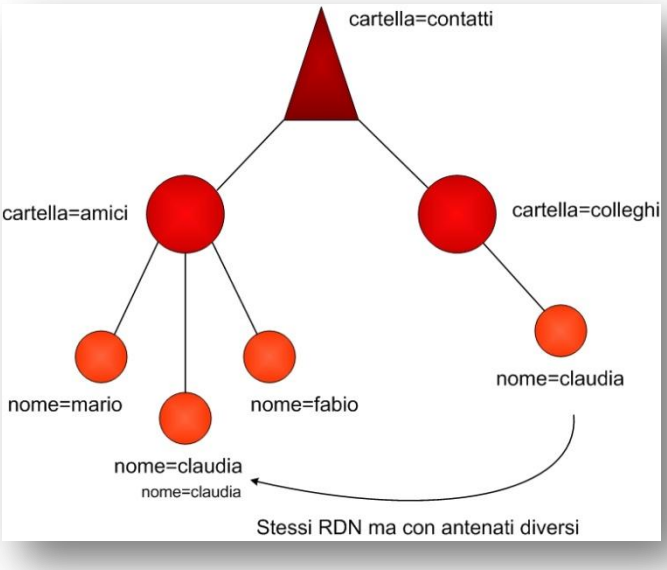
Ad esempio, nella directory LDAP delle figura successiva l'entry `mario` ha come Distinguished Name il valore:

```
dn: nome=mario,cartella=amici,cartella=contatti
```



Più precisamente ogni entry dell'albero deve avere una coppia

`<attributo><valore>` per così dire "elettiva" che prende il nome di *Relative Distinguished Name* (RDN) e che deve essere unica e differente fra tutti i discendenti diretti di uno stesso padre (questo assicura che non ci siano due entry con lo stesso nome) come visibile nella figura successiva.



Orbene, Distinguished Name di una entry altro non è che la sequenza ordinata degli RDN letti a partire dalle entry stessa e proseguendo fino alla radice, separando con una virgola ogni nodo incontrato.

1.10.2 Nomenclatura (naming)

Le specifiche che sono alla base di LDAP, X.500 prima e RFC poi, hanno ispirato l'uso di due modi o stili diversi per la nomenclatura delle radici: il *traditional naming* (che si richiama a X.500) ed il più recente *internet naming* (o stile RFC) che ricalca sostanzialmente l'organizzazione propria del DNS.

Nella nomenclatura in stile X.500 vengono tradizionalmente usati attributi che hanno a che fare con riferimenti di tipo geografico del tipo: `s (state), c (country), l (location).`

Ad esempio, dovendo descrivere con una directory LDAP l'organigramma della italianissima Ditta Rossi, potremmo porre come radice una entry del tipo:

```
c=it, o=ditta rossi
```

Nel più recente stile RFC si preferisce invece riferirsi a nomi di dominio di secondo livello o di top level domain tramite l'attributo dc (Domain Component); in questo modo la medesima radice vista poc'anzi diverrà:

```
dc=dittarossi, dc=it
```

In questo modo viene proposto come radice il più robusto `dittarossi` che ci mette al riparo da possibili ambiguità di suffissi X.500 del tipo Ditta Rossi - Italia. I due stili di naming adottano comunque medesimi nomi per le altre entry di livello inferiore (al di sotto della radice).

1.10.3 Classi e schemi

Come visto poco sopra, i nomi usati per gli attributi non sono liberamente lasciati alla fantasia dell'amministratore del server LDAP, altrimenti addio alla globlità del servizio: gli attributi usati per descrivere gli oggetti devono sottostare a specifiche ben precise, definite e raggruppate in schemi e classi standard.

Abbiamo visto come ogni entry sia rappresentata mediante un insieme di attributi e relativi valori o meglio, da un insieme di coppie `<attributo><valore>`: orbene, una classe *objectClass* (o più brevemente *classe*) è uno specifico set di attributi funzionali, alcuni dei quali obbligatori e altri opzionali (ovvero *required* e *optional*). Ogni entry può essere descritta da una o più classi e di conseguenza deve utilizzare almeno tutti gli attributi previsti come obbligatori della classi usate, mentre non ci sono limiti inferiori o superiori per quando riguarda l'uso degli attributi opzionali delle medesime classi. A titolo di esempio, per una generica entry relativa ad una `persona` potranno essere obbligatori gli attributi `<nome>`, `<cognome>` e `<nome + cognome>` e facoltativi altri, quali `<indirizzo e-mail>`, `<telefono>`, `<foto>`, etc.

Un attributo può essere riconducibile a più di una classe. Se, a puro titolo di esempio, servisse una classe necessaria alla descrizione dell'oggetto `automobile` avremmo bisogno di pescare attributi quali: `marca`, `modello`, `cilindrata`, `alimentazione`, `posti`, `categoria`… ma gli attributi `marca` e `modello` possono essere usati anche da una classe che descrive un computer: quindi non è detto che gli attributi appartengono ad una classe, quest'ultima è solo una "raccolta" di attributi finalizzata alla rappresentazione di un particolare oggetto.

Ad esempio, questa volta reale, la objectClass `Person` si propone di descrivere genericamente una persona mediante glia ttributi:

Required Attributes	Optional Attributes
cn sn	description seeAlso telephoneNumber userPassword

Il che significa che se viene usata questa classe si dovrà obbligatoriamente usare gli attributi `cn` (*Common Name*) e `sn` (*Surname*) e, qualora si voglia, uno o più fra quelli opzionali (almeno una trentina di altre objectClass impegnano l'attributo `cn`).

Così come per gli attributi, anche le classi sono specificate secondo la semantica X.500, indicando per ciascuna di esse:

- OID;
- Descrizione;
- Categoria (astratta,strutturale,ausiliaria);
- Attributi obbligatori;
- Attributi ammessi (o opzionali, facoltativi).

Essendo a sua volta `objectClass` un particolare attributo, il nome o i nomi delle classi che si desidera utilizzare per ogni entry devono essere specificati all'interno delle entry medesima tramite una apposita classe chiamata `top`, che prevede un unico attributo obbligatorio (`objectClass`, appunto) e nessuno facoltativo:

Required Attributes	Optional Attributes
objectClass	none

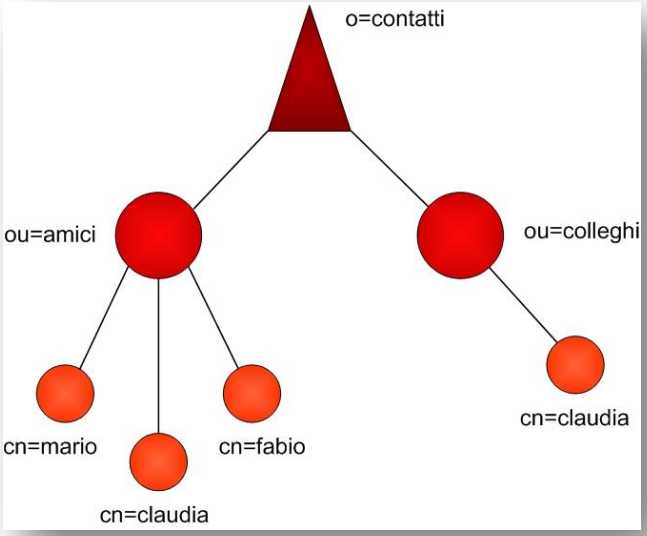
Abbiamo visto come la classe `person` non sia legata ad un particolare ambito applicativo, ma sia per così dire "all purposes", esistono altre classi generalisti che, fra le quali merita menzione le `organizationalUnit`: alla lettera *unità organizzativa* o meglio dipartimento, è quasi sempre impiegata come "contenitore" ai primissimi livelli delle directory (immediatamente sotto la radice) ed è utilissima nel disegnare l'intera ramificazione della directory.

Required Attributes	Optional Attributes
ou	businessCategory description destinationIndicator telephoneNumber facsimileTelephoneNumber postOfficeBox

	postalAddress postalCode street st ….

Questa classe prescrive un solo attributo obbligatorio (ou) ed una notevole sfilza di opzionali, la cui genericità è tale da poter essere usata nei più disparati casi.

Riferendoci all'esempio di directory illustrato nelle due figure precedenti potremo ora dargli l'aspetto più *LDAP-consono* della prossima figura, riscrivendo gli RDN delle entry e facendo uso delle due classi appena viste.



In questo modo il `DN` dell'amico `mario` si scriverà come

```
dn:  cn=mario,ou=amici,o=contatti
```

e la relativa entry conterrà gli attributi obbligatori,e a nostra discrezione quelli opzionali, previsti dalla classe `person`:

```
dn: cn=mario,ou=amici,o=contatti
objectClass: top
objectClass: person
```

```
cn: Mario
sn: Rossi
description: grande informatico Americano
telephoneNumber: 123.221212
telephoneNumber: 324.66332
```

notare la possibilità di inserire più valori per un unico attributo (ad esempio `telephoneNumber`) a dispetto di quanto invece richiesto da un database. Allo stesso modo, per la entry `amici` (che funge come contenitore) avremo:

```
dn: ou=amici,o=contatti
objectClass: organizationalUnit
ou: amici
```

1.11 Schema

Un insieme delle definizioni di attributi e classi prende il nome di schema, che, come avviene per le classi, può fare riferimento anche ad attributi e classi definiti in altri schemi. Ritorniamo all'esempio di prima, una casa automobilistica potrebbero scriversi un proprio schema integrando classi e attributi già esisteni con la creazione di nuovi, più specifici per le sue peculiari esigenze, come del resto ha fatto il team Samba, creandosi un apposito schema, il `samba_schema`, per offire il supporto a OpenLDAP.

Un discreto numero di schemi *all purpouses*, e quindi di objectClass e relativi attributi, vengono forniti di default sia dai pacchetti stessi di LDAP sia dai pacchetti di applicativi che offrono il supporto a LDAP (Samba, PAM, Apache, etc.): esistono comunque schemi per svariate esigenze di rappresentazione e quindi, prima di crearsene uno proprietario, è sempre bene consultare i cataloghi disponibili, indicati in webografia, e altri, comunque rintracciabili tramite motori di ricerca.

Tutti i dati che compongono l'albero LDAP sono descritti negli schemi, in

cui, per ogni oggetto, vengono definiti i campi che lo compongono ed i tipi di dati. Gli *attributi* sono definiti in uno schema nel seguente modo:

```
attributetype ( 2.5.4.3 NAME (‘cn’ ‘commonName’ )
       DESC ‘RFC2256: common name(s) for which the entry is known by’
       SUP name )
attributetype ( 2.5.4.4 NAME (‘sn’ ‘surname’ )
       DESC ‘RFC2256: last name(s) for which the entry is known by’ SUP
       name )
attributetype ( 2.5.4.35 NAME (‘userPassword’ )
       DESC ‘RFC2256/2307: password of user’
       EQUALITY octetStringMatch
       SYNTAX 1.3.6.1.4.1.1466.115.121.1.40{128} )
attributetype ( 2.5.4.20 NAME (‘telephoneNumber’
       DESC ‘RFC2256: Telephone Number’
       EQUALITY telephoneNumberMacth
       SUBSTR telephoneNumberSubstringsMatch
       SYNTAX 1.3.6.1.4.1.1466.115.121.1.50.{32} )
```

Gli attributi sono raggruppati dagli *oggetti*, la cui definizione è formulata come segue:

```
Objectclass ( 2.5.6.6 NAME ‘person’
        DESC ‘RFC2256: a person’
        SUP top STRUCTURAL
        MUST ( sn $ cn )
        MAY ( userPassword $ telephoneNumber ) )
```

Gli schemi principali sono definiti formalmente in diverse RFC, ma è tuttavia possibile definire degli schemi personalizzati in base alle particolari esigenze degli sviluppatori [2].

1.12 I file in formato LDIF

In generale ogni server LDAP mantiene i dati contenuti nell’elenco tramite un opportuno meccanismo di supporto. Per permettere di trasferire i dati fra server diversi è stato definito un apposito formato di interscambio, *l’LDAP Data Interchange Format* (in breve LDIF) che permette di esprimere una qualunque voce usando dei semplici file di testo.

Lo standard che definisce il formato LDIF è specificato dall'RFC 2849, questo prevede che ogni voce nel database possa essere espressa in testo semplice, con una schematizzazione della stessa nella forma:

```
# commento
dn: <distinguished name>
<nome attributo>: <valore>
<nome attributo>: <valore>
...
```

Al solito il carattere "`#`" viene usato per indicare una linea di commento e le righe vuote vengono ignorate. Ciascuna voce deve essere introdotta da una riga iniziante per `dn:` che ne dichiari il *Distinguished Name* in modo da identificarla univocamente; Alla dichiarazione del *Distinguished Name* seguono le assegnazioni dei vari attributi nella forma illustrata, questi devono essere indicati tramite il relativo nome (come `cn` o `objectClass`), seguito dal carattere "`:`" da uno spazio e poi dal valore. Per poter utilizzare uno specifico attributo occorrerà ovviamente che l'oggetto derivi da una *objectClass* che lo definisce; se il file specifica un oggetto che deve essere creato si può indicare da quali *objectClass* derivarlo attraverso l'attributo speciale `objectClass`.

Se una riga è troppo lunga può essere fatta proseguire sulla successiva usando come primo carattere di quest'ultima o uno spazio o un tabulatore. Si tenga inoltre conto che gli ulteriori spazi iniziali che seguono il carattere "`:`" non vengono ignorati, e che la presenza di spazi multipli all'interno dei valori viene mantenuta tale e quale; pertanto se non si vogliono spazi aggiuntivi occorre stare attenti a non metterceli. Qualora il valore dell'attributo non sia esprimibile con caratteri stampabili, o inizi per uno spazio o con i caratteri riservati "`:`" e "`<`" questo dovrà essere specificato usando una sintassi diversa; le opzioni sono due, la prima prevede l'uso di un valore codificato in formato *Base-64*, la seconda invece prevede la lettura dei dati direttamente da una fonte di dati esterna specificata tramite la sua URL. In tal caso la dichiarazione del valore di un attributo user`a le

due forme alternative "::" e ":<" ad esempio per specificare il valore di un attributo `jpegPhoto` si potranno usare le sintassi:

```
jpegPhoto::/9j/4AAQSkZJRgABAgAAZABkAAD/7AARRHVja3kAAQAEAAAAUAAA/+
 4ADkFkb2JlAGTAAAAAAf/bAIQAAgICAgICAgICAgMCAgIDBAMCAgMEBQQEBAQEB
 QYFBQUFBQUGBgcHCAcHBgkJCgoJCQwMDAwMDAwMDAwMDAwMDAEDAwMFBAUJBgYJ
 ...
jpegPhoto:<   file:///path/to/photo.jpeg
```

Qualora un attributo compaia più volte questo dovrà essere ripetuto su righe distinte; infine si possono inserire più voci all'interno di uno stesso file separandole con una o più righe vuote.

Un esempio di file LDIF è allora il seguente:

```
# Truelite Srl, Contacts, truelite.it
dn: cn=Truelite Srl,ou=Contacts,dc=truelite,dc=it
cn: Truelite Srl
sn: Srl
mail: info@truelite.it
telephoneNumber: 0557879597
facsimileTelephoneNumber: 0557333336
postalAddress::
VmlhIE1vbmZlcnJhdG8sIDYKRmlyZW56ZSwgRkkgNTAxNDIKSXRhbHk=
labeledURI: http://www.truelite.it
o: Truelite Srl

# Antonio Javier Russo, Contacts, truelite.it
dn: cn=Antonio Javier Russo,ou=Contacts,dc=truelite,dc=it
cn: Antonio Javier Russo
sn: Russo
mobile: 0471XXXXXX
fileAs: Russo, Antonio
mail: russo@indirizzo.fake.it
mail: antonio.russo@no.spamming.allowed.de
o: Associazione Software Libero
title: Coordinatore
```

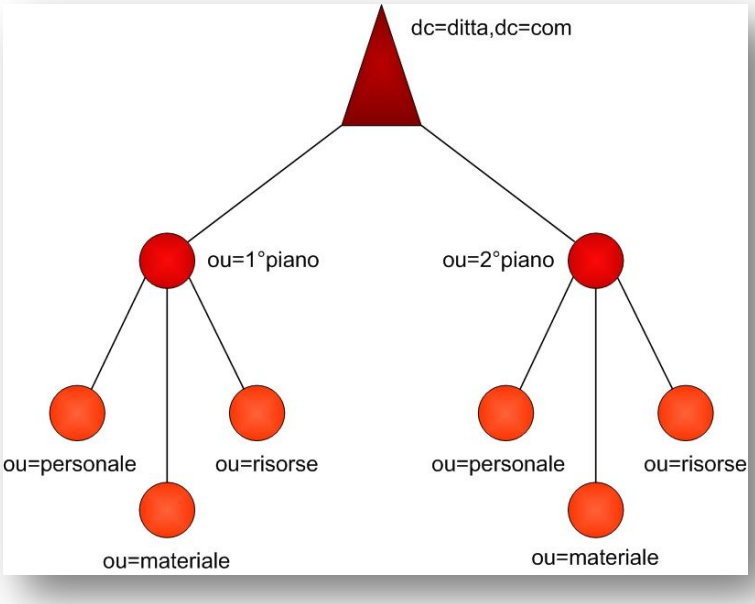
in cui sono definite due voci nella unità operativa Contacts (nel caso utilizzata per mantenere un indirizzario); si noti come trattandosi di voci relative a tipi di dati diversi queste siano realizzate con oggetti diversi, che hanno diversi attributi [3].

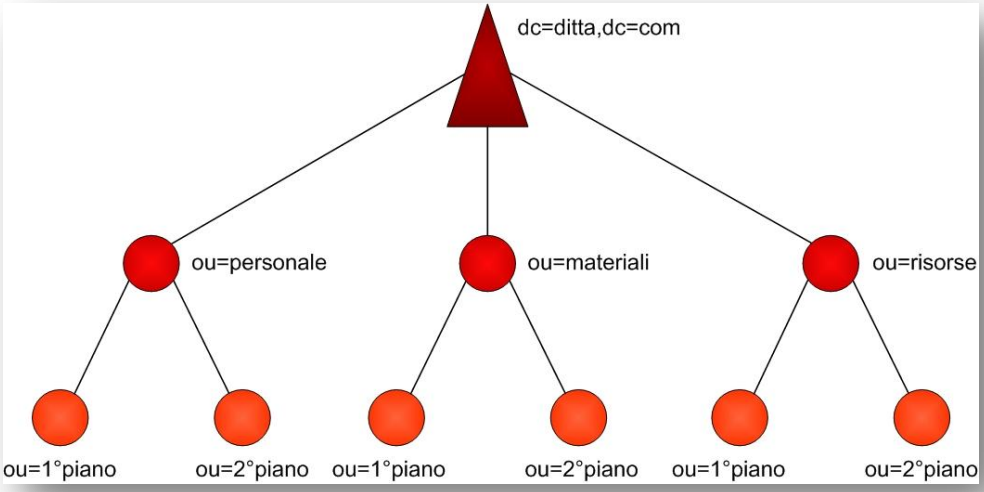
1.13 Disegno del DIT

Vedremo nel proseguio come una directory LDAP possa essere suddivisa in partizioni, ciascuna facente capo ad un server. Per il momento soffermiamoci su quale tipo di gerarchia si debba dare ad una directory LDAP. All'inizio non è facile, o perlomeno immediato, stabilire che tipo di gerarchia mettere in piedi, benché a priori siano note le informazioni che si desidera trattare, i tipi e le modalità di ricerche che saranno richeste e tutti gli schemi necessari. Così come visto per il naming delle radici, anche in questo caso si confrontano due scuole di pensiero:

- Gerarchia per categoria funzionali;
- Gerarchia per categorie omogenee.

In entrambi i casi, visibili nelle immagini seguenti, viene fatto un largo uso di entry di classe `organizationalUnit`, i generici contenitori ai quali si è fatto ricorso precedentemente.





E' comunque consigliabile scegliere tipi di organizzazione dei dati che non siano né troppo superficiali né troppo paeticolareggiati fino alla ingestibilità.

1.14 Filtri e ambienti di ricerca

Benchè raramente avremo a che farecon comandi LDAP diretti (viene fatto largo uso di tool di amministrazione sia a linea di comando che da GUI) la comprensione di parametri quali `base` e `scope` e la sintassi dei filtri sono di grande importanza nell'uso di LDAP e nelle configurazione dei vari plugin dei pacchetti applicativi che lo supportano.

Per la consultazione delle directory ed il recupero delle informazioni mantenute si ricorre all'uso di alcuni paramentri che consentono di specificare in modo semplice *cosa-cercare* e *dove-cercare*:

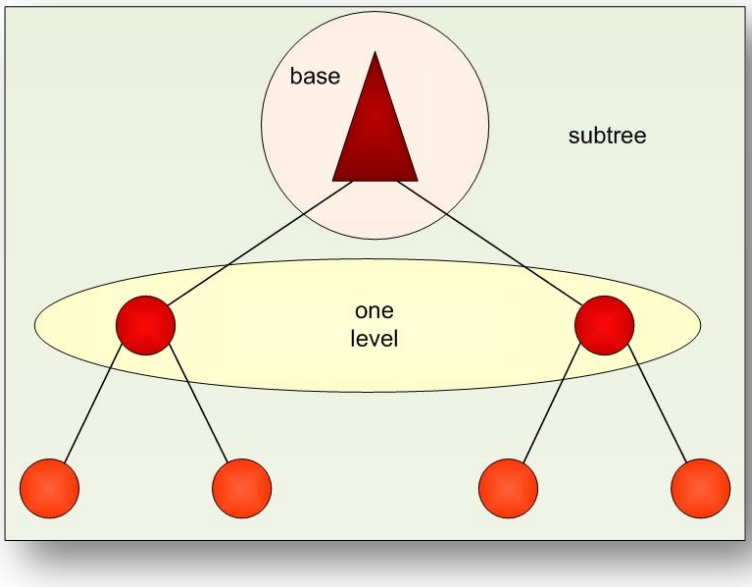
- `base` - da dove inizia la ricerca;
- `scope` - l'abito della ricerca;
- `filter` - i criteri di confronto;

- valori da restituire - ovvero le coppie `<attributo><valore>` che si desidera recuperare (`null` per ottenere tutte le coppie).

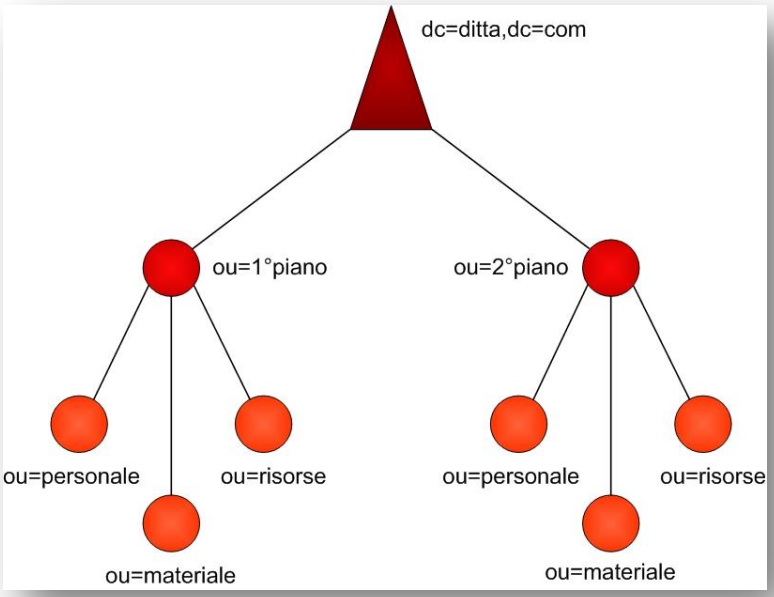
Tramite il valore del parametro scope si specifica l'ambito o la profondità di ricerca che si desidera effettuare.

- `scope = base` solo nella entry specificata;
- `scope = one level` solo nei figli diretti della query specificata con il paramentro base (attenzione: l'entry di base non è ricompresa nel perimetro di ricerca);
- `scope = subtree` nella entry specificata e in tutti i suoi discendenti diretti e indiretti.

E' possibile vedere un esempio nella figura sottostante.



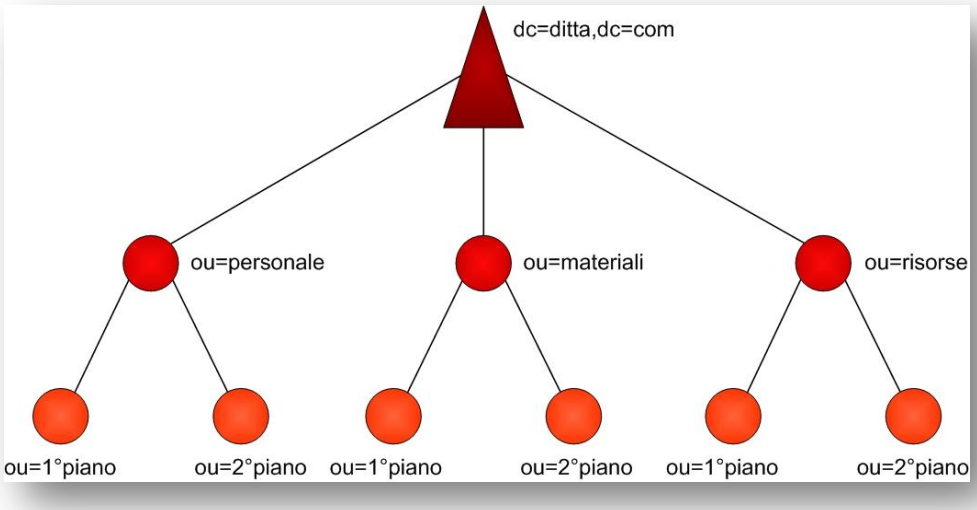
Ad esempio, per la ricerca di tutto il personale nella directory,



dovremo porre:

```
base: dn=ditta,dc=com – scope: subire
```

Nel caso invece fosse stato scelta la gerarchia della figura sottostante:



avremo:

```
base: ou=personale,dc=ditta,dc=com – scope: one level
```

I filtri rappresentano i criteri secondo i quali viene effettuata la ricerca: ogni entry che corrisponde ai filtri indicati verrà restituita. La sintassi dei filtri prevede operatori logici, comparatori (anche di assonanza fonetica) e la wild-card * tutti in notazione prefissa. Ad esempio:

```
il personale del primo piano: (ou=1'piano)
nome Antonio: (|(n=antonio) (cn=antonio))
telefono a Roma: (telephoneNumber=06*)
```

Alla stregua di un DNS, se il server LDAP non è autoritativo per l'albero (o la base) richiesto la ricerca potrà restituire un referral, ovvero un rinvio alla URL del server LDAP al quale ripresentare la richiesta [4].

1.15 Il meccanismo delle interrogazioni LDAP

LDAP nasce come un sistema in grado di offrire dei servizi di elenco a livello globale. Questo significa che, come accade con il meccanismo delle delegazioni del DNS, è possibile suddividere l'albero in maniera che ciascun server possa rispondere per la sua sezione di albero, ottenendo così una distribuzione delle informazioni.

Per poter richiedere le informazioni il protocollo LDAP prevede l'utilizzo di una URL estesa che consenta di eseguire in maniera generale una richiesta ad un server LDAP, questa URL ha una forma generica del tipo:

```
ldap://server/base?attributi?profondità?filtro
```

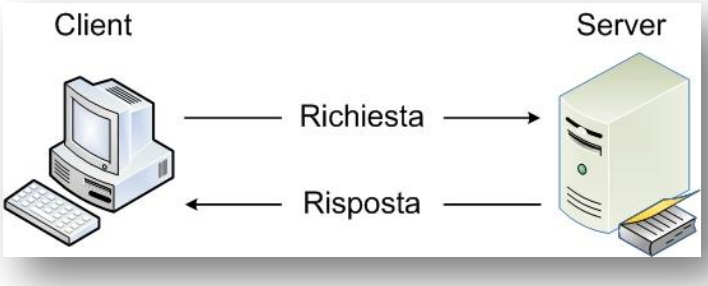
dove la prima parte, che specifica l'indirizzo del server da contattare, è identica a quella di una URL consueta, mentre la seconda parte, che indica la ricerca da effettuare, ha una sua sintassi specifica composta, come mostrato nell'esempio, da diversi elementi separati dal carattere "?".

Il primo elemento è l'indicazione del punto di partenza della ricerca all'interno dell'albero dei dati, la cosiddetta *base* della ricerca; questa deve essere espressa con il suo *Distinguished Name*. Il secondo elemento indica la lista, separata da virgole, dei nomi degli attributi che si intendono cercare, se non specificato verranno restituiti tutti gli attributi presenti. Il terzo elemento è una parola chiave che indica la *profondità* della ricerca e l'ultimo un filtro di ricerca.

Inoltre dato che esistono diverse modalità con cui si può contattare un server, l'identificativo iniziale della URI, oltre a quanto mostrato nell'esempio precedente, può assumere una delle tre forme illustrate nella tabella sottostante, che identificano la modalità con cui collegarsi al server.

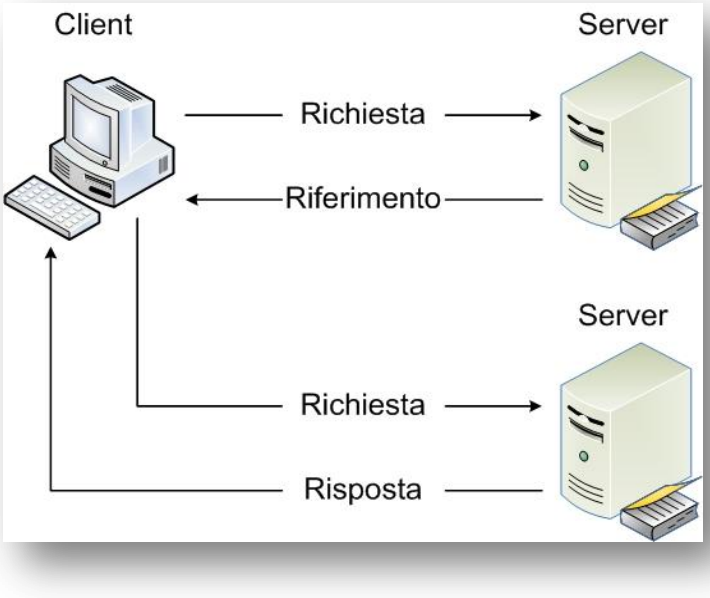
Indicatore	Significato
ldap://	Indica una normale connessione tramite socket
ldaps://	Indica una connessione cifrata con SSL
ldapi://	Indica una connessione ad un socket locale.

Il caso più comune di uso di interrogazione col protocollo LDAP resta quello in cui un client effettua una richiesta ad un server via rete, usando una URL nella forma appena descritta, e ottiene direttamente da questo la risposta, secondo lo schema illustrato. Questo caso ovviamente comporta che il server gestisca i dati relativi alla richiesta; quando si usano delle risorse *locali* questo avviene sempre, e nella nostra analogia con il DNS ciò equivale all'effettuare richieste solo per il dominio di cui siamo direttamente responsabili.



Dato che molto spesso LDAP viene utilizzato solo per mantenere informazioni locali (come una rubrica di indirizzi condivisa) quello della figura precedente è lo scenario di utilizzo più comune, ma benchè ciò sia meno diffuso è possibile uscire dall'ambito locale ed eseguire delle interrogazioni generiche in ambito globale. In questo caso il meccanismo di funzionamento del protocollo è simile a quello del DNS, è necessario cioè inserire il nostro server all'interno di una gerarchia, così che sia possibile redirigere le richieste verso server di livello superiore che possono a loro volta redirigere verso altri server subordinati che mantengano le informazioni che cerchiamo.

La redirezione avviene tramite il meccanismo detto dei *referral*, che si è illustrato nella figura successiva. Si può cioè configurare un server LDAP che fornisce dati per un certo dominio perchè per richieste che escono da detto dominio possa fornire un *riferimento* ad un server di livello superiore in grado di rispondere (o di fornire riferimenti ad altri server). Allo stesso modo un server di livello superiore può redirigere richieste ad altri server sotto di lui che mantengono quella particolare sezione di albero.



La potenza del meccanismo dei *referral* è che, come per il DNS, esso è del tutto trasparente rispetto alle richieste di un client, che riceverà solo la risposta

finale. Ovviamente perchè tutto questo sia possibile occorre, come per il DNS, la presenza di una gerarchia globale di server. Benchè questa funzionalità sia scarsamente utilizzata, una tale gerarchia è possibile.Si tenga presente comunque che anche quando non si è interessati a far parte di un servizio strutturato a livello globale, questa caratteristica di LDAP risulta particolarmente utile in quanto consente, anche all'interno di una singola organizzazione, di suddividere le informazioni (ad esempio relative alle varie divisioni) su server diversi messi in relazione fra loro e mantenuti coerenti in un unico albero grazie alla presenza dei riferimenti [3].

CAPITOLO 2

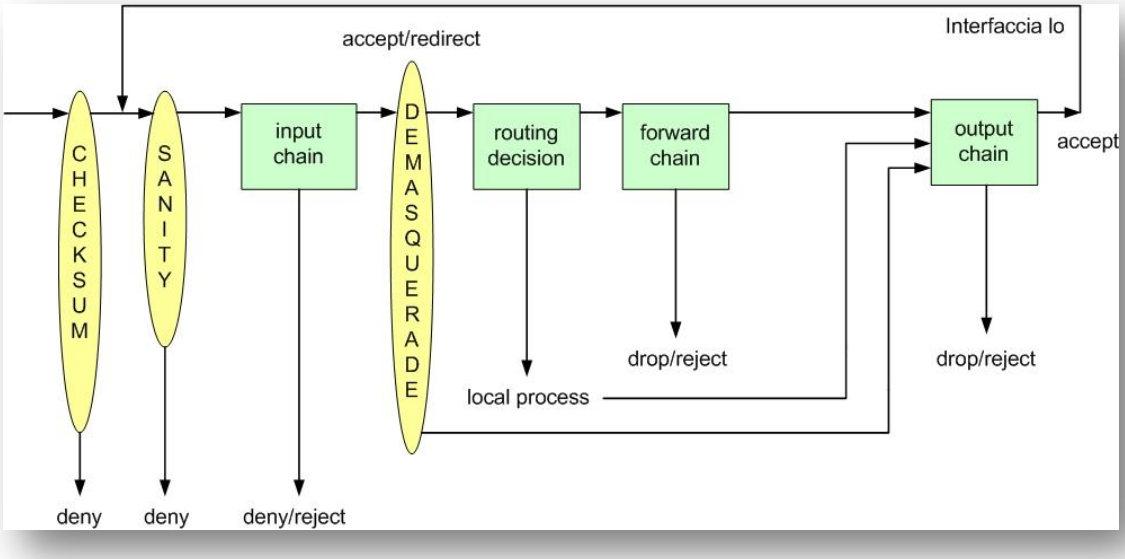
IMPLEMENTAZIONE DI UN SISTEMA PROTETTO DA FIREWALL

2.1 Realizzazione di una Rete con Firewall IPTables

Per proteggere la rete privata in cui ho avuto modo di analizzare il funzionamento delle directory services ho installato e configurato il firewall IPTables.

IPTables è un pacchetto open source operante in ambiente GNU/Linux che utilizza gli strumenti messi a disposizione dai kernel della serie 2.4 e successivi.

Il programma IPTables rappresenta solo un'applicazione in spazio utente. Quando un pacchetto IP entra nel firewall, viene passato al corrispondente driver all'interno del kernel. Quindi il pacchetto attraverserà una serie di stati prima di essere inviato ad un'applicazione locale o inoltrato attraverso un'altra interfaccia di rete.



IPTables è strutturato internamente attraverso delle catene (chains). Un pacchetto, una volta immesso in una di queste, può essere bloccato o accettato, a seconda delle regole impostate dall'utente. Un altro concetto importante è quello di tabella (table). Non appena IPTables viene caricato all'interno del kernel, verranno create tre tabelle e diverse catene già preimpostate [5].

Il firewall che ho attivato ha una configurazione hardware che può essere così riassunta nelle sue componenti principali:

- processore Atlhon 1,8 GHz;
- 512 MB di memoria RAM;
- due schede di rete, una 3Com e l'altra RealTek Ethernet;
- un'hard-disk, da 40 Gb contenete il sistema operativo Linux.

Il sistema operativo installato è Linux, distribuzione Fedora 8, con il kernel versione 2.6.23.1-49 opportunamente configurato.

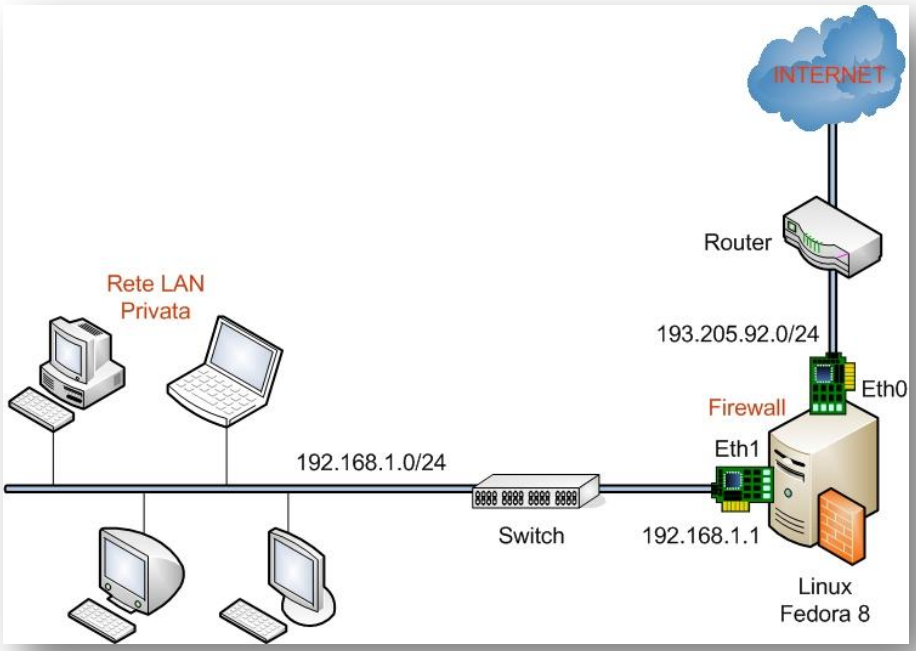
Il sistema Linux conteneva già il pacchetto IPTables necessario per poter configurare un firewall.

Come vedremo in dettaglio nel paragrafo successivo, esiste un solo file di configurazione (`/etc/sysconfig/iptables`) che può essere modificato con un editor testuale o in alternativa configurato e gestito completamente via web, tramite il software Webmin (http://www.webmin.com).

La rete LAN realizzata era collegata all'interfaccia `eth1` del computer e aveva come indirizzi privati `192.168.1.0/24`;

Mente internet era collegata all'interfaccia `eth0` e l'indirizzo gli veniva fornito automaticamente, tramite DHCP.

Lo schema di rete con firewall IPTables realizzato è il seguente:



Per aumentare la sicurezza della rete LAN e creare una rete con indirizzi IP privati, ho implementare il masquerading con la seguente regola:

```
-A POSTROUTING  -o eth0 -s 192.168.1.0/24  -j MASQUERADE
```

Tale regola stabilisce che per qualsiasi pacchetto proveniente dalla rete interna `192.168.1.0/24` e che debba uscire dall'interfaccia `eth0`, deve essere effettuato il mascheramento dell'indirizzo mittente (`-j MASQUERADE`). Grazie ad essa viene effettuta una traduzione da indirizzi privati della rete interna, a indirizzo pubblico e viceversa. Inoltre i computers appartenenti alla rete internet non hanno la possibilità di accedere ai computers appartenenti alla rete interna.

Per rendere operativo il forwarding, ossia lo scambio di pacchetti tra le interfacce di rete, è necessario invocare un file con il parametro 1, in quanto di default Linux non permette che i pacchetti vengano passati tra le diverse interfacce, ovvero:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Quando il valore è `0`, infatti significa che il forward dei pacchetti tra le interfacce è disattivo. Tale comando occorre invocarlo prima che vengano caricate le regole di IPTables [6]. In alternativa per impostare lo stesso valore ad 1 è possibile richiamare il seguente comando da shell:

```
sysctl –w net.ipv4.ip_forward=1
```

Invece per poter visualizzare lo stato del forwarding occorre richimare il seguente comando [7]:

```
sysctl net.ipv4.ip_forward
```

Gli Indirizzi IP alle macchine, reale e virtuale, connesse alla rete LAN privata venivano assegnati tramite un server DHCP. Il file (`/etc/dhcpd.conf`) di configurazione è il seguente:

```
ddns-update-style ad-hoc;
option domain-name-servers 192.168.1.100;
option domain-name "server2003.uninf.it"
default-lease-time 259200;
max-lease-time 518400;

# Configurazione delle Subnet

# Rete Interna
subnet 192.168.1.0 netmask 255.255.255.0 {
      option routers 192.168.1.1;
      range 192.168.1.200 192.168.1.250;
      }
```

Come risulta evidente dal file, il server DNS per la risoluzione dei nomi è all'indirizzo `192.168.1.100`, ossia all'interno della rete privata e il nome del server è `server2003.uninf.it`. Ho specificato inoltre il tempo di *lease* quantificato in tre giorni; che rappresenta il tempo massimo per cui il client può utilizzare l'indirizzo affittato. Inoltre sono evidenti i range degli indirizzi assegnabili ai computer che si connettono alla rete (`Rete Interna`) con il relativo indirizzo IP del option routers [8].

2.2 Configurazione del Firewall

Per poter effettuare la configurazione del firewall è possibile utilizzare due modalità differenti; la prima consiste nello scrivere le regole, presenti nell'appendice, tramite un editor di testo come *Vi*, l'altra invece consiste nel utilizzare una comoda un'interfaccia web come *Webmin*.

2.2.1 Configurazione mediante l'editor Vi

È presente un solo file, `/etc/sysconfig/iptables`, che contiene l'intera configurazione del firewall. Per poter impostare le varie regole, che formano il sistema firewall, ho editato il file citato mediante l'editor *Vi*.

Le politiche di default per le catene di INPUT, OUTPUT e FORWARD sono impostate ad ACCEPT, se non specificato diversamente. Quindi con le seguenti regole ho chiuso tutto il traffico in INPUT, OUTPUT e FORWARD.

```
:FORWARD DROP [0:0]
:INPUT DROP [0:0]
:OUTPUT DROP [0:0]
```

successivamente ho specificato le regole che mi consentissero di far passare solo il tipo di traffico da me stabilito, come risulta evidente dalle regole sottostanti.

Le opzioni che è possibile stabilire per poter definire le regole sono le seguenti:

- -*N* crea una nuova catena;
- -*A* aggiunge una regola ad una catena;
- -*i* consente, in una regola, di discriminare i pacchetti in base all'interfaccia fisica da cui sono entrati;
- -*o* in base all'interfaccia fisica da cui usciranno (scelta in base alle tabelle di routing da noi impostate);

- *-j* di mandare i pacchetti ad un'altra catena.

Abbiamo visto quindi come una regola può identificare dei pacchetti in base alle schede di rete coinvolte. È però possibile utilizzare molti altri criteri, per esempio:

- il protocollo (-p);
- l'indirizzo ip sorgente (-s);
- l'indirizzo ip destinazione (-d);
- se si tratta di un frammento (-f);
- se non lo è (! -f).

Dove ogni protocollo può aggiungere dei criteri di classificazione. Per esempio, se specifichiamo "-p tcp" per indicare il protocollo tcp, possiamo poi dividere i pacchetti in base anche

- alla porta sorgente (–sport);
- alla porta destinazione (–dport);
- ai flag del tcp (–tcp-flags SYN, ACK, FIN...);
- alle opzioni (–tcp-option).

Qui di seguito sono descritte le regole principale, per quanto riguarda la catena di OUTPUT, che fanno parte della configurazione da me realizzata.

```
-A OUTPUT -p TCP -o eth0 --dport 53  -j ACCEPT
-A OUTPUT -p UDP -o eth0 --dport 53  -j ACCEPT
-A OUTPUT -p TCP -o eth0 --dport 443 -j ACCEPT
-A OUTPUT -p TCP -o eth0 --dport 80  -j ACCEPT
```

Il significato della sintassi, delle regole precedenti è il seguente: aggiungi (`-A append`) alla catena di OUTPUT, delle regole per cui se un pacchetto che utilizza il protocollo TCP o UDP (`-p`), uscente dalla scheda di rete `eth0` (`-o`) destinato alle porte `53,80,443` (`--dport`), devono essere accettati (`-j ACCEP`).

Tali regole stabilisco che il computer che implementa il firewall abbia la possibilità di navigare in internet e per questo sono state abilitate la porta 53 per il DNS sia con il protocollo UDP che TCP, la 443 per l'HTTPS e la 80 per l'HTTP.

```
-A OUTPUT -p TCP -o eth1 --dport 53 -j ACCEPT
-A OUTPUT -p UDP -o eth1 --dport 53 -j ACCEPT
-A OUTPUT -p TCP -o eth1 --dport 389 -j ACCEPT
-A OUTPUT -p TCP -o eth1 --dport 636 -j ACCEPT
```

Tali regole stabilisco invece, che occorre aggiungere (`-A append`) alla catena di OUTPUT, delle regole per cui se un pacchetto che utilizza il protocollo TCP o UDP (`-p`), uscente dalla scheda di rete `eth1` (`-o`) destinato alle porte `53,389,636` (`--dport`), devono essere accettati (`-j ACCEP`).

Le regole sovrastanti permettono ai pacchetti provenienti dal DNS e da LDAP siano recapitati ai computers connessi con la rete LAN privata, per questo sono state abilitate le porte 53 per il DNS sia con il protocollo UDP che TCP, la porta 389 per l'LDAP in chiaro e la 636 per l'LDAP protetto da crittografia.

```
-A OUTPUT -p TCP -o eth0 --dport ftp -j ACCEPT
-A OUTPUT -s 0/0 -p tcp ! --syn --sport ftp -j ACCEPT
-A OUTPUT -s 193.205.92.0/24 -p tcp --sport 1024: -d 0/0 --dport 1024: -
j ACCEPT
-A OUTPUT -s 0/0 -p tcp ! --syn --sport 1024: -d 193.205.92.0/24 --dport
1024: -j ACCEPT
```

Le regole sovrastanti invece permettono di poter utilizzare il protocollo FTP (*file trasfer protocol*) per il trasferimento di dati dal computer in cui è implenetato il firewall ad internet e viceversa.

```
-A OUTPUT -p TCP -m state --state RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -p UDP -m state --state RELATED,ESTABLISHED -j ACCEPT
```

Tali regole, possibile solo con IPTables e non con gli altri tipi di firewall, fa in modo che i pacchetti di ritorno, che arrivano al firewall, siano effettivamente associati a una richiesta precedentemente effettuata. Infatti IPTables mantiene lo

stato di tutte le richieste interne.

Qui di seguito sono descritte le regole principale, per quanto riguarda la catena di INPUT.

```
-A INPUT -p TCP -i eth0 --dport 389 -j ACCEPT
-A INPUT -p TCP -i eth0 --dport 636 -j ACCEPT
-A INPUT -p TCP -i eth0 --dport 23384 -j ACCEPT
```

Il significato delle regole precedenti è il seguente: aggiungi (`-A append`) alla catena di INPUT, delle regole per cui se un pacchetto che utilizza il protocollo TCP o UDP (`-p`), entrante dalla scheda di rete `eth0` (`-i`) destinato alle porte `389,636,23384` (`--dport`), devono essere accettati (`-j ACCEP`).

Le regole sovrastanti permettono hai compuets presenti nella rete esterna di poter interrogare LDAP sia in chiaro utilizzando la porta 389 che in modo protetto (*ssl*) utilizzando la porta 636. La porta 23384 invece permette di poter accedere tramite HTTP ad un'interfaccia web con cui poter configurare la *Fedora Directory Server*.

```
-A INPUT -p TCP -i eth1 --dport 80 -j ACCEPT
-A INPUT -p TCP -i eth1 --dport 53 -j ACCEPT
-A INPUT -p UDP -i eth1 --dport 53 -j ACCEPT
-A INPUT -p TCP -i eth1 --dport 443 -j ACCEPT
-A INPUT -p TCP -i eth1 --dport 389 -j ACCEPT
-A INPUT -p TCP -i eth1 --dport 636 -j ACCEPT
-A INPUT -p TCP -i eth1 --dport 23384 -j ACCEP
```

Tali regole stabilisco, che occorre aggiungere (`-A append`) alla catena di INPUT, delle regole per cui se un pacchetto che utilizza il protocollo TCP o UDP (`-p`), entrante dalla scheda di rete `eth1` (`-i`) destinato alle porte `53,80,443,389,636,23384` (`--dport`), devono essere accettati (`-j ACCEP`).

Le regole sovrastanti permettono ai pacchetti provenienti dai computers della rete LAN interna, di essere recapitati al computer in cui è implementato il firewall, per questo sono state abilitate le porte 53 per il DNS sia con il protocollo

UDP che TCP, la porta 80 per l'HTTP, la porta 443 per l'HTTPS, la porta 23384 per la configurazione tramite il protocollo HTTP della *Fedora Directory Server* e le porta 389 e 636 per l'LDAP in chiaro e in modalità protetta da crittografia.

```
-A INPUT -p TCP -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p UDP -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Tali regole, come le stesse regole precedenti, fa in modo che i pacchetti di ritorno, che arrivano al firewall, siano effettivamente associati a una richiesta precedentemente effettuata.

Qui di seguito sono descritte le regole principale, per quanto riguarda la catena di FORWARD.

```
-A FORWARD -p TCP -i eth1 -o eth0 --dport 53 -j ACCEPT
-A FORWARD -p UDP -i eth1 -o eth0 --dport 53 -j ACCEPT
-A FORWARD -p TCP -i eth1 -o eth0 --dport 80 -j ACCEPT
-A FORWARD -p TCP -i eth1 -o eth0 --dport 443 -j ACCEPT
```

Il significato della sintassi, delle regole precedenti è il seguente: aggiungi (`-A append`) alla catena di FORWARD, delle regole per cui se un pacchetto che utilizza il protocollo TCP o UDP (`-p`), entrante dalla scheda di rete `eth1` (`-i`) e uscente dalla scheda di rete `eth0` (`-o`) destinato alle porte `53,80,443` (`--dport`), devono essere accettati (`-j ACCEP`).

Tali regole stabilisco che i computers appartenenti alla rete LAN privata abbiano la possibilità di navigare in internet e per questo sono state abilitate la porta 53 per il DNS sia con il protocollo UDP che TCP, la 443 per l'HTTPS e la 80 per l'HTTP.

```
-A FORWARD -s 0/0 -p tcp ! --syn --sport ftp -j ACCEPT
-A FORWARD -s 192.168.1.0/24 -p tcp --sport 1024: -d 0/0 --dport 1024: -
j ACCEPT
-A FORWARD -s 0/0 -p tcp ! --syn --sport 1024: -d 192.168.1.0/24 --dport
1024: -j ACCEPT
-A FORWARD -p icmp -i eth1 -o eth0 -j ACCEPT
```

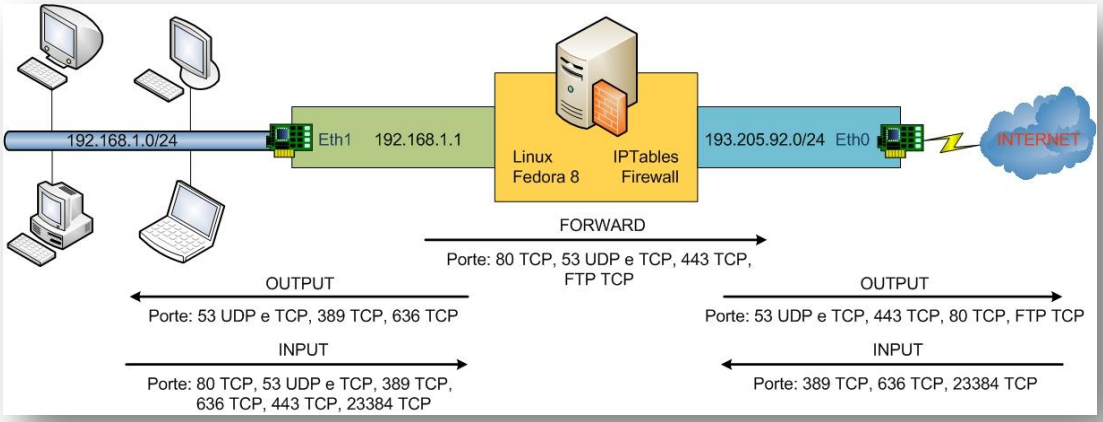
Le regole sovrastanti fanno in modo che la rete privata `192.168.1.0/24` abbia la possibilità di effettuare dei trasferimenti di dati tramite il protocollo ftp (*file trasfer protocol*).

```
-A FORWARD -i eth0 -o eth1 -m state --state ESTABLISHED,RELATED -j
ACCEPT
-A FORWARD -i eth1 -o eth0 -m state --state ESTABLISHED,RELATED -j
ACCEPT
```

Anche in questo caso tali regole, come le regole sovrastanti, fa in modo che i pacchetti di ritorno, siano effettivamente associati a una richiesta precedentemente effettuata.

Il file `/etc/sysconfig/iptables` completo di tutte le regole è presente nell'appendice.

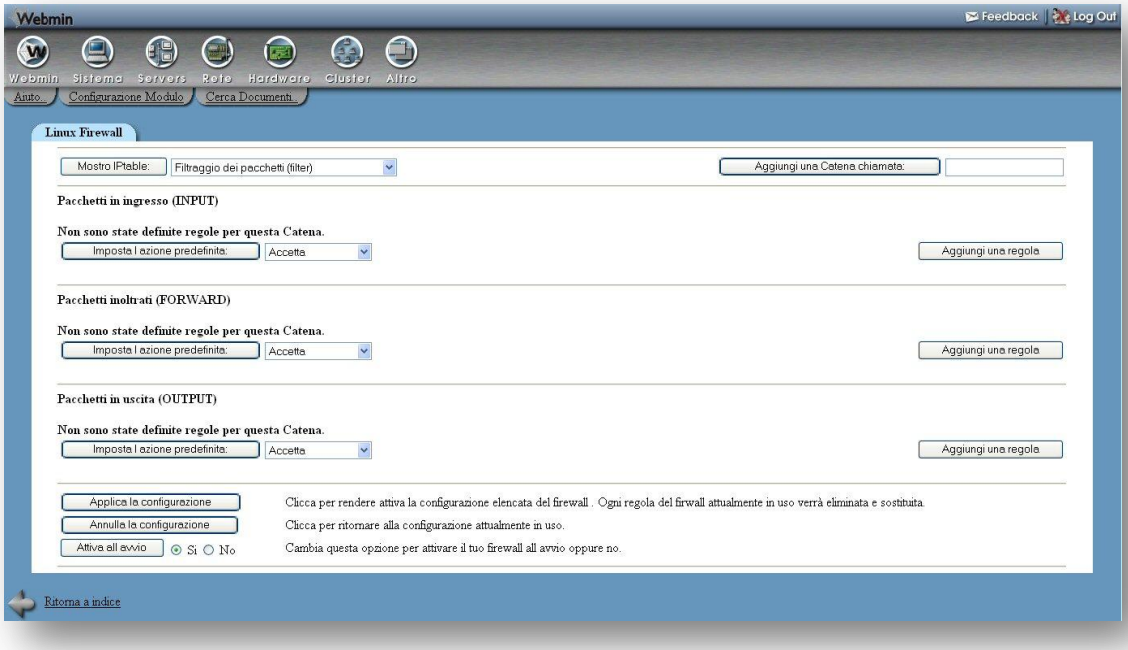
Nella figura sottostante viene riportata una schematizzazione riassuntiva della configurazione del firewall, con le relative porte aperte.



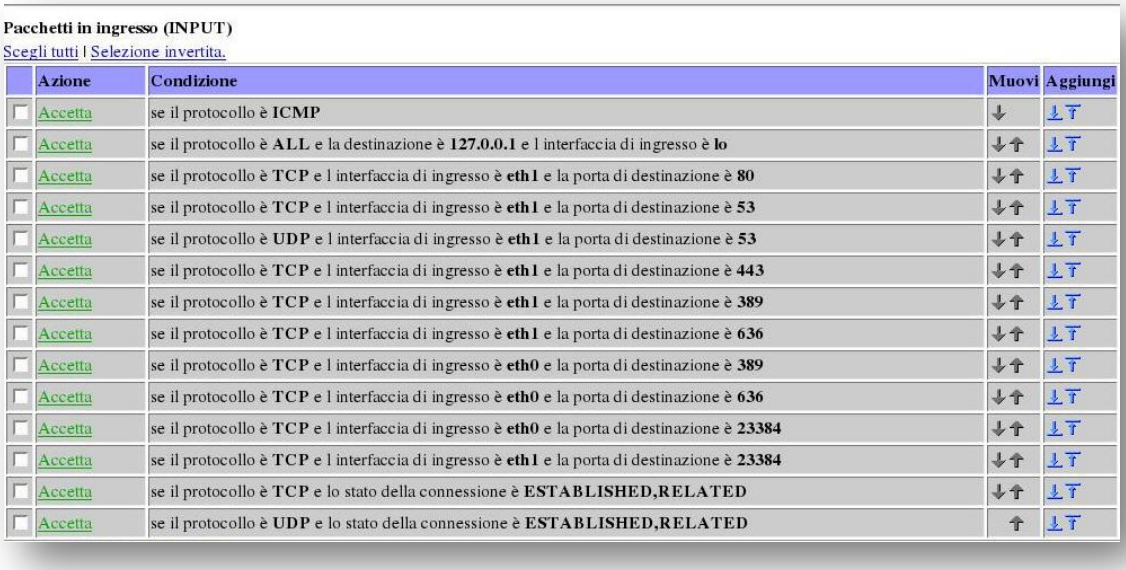
2.2.2 Configurazione mediante Webmin

Webmin, è un sistema modulare per la configurazione di tutte le sfaccettature del proprio OS. Per questo sistema di gestione viene semplicemente utilizzato il Web, per cui l'unica cosa di cui si ha bisogno è un browser, sia esso

testuale (come lynx o links) oppure grafico (come il classico Mozilla, Galeon, Konqueror o Netscape). La sua struttura client-server consente agevolmente l'amministrazione da remoto. Il motore di Webmin è un piccolo webserver (sostituibile tra l'altro da Apache, qualora fosse già presente) che utilizza degli script CGI scritti in perl che si occupano della configurazione del sistema. Questo tipo di approccio rende particolarmente modulare questo programma consentendo di "espanderelo" agevolmente utilizzando dei moduli esterni, alcuni sviluppati direttamente dal team di Webmin, altri da terze parti. Nella figura sottostante viene riportata la schermata iniziale di Webmin che è possibile visualizzare tramite l'url sul browser web: *https://fedora8.uninf.it:10000*, in cui è possibile impostare le regole del firewall per le catene di INPUT, FORWARD e OUTPUT.



Nell'immagine successiva, vengono mostrato le regole, per quanto riguarda la catena dell'INPUT, impostate nella configurazione del firewall.

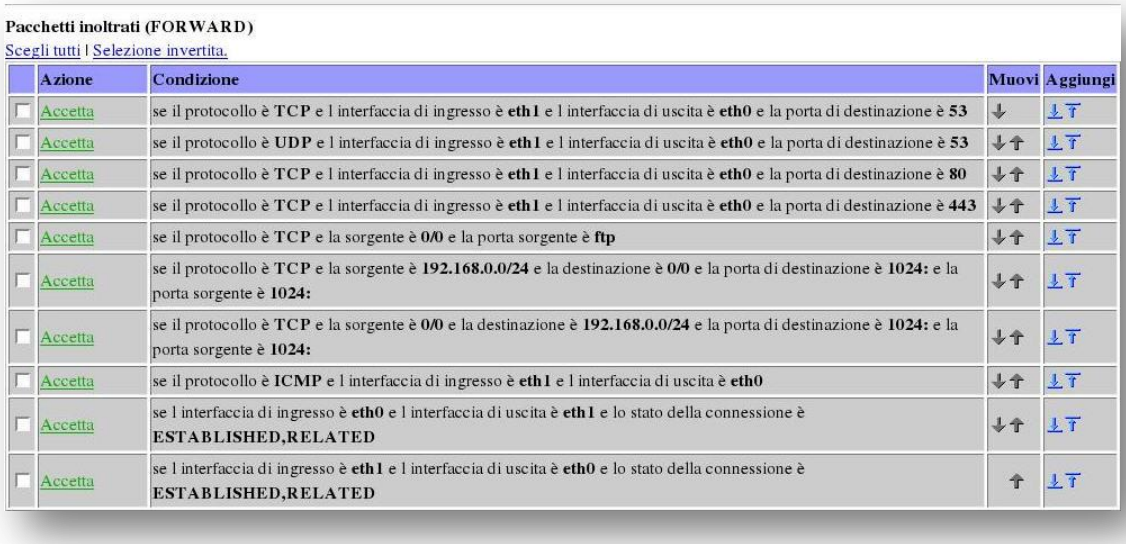


Pacchetti in ingresso (INPUT)

Scegli tutti | Selezione invertita.

	Azione	Condizione	Muovi	Aggiungi
☐	Accetta	se il protocollo è **ICMP**	↓	⊥ T
☐	Accetta	se il protocollo è **ALL** e la destinazione è **127.0.0.1** e l interfaccia di ingresso è **lo**	↓↑	⊥ T
☐	Accetta	se il protocollo è **TCP** e l interfaccia di ingresso è **eth1** e la porta di destinazione è **80**	↓↑	⊥ T
☐	Accetta	se il protocollo è **TCP** e l interfaccia di ingresso è **eth1** e la porta di destinazione è **53**	↓↑	⊥ T
☐	Accetta	se il protocollo è **UDP** e l interfaccia di ingresso è **eth1** e la porta di destinazione è **53**	↓↑	⊥ T
☐	Accetta	se il protocollo è **TCP** e l interfaccia di ingresso è **eth1** e la porta di destinazione è **443**	↓↑	⊥ T
☐	Accetta	se il protocollo è **TCP** e l interfaccia di ingresso è **eth1** e la porta di destinazione è **389**	↓↑	⊥ T
☐	Accetta	se il protocollo è **TCP** e l interfaccia di ingresso è **eth1** e la porta di destinazione è **636**	↓↑	⊥ T
☐	Accetta	se il protocollo è **TCP** e l interfaccia di ingresso è **eth0** e la porta di destinazione è **389**	↓↑	⊥ T
☐	Accetta	se il protocollo è **TCP** e l interfaccia di ingresso è **eth0** e la porta di destinazione è **636**	↓↑	⊥ T
☐	Accetta	se il protocollo è **TCP** e l interfaccia di ingresso è **eth0** e la porta di destinazione è **23384**	↓↑	⊥ T
☐	Accetta	se il protocollo è **TCP** e l interfaccia di ingresso è **eth1** e la porta di destinazione è **23384**	↓↑	⊥ T
☐	Accetta	se il protocollo è **TCP** e lo stato della connessione è **ESTABLISHED,RELATED**	↓↑	⊥ T
☐	Accetta	se il protocollo è **UDP** e lo stato della connessione è **ESTABLISHED,RELATED**	↑	⊥ T

La seguente immagine invece riporta le regole impostate nella catena dell'FORWARD della configurazione del firewall.

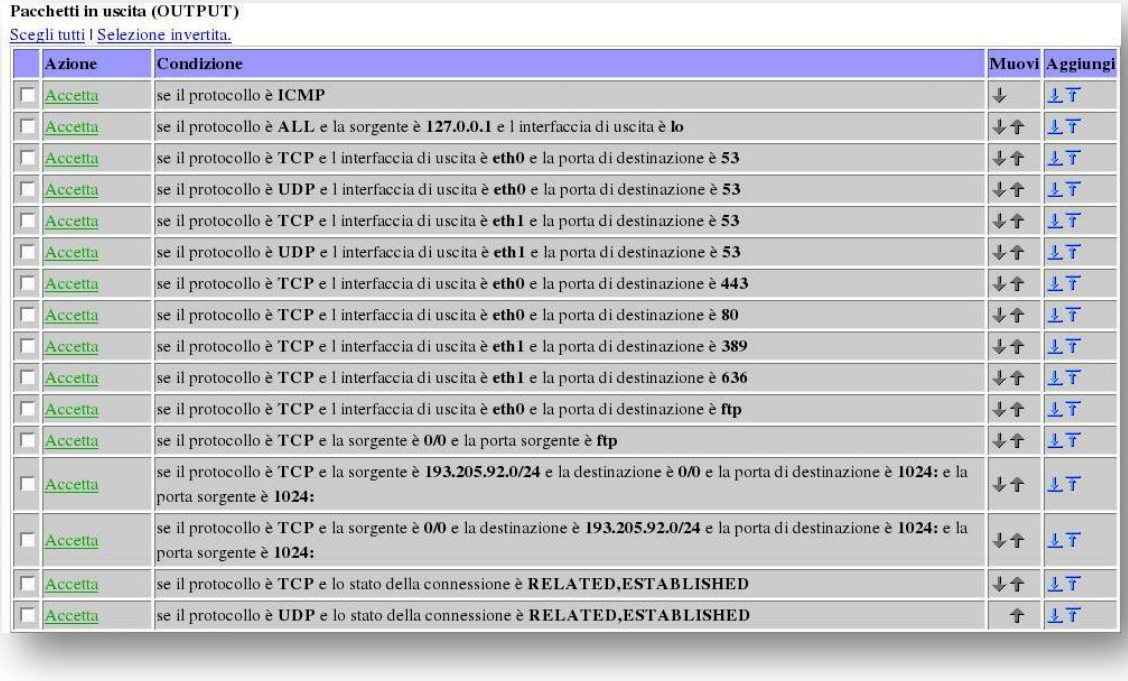


Pacchetti inoltrati (FORWARD)

Scegli tutti | Selezione invertita.

	Azione	Condizione	Muovi	Aggiungi
☐	Accetta	se il protocollo è **TCP** e l interfaccia di ingresso è **eth1** e l interfaccia di uscita è **eth0** e la porta di destinazione è **53**	↓	⊥ T
☐	Accetta	se il protocollo è **UDP** e l interfaccia di ingresso è **eth1** e l interfaccia di uscita è **eth0** e la porta di destinazione è **53**	↓↑	⊥ T
☐	Accetta	se il protocollo è **TCP** e l interfaccia di ingresso è **eth1** e l interfaccia di uscita è **eth0** e la porta di destinazione è **80**	↓↑	⊥ T
☐	Accetta	se il protocollo è **TCP** e l interfaccia di ingresso è **eth1** e l interfaccia di uscita è **eth0** e la porta di destinazione è **443**	↓↑	⊥ T
☐	Accetta	se il protocollo è **TCP** e la sorgente è **0/0** e la porta sorgente è **ftp**	↓↑	⊥ T
☐	Accetta	se il protocollo è **TCP** e la sorgente è **192.168.0.0/24** e la destinazione è **0/0** e la porta di destinazione è **1024:** e la porta sorgente è **1024:**	↓↑	⊥ T
☐	Accetta	se il protocollo è **TCP** e la sorgente è **0/0** e la destinazione è **192.168.0.0/24** e la porta di destinazione è **1024:** e la porta sorgente è **1024:**	↓↑	⊥ T
☐	Accetta	se il protocollo è **ICMP** e l interfaccia di ingresso è **eth1** e l interfaccia di uscita è **eth0**	↓↑	⊥ T
☐	Accetta	se l interfaccia di ingresso è **eth0** e l interfaccia di uscita è **eth1** e lo stato della connessione è **ESTABLISHED,RELATED**	↓↑	⊥ T
☐	Accetta	se l interfaccia di ingresso è **eth1** e l interfaccia di uscita è **eth0** e lo stato della connessione è **ESTABLISHED,RELATED**	↑	⊥ T

L'ultima immagine della schermata iniziale è la seguente, in cui sono riportare le regole relative alla catena di OUTPUT.



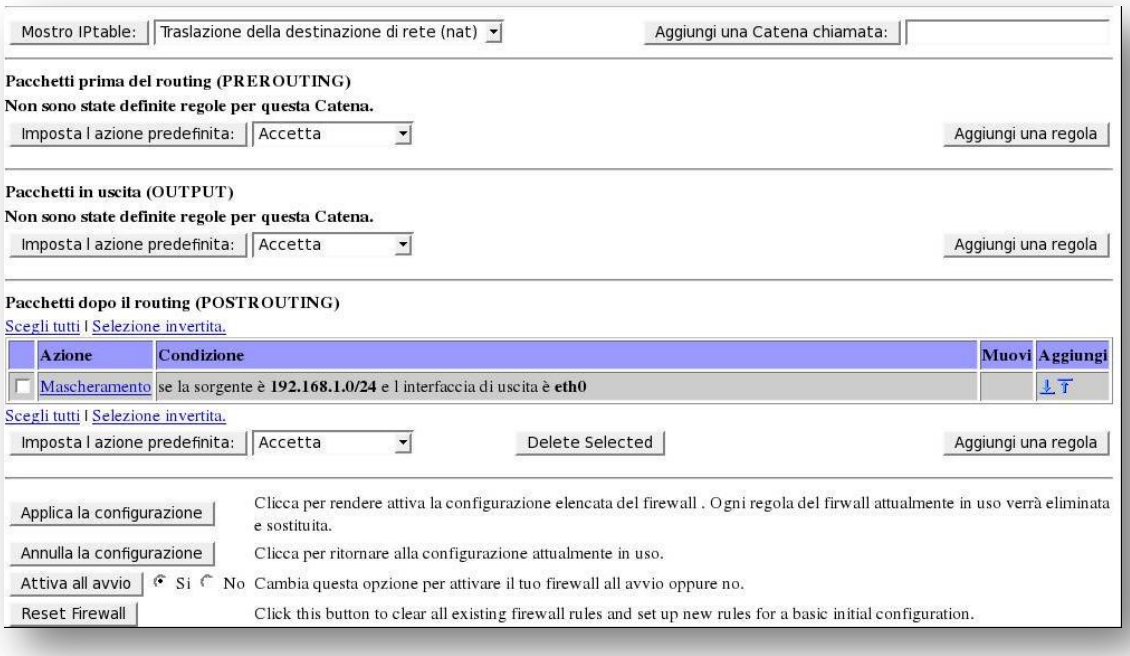
Pacchetti in uscita (OUTPUT)

Scegli tutti | Selezione invertita.

	Azione	Condizione	Muovi	Aggiungi
☐	Accetta	se il protocollo è **ICMP**	↓	⤓ ⤒
☐	Accetta	se il protocollo è **ALL** e la sorgente è **127.0.0.1** e l interfaccia di uscita è **lo**	↓ ↑	⤓ ⤒
☐	Accetta	se il protocollo è **TCP** e l interfaccia di uscita è **eth0** e la porta di destinazione è **53**	↓ ↑	⤓ ⤒
☐	Accetta	se il protocollo è **UDP** e l interfaccia di uscita è **eth0** e la porta di destinazione è **53**	↓ ↑	⤓ ⤒
☐	Accetta	se il protocollo è **TCP** e l interfaccia di uscita è **eth1** e la porta di destinazione è **53**	↓ ↑	⤓ ⤒
☐	Accetta	se il protocollo è **UDP** e l interfaccia di uscita è **eth1** e la porta di destinazione è **53**	↓ ↑	⤓ ⤒
☐	Accetta	se il protocollo è **TCP** e l interfaccia di uscita è **eth0** e la porta di destinazione è **443**	↓ ↑	⤓ ⤒
☐	Accetta	se il protocollo è **TCP** e l interfaccia di uscita è **eth0** e la porta di destinazione è **80**	↓ ↑	⤓ ⤒
☐	Accetta	se il protocollo è **TCP** e l interfaccia di uscita è **eth1** e la porta di destinazione è **389**	↓ ↑	⤓ ⤒
☐	Accetta	se il protocollo è **TCP** e l interfaccia di uscita è **eth1** e la porta di destinazione è **636**	↓ ↑	⤓ ⤒
☐	Accetta	se il protocollo è **TCP** e l interfaccia di uscita è **eth0** e la porta di destinazione è **ftp**	↓ ↑	⤓ ⤒
☐	Accetta	se il protocollo è **TCP** e la sorgente è **0/0** e la porta sorgente è **ftp**	↓ ↑	⤓ ⤒
☐	Accetta	se il protocollo è **TCP** e la sorgente è **193.205.92.0/24** e la destinazione è **0/0** e la porta di destinazione è **1024:** e la porta sorgente è **1024:**	↓ ↑	⤓ ⤒
☐	Accetta	se il protocollo è **TCP** e la sorgente è **0/0** e la destinazione è **193.205.92.0/24** e la porta di destinazione è **1024:** e la porta sorgente è **1024:**	↓ ↑	⤓ ⤒
☐	Accetta	se il protocollo è **TCP** e lo stato della connessione è **RELATED,ESTABLISHED**	↓ ↑	⤓ ⤒
☐	Accetta	se il protocollo è **UDP** e lo stato della connessione è **RELATED,ESTABLISHED**	↑	⤓ ⤒

L'immagine successiva invece riporta la configurazione della regola, riportata di seguito, relativa al Masquerading.

```
-A POSTROUTING  -o eth0 -s 192.168.1.0/24  -j MASQUERADE
```



Mostro IPtable: Traslazione della destinazione di rete (nat) — Aggiungi una Catena chiamata:

Pacchetti prima del routing (PREROUTING)

Non sono state definite regole per questa Catena.

Imposta l azione predefinita: Accetta — Aggiungi una regola

Pacchetti in uscita (OUTPUT)

Non sono state definite regole per questa Catena.

Imposta l azione predefinita: Accetta — Aggiungi una regola

Pacchetti dopo il routing (POSTROUTING)

Scegli tutti | Selezione invertita.

	Azione	Condizione	Muovi	Aggiungi
☐	Mascheramento	se la sorgente è **192.168.1.0/24** e l interfaccia di uscita è **eth0**		⤓ ⤒

Scegli tutti | Selezione invertita.

Imposta l azione predefinita: Accetta — Delete Selected — Aggiungi una regola

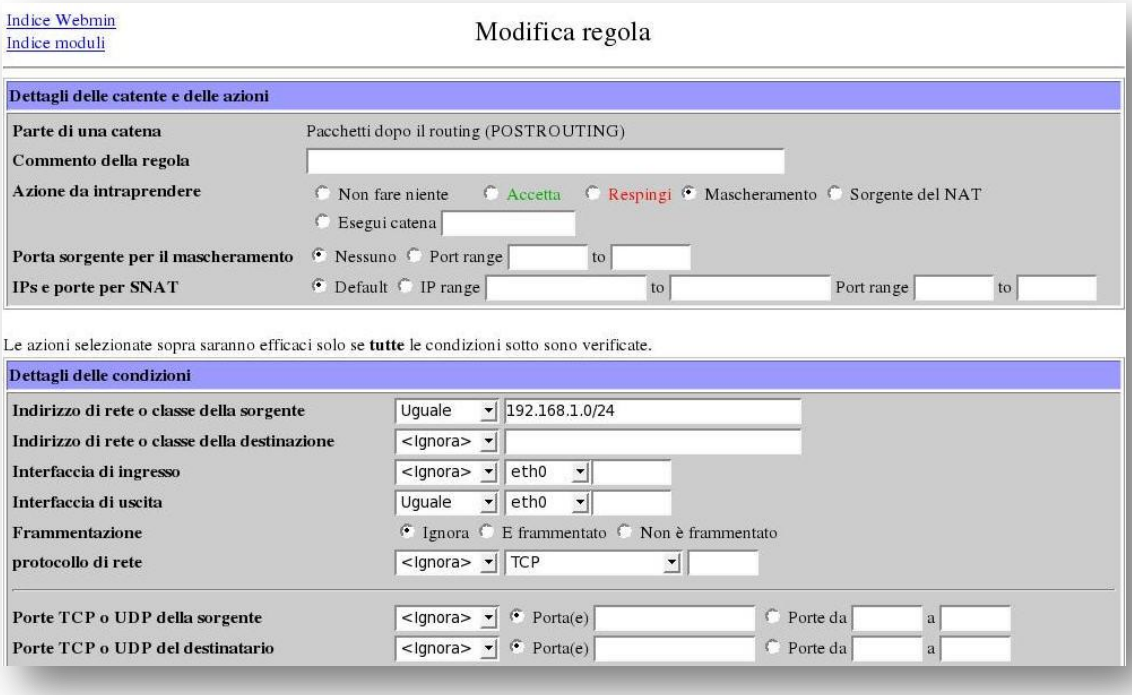
Applica la configurazione — Clicca per rendere attiva la configurazione elencata del firewall . Ogni regola del firwall attualmente in uso verrà eliminata e sostituita.

Annulla la configurazione — Clicca per ritornare alla configurazione attualmente in uso.

Attiva all avvio ◉ Si ○ No — Cambia questa opzione per attivare il tuo firewall all avvio oppure no.

Reset Firewall — Click this button to clear all existing firewall rules and set up new rules for a basic initial configuration.

Vediamo invece nell'immagine successiva la schermata, sempre relativa a Webmin, con il quale è possibile realizzare e modificare regole per il firewall, in particolare la regola per il NAT precedentemente vista.



L'ultima schermata visibile riporta invece una regola relativa alla catena di FORWARDING per fare in modo che i computers connessi alla rete LAN privata abbia la possibilità di navigare nel web.

```
-A FORWARD -p TCP -i eth1 -o eth0 --dport 80 -j ACCEPT
```

2.2.3 Logging con IPTables

È possibile tenere traccia dei pacchetti che attraversa il firewall IPTables utilizzando la seguente regola:

```
-A INPUT -m limit --limit 50/minute --limit-burst 3 -j LOG --log-level
debug
```

Il significato della sintassi, della regola precedente è il seguente: aggiungi (`-A append`) alla catena di INPUT, `-m limit --limit 50/minute` stabilisce il *maximum average matching rate* impostato a 50 minuti `--limit-burst 3` che riduce il numero di match ad un certo limite per secondo. In definitiva le due opzioni stabiliscono che il numero massimo di pacchetti, da controllare e quindi inserire nel file di log (`-j LOG`), è di 3 ogni 50 minuti. Tali opzioni sono comodissime col target LOG perché diminuisce la produzione dei log. Mentre l'opzione `--log-level debug` stabilisce la priorità da associare al relativo messaggio di log ossia di debug. In questo caso il kernel registrerà i pacchetti che passeranno attraverso la catena di INPUT e li associerà ad una chiamata `printk()`. L'output sarà memorizzato nel file di log di linux, simile al seguente formato:

```
Nov 18 14:51:12 localhost kernel: IN=eth0 OUT=
MAC=ff:ff:ff:ff:ff:ff:00:00:e2:76:d4:0d:08:00 SRC=193.205.92.189
DST=193.205.92.255 LEN=229 TOS=0x00 PREC=0x00 TTL=128 ID=31213 PROTO=UDP
SPT=138 DPT=138 LEN=209
```

ovviamente se si imposta un log level più o meno alto è possibile ottenere rispettivamente più o meno informazioni.

Un altro metodo per loggare le informazioni, del traffico scartato, è la seguente:

```
-A INPUT -p icmp -j LOG --log-prefix "ICMP drop:"
-A INPUT -p icmp -j DROP
```

Tali regole indicano al kernel di scrivere nel file di log un messaggio con il prefisso “ICMP drop:” che identificano i pacchetti ICMP che vengono scartati. Ciò permette di individurare i ping effettuati verso il server. L’output memorizzato nel file di log sarà simile al seguente formato:

```
Nov 18 14:55:30 localhost kernel: ICMP drop:IN=eth0 OUT=
MAC=00:50:ba:5c:f2:1a:00:a0:d1:b6:4e:6f:08:00 SRC=193.205.92.229
DST=193.205.92.69 LEN=60 TOS=0x00 PREC=0x00 TTL=128 ID=20950 PROTO=ICMP
TYPE=8 CODE=0 ID=512 SEQ=1792
```

I messaggi di log precedenti contengono le seguenti informazioni:

- Data e ora del log;
- Nome del server (srv in questo caso);
- kernel: messaggio impostato con il parametero --log-prefix "messaggio";
- IN=nome interfaccia;
- OUT=nome interfaccia;
- MAC=Mac address della scheda;
- SRC=ip sorgente del pacchetto;
- DST=ip di destinazione;
- LEN=lunghezza;
- TOS=valore ToS (prossimamente spiegherò questo tipo di parametrizzazione per la lunghezza e l'ampiezza di banda);
- Proto=protocollo utilizzato (TCP,UDP,ICMP ....)
- SPT: Porta utilizzata dall'indirizzo chiamante;
- DPT: Porta richiesta sulla scheda di rete dall'indirizzo chiamante;

e poi tutti i vari flag.

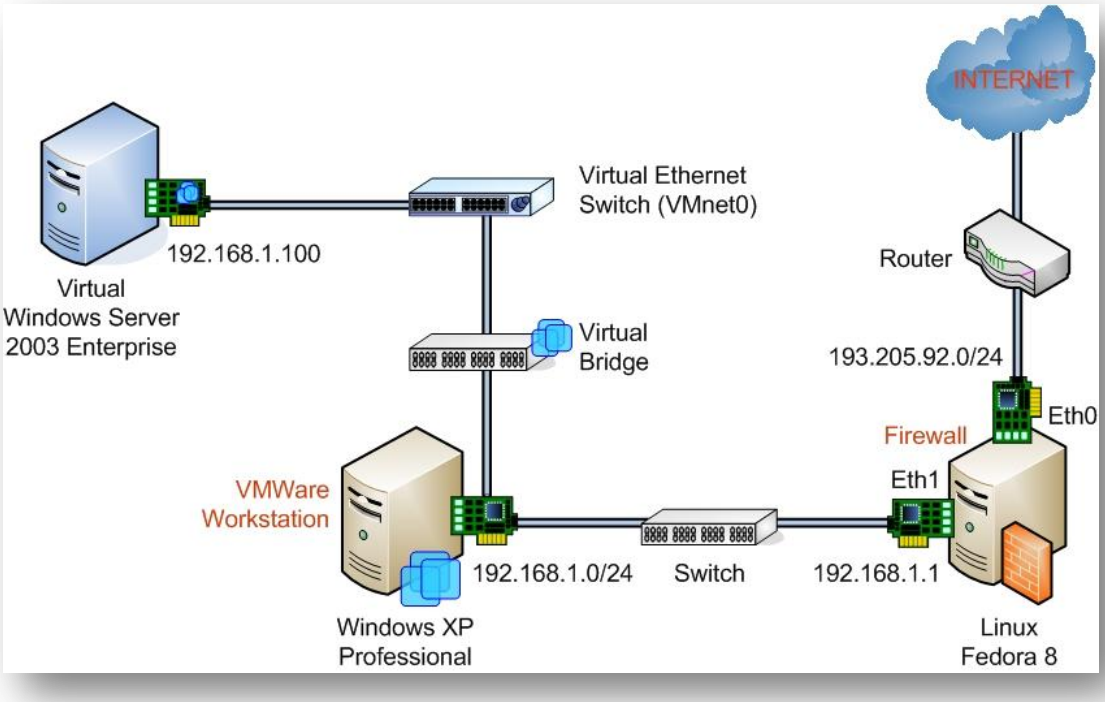
Solitamente il file di log in cui vengono salvate tali informazioni è `/var/log/messages` tale file è presente sulla root del sistema [9].

2.3 Configurazione di una Macchina Virtuale VMware.

Come client presente nella rete LAN privata ho utilizzato un notebook con le seguenti caratteristiche:

- processore Pentium 4 3,06 GHz;
- 1 GB di memoria RAM;
- una schede di rete, SiS 900-Based PCI Fast Ethernet Adapter;
- un'hard-disk, da 80 Gb contenete il sistema operativo Windows XP Professional.

Come risulta evidente dallo schema sottostante in cui è riportato l'intero sistema utilizzato, composto da due macchine e tre diversi sistemi operativi.



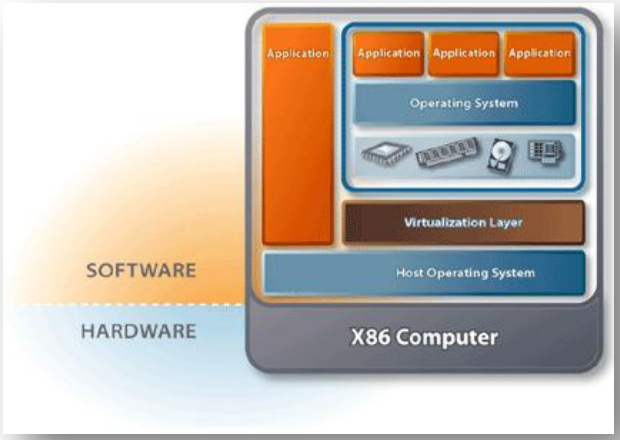
La macchina client nella rete privata riceve le impostazioni di rete automaticamente, tramite DHCP configurato sulla macchina Linux. Come risulta evidente dal file di configurazione del DHCP (`/etc/dhcpd.conf`), essendo l'unica macchina presente, riceverà i seguenti parametri dal server DHCP.

```
Indirizzo IP: 192.168.1.250
Subnet mask: 255.255.255.0
Gateway predefinito: 192.168.1.1
Server DNS preferito: 192.168.1.100
```

Come risulta evidente l'indirizzo IP appartiene al range degli indirizzi, impostato sul file di configurazione del DHCP. Per quando riguarda inverce l'indirizzo IP del gateway predefinito appartiene alla macchina Linux configurata, con il firewall; mentre l'indirizzo IP del DNS preferito è della macchina virtuale, in esecuzione sul client, ed esegue il sistema operativo Windows Server 2003. Infatti l'IP della macchina virtuale è statico e non impostabile automaticamente dal DHCP.

2.3.1 Configurazione della Macchina Virtuale

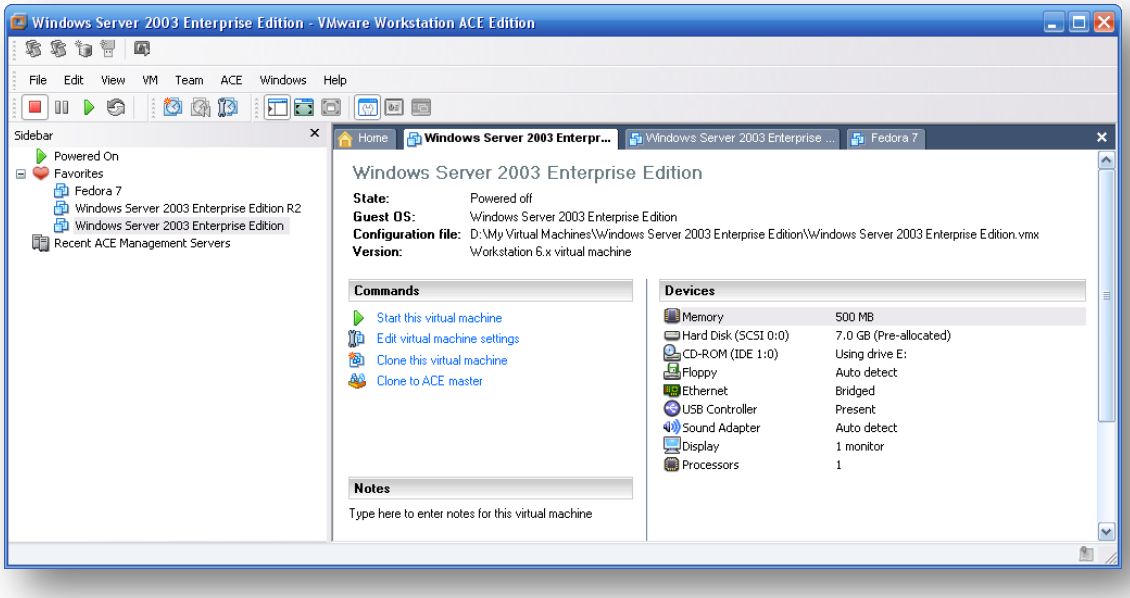
VMware è un software multi-piattaforma per la virtualizzazione dei sistemi, per ambienti di sviluppo professionali e per il consolidamento e partizionamento di ambienti server ad alte prestazioni. La virtualizzazione sta trasformando le modalità di sviluppo dei software e delle infrastrutture IT ed è diventata lo standard per i professionisti IT world-wide. Un'infrastruttura virtuale genera benefici immediati: semplifica e accelera lo sviluppo, i test e il rilascio di software e infrastrutture, aumentando la produttività e la qualità dei progetti; partiziona e isola i server in macchine virtuali sicure e trasportabili, ciascuna delle quali può eseguire un sistema operativo diverso (tra cui Windows, Linux, Netware). Qualunque sistema operativo in ambiente VMware Workstation può essere rapidamente trasferito ed eseguito su un'altra macchina (il tempo che occorre è quello per la copia di un file), rendendo estremamente flessibili e low-cost gli ambienti di sviluppo, test e produzione.



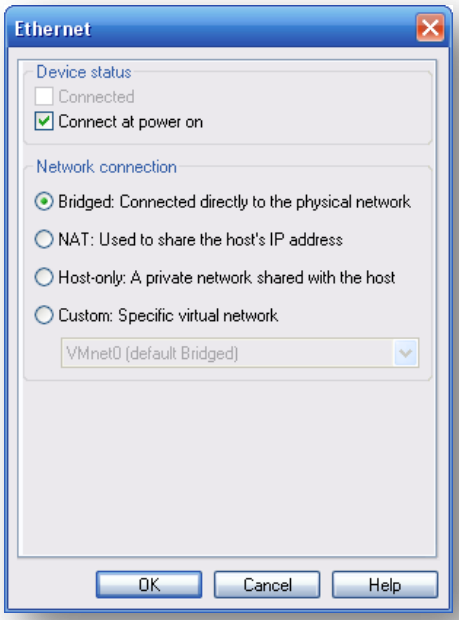
Si hanno a disposizione in questo modo una serie di di computer virtuali in una configurazione sicura, personalizzabile e ad alta efficienza. VMware Workstation aumenta la produttività nell'uso professionale del PC perchè gli operatori I.T. spendono meno tempo a configurare l'ambiente hardware, a installare pacchetti software, o a riavviare il computer.

L'interfaccia semplice, simula tutte le funzionalità dell'hardware (accensione, spegnimento, reset) e permette la configurazione di alcune caratteristiche della macchina virtuale (p.es. memoria, dimensione del disco) a patto naturalmente di rimanere sotto le reali risorse a disposizione. Tutta la macchina virtuale è salvata su un file, garantendone in questo modo portabilità e facilià di ripristino[10][11].

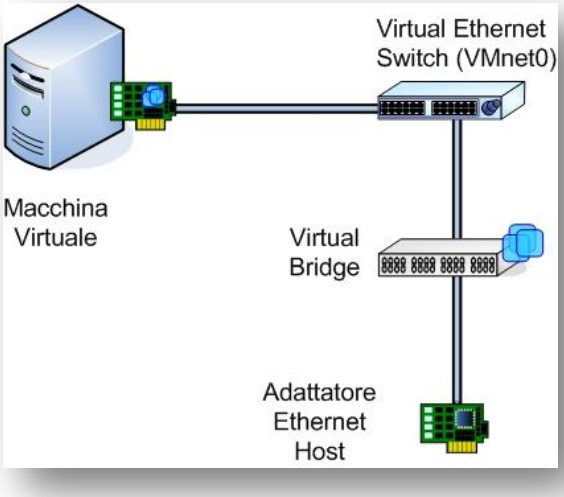
Nella computer interno alla rete LAN privata, ho avuto modo di installare il software precedentemente descritto e il sistema operativo virtuale, Windows Server 2003 Enterprise Edition. Per una fluida esecuzione del sistema operativo ho riservato alla macchina virtuale le seguenti risorse, visibili nell'immagine successiva.



Le impostazioni più importanti nella precedente configurazione riguardano le impostazioni per la rete virtuale, che sono visibili nell'immagine successiva.

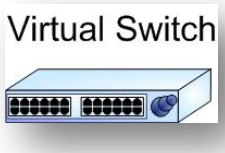


Con le seguenti impostazioni viene creata la seguente configurazione per fornire al sistema operativo virtuale una connettività simile ad una macchina reale connesa alla rete LAN.



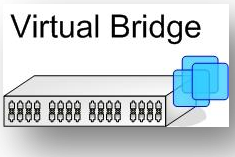
Il tipo di networking bridged è quello selezionato di default quando si crea una macchina virtuale con l'apposito Wizard. E' il modo più semplice per dare accesso alle rete a una macchina virtuale. E' possibile utilizzare questo modello sia con scheda fisica dell'host Ethernet sia con scheda Wi-Fi. Configurata con questa modalità una macchina virtuale deve avere la propria identità sulla rete e quindi deve necessariamente avere un indirizzo IP valido. Genericamente il sistema operativo guest riceverà un indirizzo IP dal DHCP configurato eventualmente su quel segmento LAN. Questa configurazione permette alla macchina virtuale di partecipare in pieno alla rete, accedere alle condivisioni, condividere documenti e fornire servizi esattamente come se fosse una macchina fisica.

Nello schema dell'immagine precedente sono riportati i seguenti componenti di una rete virtuale secondo la terminologia di vmware.

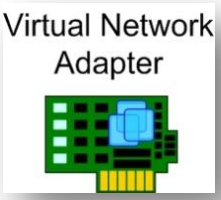


Allo stesso modo di uno switch fisico un virtual switch permette di collegare tra di loro tutti i componenti della rete. Vengono identificati come VMNETx dove x è il numero progressivo. E' possibile creare su un sistema host Windows fino a

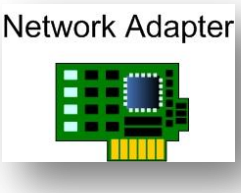
10 virtual switch. Alcuni switch virtuali sono creati al momento dell'installazione; ad esempio la bridged network usa di default *VMnet0*, la host-only network usa *VMnet1* e la NAT network usa di default *VMnet8*. E' possibile creare altri VMnet a seconda delle necessità.



Il bridge permette di collegare una virtual machine alla LAN usata dal computer host, ovvero quello che esegue vmware workstation. Connette la scheda di rete virtuale alla scheda di rete fisica. Il bridge è installato automaticamente durante il setup. E' possibile creare più bridge per utilizzarli in configurazioni personalizzate con più di una scheda di rete fisica sul server host.



E' la scheda di rete virtuale montata su una macchina virtuale. Appare al sistema operativo guest come una AMD PCNET PCI adapter.



E' la scheda di rete fisica del server host. Possono esserne presenti più di una per garantire una fault tolerance e per connettere in diverso modo una macchina virtuale alla rete [12].

La macchina virtuale con installato il sistema operativo Windows server 2003 Enterprise Edition, ha assegnato un'indirizzo IP statico, questo perché, per far funzionare adeguatamente il server DNS e Active Directory, l'indirizzo IP deve essere per forza statico e anche per il fatto che le altre macchine reali della rete effettuano interrogazioni al server DNS configurato sulla macchina virtuale. I parametri configurati manualmente sono i seguenti.

```
Indirizzo IP: 192.168.1.100
Subnet mask: 255.255.255.0
Gateway predefinito: 192.168.1.1
Server DNS preferito: 192.168.1.100
```

Come risulta evidente, l'indirizzo IP non appartiene al range degli indirizzi, impostato sul file di configurazione del DHCP, ma comunque è un'indirizzo valido nella rete LAN privata. Invece per quanto riguarda l'indirizzo IP del gateway predefinito, esso appartiene della macchina Linux configurata, con il firewall; mentre l'indirizzo IP del DNS preferito è della stessa macchina virtuale, in esecuzione sul client.

CAPITOLO 3

ACTIVE DIRECTORY COME DIRECTORY SERVICE

3.1 Active Directory

Un directory service è un servizio che restituisce informazioni a seguito di una specifica richiesta fornita secondo una sintassi convenuta. Le informazioni di un directory service vengono conservate in una base dati secondo una qualche logica organizzativa, ad esempio come nodi di un albero distribuiti localmente o geograficamente, oppure come tabelle, oppure come semplici file; ogni logica aderisce a modelli caratteristici e fornisce specifici vantaggi. Seguendo una certa terminologia potremmo dire che un directory service è un programma "un agente" che ha il compito di introdurre, conservare e reperire informazioni mantenute all'interno di una base di dati, offrendo al cliente metodi per la manipolazione degli stessi; a questo scopo il directory service deve fornire un modello di accesso ai dati efficace in grado di mantenere il database consistente. Naturalmente una base di dati può essere conservata in modo assolutamente centralizzato (alcune basi di dati esposte dai web server lo sono), oppure ripartita su differenti punti di rete connessi tra loro da agenti cooperanti (i DNS internet sono un esempio tipico di base dati e al tempo stesso di servizio distribuito di questo tipo); in quest'ultimo caso i dati dovranno essere distribuiti e replicati secondo una qualche logica che ne preservi la consistenza e successivamente ricostruiti secondo la visione unitaria che il cliente ha dei medesimi. Un'implementazione di directory service nota è Active Directory, ampiamente ispirata al modello X.500 e fondata su LDAPv3 e LDAPv2 (RFC2251, et altera). In Active Directory la logica per la manipolazione dei dati e la loro logica di rappresentazione posseggono alcuni punti di intersezione (sono ovviamente collegati) ma fondamentalmente aderiscono a definizioni ortogonali e separate; Microsoft, pur appoggiandosi al modello LDAP per la manipolazione, utilizza una

metafora ad oggetti per rappresentare i medesimi, seguendo quella che è la tendenza più moderna per la definizione delle basi di dati.

3.2 Directory Service: a deeper view.

Active Directory è un directory service che assolve anche a funzioni di security database (database di password). Il Domain Controller (DC) grazie alla Active Directory fornisce un singolo punto di autenticazione (Single Sign On, SSO), permettendo di centralizzare l'utenza e garantendo una visione degli utenti all'interno del dominio coerente e indipendente dal luogo di autenticazione; ma permette anche di conservare informazioni di svariato tipo che possono essere condivise tra gli utenti o tra le applicazioni distribuite di dominio, al fine di essere reperite e utilizzate. In definitiva Active Directory costituisce una componente importante e complessa del dominio. Active Directory definisce il dominio "per sè" (cosa), il suo boundary di autenticazione (dove) e il suo boundary di sicurezza (chi); questo per dare un definizione funzionale o, per così dire, di "alto livello" di questo servizio. Per dare un definizione architetturale, o di "basso livello", Active Directory è un directory service partizionato, distribuito, replicato, sicuro e ad oggetti. Cercheremo di descrivere di seguito ciascuna di queste caratteristiche, addentrandoci prima nei dettagli architetturali per meglio capire le singole funzionalità.

3.2.1 Active Directory è un directory service

Active Directory è un directory service, vale a dire un servizio che fornisce informazioni specifiche contenute nella base di dati, in risposta a query ben formate. Il protocollo LDAP permette di interloquire con AD a questo fine, per creare, modificare e ottenere informazioni.

3.2.2 Active Directory Partizionato

Un directory service AD è una collezione di *namespace*, altrimenti detti *partizioni* o *Naming Context*; ogni partizione permette sostanzialmente di identificare una parte del directory service. All'interno di una partizione possono essere conservati gli elementi della AD (oggetti); gli oggetti della AD sono essi stessi informazioni o contengono informazioni al proprio interno sotto forma di attributi.

3.2.3 Active Directory ad Oggetti

Active Directory fornisce una visione ad oggetti di tutto ciò che contiene; gli elementi costitutivi della AD sono oggetti composti semplicemente da attributi. Oggetti e attributi sono istanze di astrazioni, in parole povere sono istanze di classi predefinite e contenuti all'interno di una particolare partizione della directory detta Schema; come vedremo lo stesso Schema è un oggetto e anche i dati in esso contenuti sono oggetti: lo schema usa gli oggetti per definire le sue stesse astrazioni.

3.2.4 Active Directory Distribuito

Le partizioni non hanno vincoli sulla loro posizione, possono essere collocate anche su differenti Domain Controller (DC), ma sono connesse tra loro secondo una logica di riferimenti detta *knowledge* che permette di ricostruire la struttura stessa della directory.

3.2.5 Active Directory Replicato

Alcuni dati, alcuni oggetti, all'interno di una foresta sono di tipo globale (interessano tutta la foresta) altri sono di tipo locale (interessano il dominio). I dati globali vengono replicati (shadowing) su tutti i DC della foresta per garantire migliori prestazioni; i dati locali possono essere collocati su più di un DC per

motivi di fault tolerance e load balancing. Inoltre, per permettere di reperire informazioni in modo efficace, un servizio detto Global Catalog raccoglie ed espone alcuni tipi di dati provenienti da tutta la foresta. Molti tipi di dati quindi devono essere replicati nelle foresta passando da DC a DC e questa operazione deve essere effettuata in modo sicuro, consistente ed efficiente.

3.2.6 Active Directory è sicuro

Active Directory richiede l'autenticazione prima di permettere l'accesso alla sua base di dati e supporta l'autorizzazione per le operazioni di lettura e scrittura sui propri dati: Discretionary Access Control List (analoghe a quelle usate per file system NTFS) sono associate ad ogni oggetto della AD ai fini di garantire un accesso controllato e una migliore amministrazione.

3.2.7 Active Directory rappresenta il dominio

Nonostante la dicitura "directory service", lo scopo nativo di AD è rappresentare il dominio e mantenere il database delle password; questo significa che AD può essere usato anche come directory service. In sintesi, AD è un directory service che può assolvere a differenti scopi, ma quando viene installato aggiunge funzionalità necessarie a rappresentare il dominio; questa funzione non contrasta con la sua natura di directory service, ma la integra.

3.2.8 Active Directory, Ldap Server e DSA

I Domain Controller dei domini Microsoft sono degli ldap server, ma non solo. Il protocollo di elezione per l'interrogazione, la modifica e l'inserzione dei dati della Active Directory è LDAP, definito nelle RFC 1777 (LDAPv2), RFC 2251, 2252, 2253, 2254, 2256, et altera (LDAPv3). LDAPv2 è stato usato da Microsoft per il directory service di Exchange 5.x; LDAPv3 è utilizzato per AD e per Exchange 2000 (che è integrato con AD). Altri protocolli permettono l'interazione con il directory service: il DSA (Directory System Agent), il cuore

operativo della AD, espone differenti interfacce per permetterne l'uso.

Verranno analizzate ora con maggior dettaglio ciascuna delle parti definite precedentemente.

3.3 Active Directory è un directory service

Un directory service espone informazioni; in particolare AD espone informazioni reperibili attraverso alcuni access point (servizi) detti provider che utilizzano differenti protocolli di interazione o corrispondono a differenti implementazioni del protocollo LDAP.

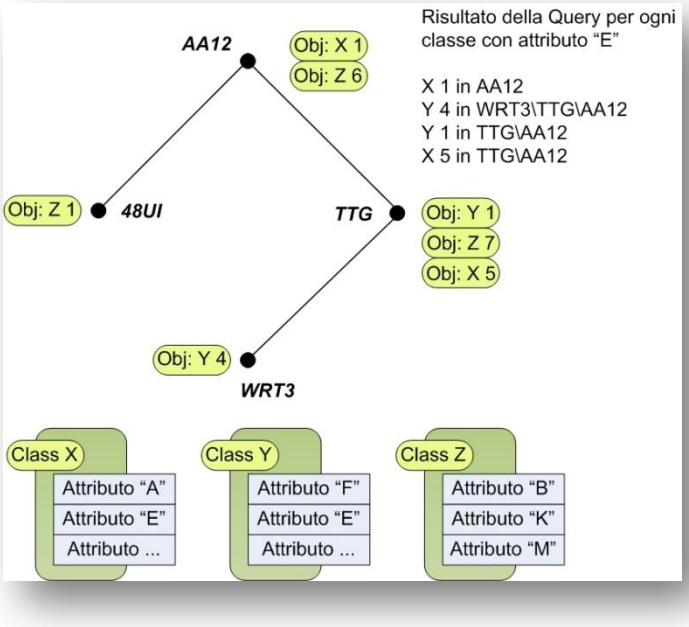
Provider	Description
LDAP	Compatibile con Lightweight Directory Access Protocol
GC	Compatibile con LDAP, specifica la richiesta di connessione con un Global Catalog server
WinNT	Compatibile con sistemi Windows NT/2000/XP/.NET
NDS	Compatibile con Novell NetWare Directory Service
NWCOMPAT	Compatibile con Novell NetWare 3.x

In questa capitolo verrà descritto solo il protocollo LDAP, che rappresenta il protocollo preferenziale dei domini .NET/2000 e quindi verranno analizzati i provider che ne fanno uso, vale a dire GC e LDAP.

3.3.1 Struttura ad albero e attributi

Sia AD che X.500 organizzano i propri dati in una struttura ad albero, i cui nodi sono identificati da nomi; i directory service come X.500, si basano sull'idea che i dati contenuti nei nodi siano composti da collezioni di attributi e che sia possibile operare ricerche su base attributo; questo permette di ottenere dati categorizzati secondo specifiche viste definite dagli attributi stessi anzichè, come avviene nei name service (il DNS, ad esempio), ottenere informazioni singole. La differenza esistente tra un name service e un directory service è simile a quella che

può esistere tra l'elenco telefonico delle pagine bianche e quello delle pagine gialle: nelle pagine bianche l'informazione cercata (il nome dell'abbonato) non appartiene ad una categoria ma è piuttosto un'informazione univoca; ciò a cui siamo interessati è trasformare un'informazione di alto livello, che è più facile rammentare (il nome dell'abbonato), in una informazione di basso livello più funzionale (il numero di telefono). Le pagine gialle hanno uno scopo differente: in questo elenco gli utenti sono raggruppati per categorie (Dentisti, Ristorazione, Ferramenta, ecc.), identificabili grazie ad una specifica caratteristica posseduta da chi ne fa parte; se siamo interessati ad una ricerca per categoria, di norma ricorriamo a quest'ultimo tipo di elenco, raffinando eventualmente la selezione fino ad ottenere i tipi di dati desiderati (nomi, indirizzi, numeri di telefono, etc.). Nei directory service il concetto è analogo: se in una base di dati inserisco informazioni corredate da uno o più attributi che ne descrivono le caratteristiche, diviene possibile effettuare ricerche che permettono di collezionare i dati per categorie; in definitiva è possibile ottenere viste differenti sulla stessa base di dati. Quindi è importante che i dati nella directory siano rappresentati in modo adeguato e che il protocollo che permette di interloquire con l'Active Directory consenta al cliente di ottenere informazioni su base attributo.



3.3.2 LDAP Request

Tramite LDAP è possibile creare un oggetto, rimuoverlo, spostarlo, elencare il contenuto di un container, e così via. In questo paragrafo, vedremo come è possibile ottenere informazioni relative ad oggetti contenuti nella AD utilizzando una specifica sintassi che consente di cercare gli oggetti della directory e selezionarli sulla base dei loro attributi.

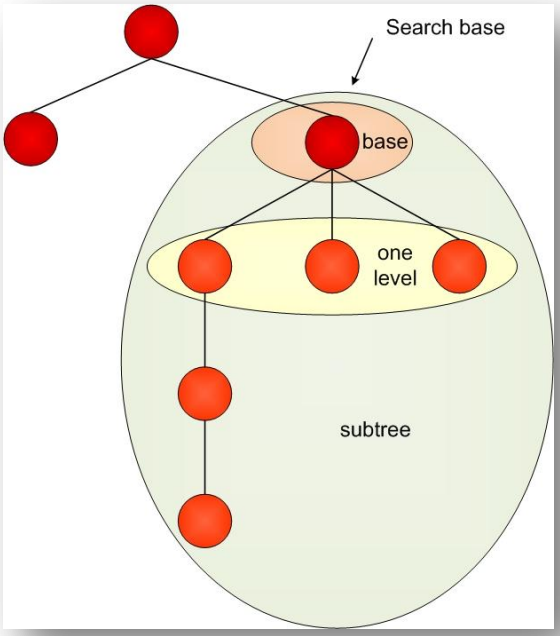
Una query ldap ben formata, è un messaggio di livello applicativo di tipo *SearchRequest (3),* composto di un insieme di parametri che permettono di stabilire i criteri di ricerca:

- *search base* (o *base object*): definisce la locazione di base, il nodo o la foglia della foresta, da cui la ricerca deve partire; la locazione viene definita usando un Distinguished Name LDAP (cfr. par.3.3). La search base serve a specificare in quale sezione della directory effettuare la ricerca.

- *scope*: definisce il livello di profondità della ricerca; uno scope può essere di tre tipi: *base, one level,* e *subtree*. Lo scope di tipo *base* limita la profondità di ricerca 8 malla sola search base; se la search base, ad esempio, è un oggetto container vengono elencati solo i suoi attributi, non il suo contenuto; se lo scope è di tipo *one level,* la ricerca coinvolge il livello appena sottostante l'oggetto base, escludendo l'oggetto base stesso; se lo scope è di tipo *subtree,* la ricerca viene effettuata in modo estensivo su tutta la sottodirectory (incluso l'oggetto base).

- *filter*: permette di indicare gli elementi a cui siamo interessati tra quelli presenti nella sezione di albero specificata.

- *selection* (*o attribute description list*): determina a quali degli attributi degli oggetti selezionati siamo interessati.



Per fare un parallelo con l'espressione SQL (Structured Query Language)

```
SELECT <field> FROM <table> WHERE <condition>
```

potremmo dire che la selection ha funzioni analoghe all'espressione <field>, search base e scope alla espressione <table> e filter all'espressione <condition>; in parole povere e con forte abuso di notazione è come se scrivessimo:

```
SELECT <selection> FROM <search base> WHERE <filter>
```

Questo raffronto con una query SQL semplificata ha solo lo scopo di aiutare a comprendere il ruolo delle relative espressioni nella sintassi delle query LDAP; il cuore operativo della directory, comunque, non è SQL ma LDAP.

Un Search Request permette di definire anche altri importanti parametri come:

- *size limit*: INTEGER (0 .. max); permette al richiedente di definire un numero massimo di elementi che devono essere restituiti da una ricerca; 0 (zero) significa nessuna restrizione.

- *time limit*: INTEGER (0 .. max); permette al richiedente di definire quale sia il tempo massimo possibile, in secondi, per rispondere alla richiesta; 0 (zero) significa nessuna restrizione.

- *types only*: BOOLEAN; serve a stabilire se il richiedente è interessato solo ai nomi degli attributi (TRUE) o anche ai relativi valori (FALSE).

3.3.3 Sintassi di un filtro

La sintassi di un filtro è la seguente:

```
([<operator>](<filter>)[(<filter>)...])
```

dove

```
<filter> = (<attribute><operator><value>)
```

- <attribute> è l'attributo di un oggetto;

- <operator> è uno dei valori descritti nella seguente tabella;

- <value> è un valore compatibile col tipo attribute.

Operator	Descrizione	Tipo a cui si applica
&	And logico	<filter>
|	Or logico	<filter>
!	Not logico	<filter>
=	Equality	<attribute>
>=	Greater Or Equal	<attribute>
<=	Less OR Equal	<attribute>
~=	Approximate Equal to	<attribute>

Un esempio di filtro è

```
(&(objectCategory=Person)(name=ma*))
```

che restituisce tutti gli utenti (classe *Person*) il cui nome comincia con "ma" nella *search base* specificata, con lo *scope* precisato.

3.4 Active Directory Partizionato

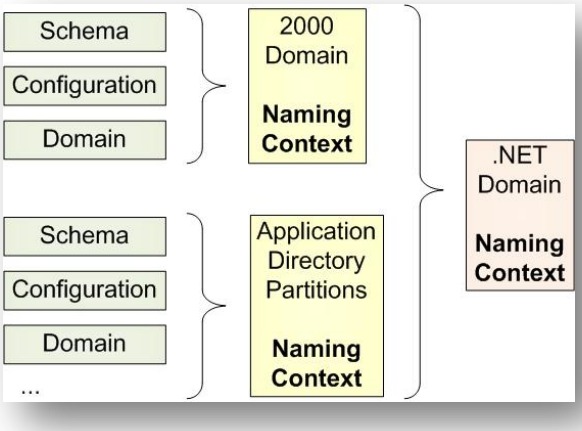
Partizionare, replicare e distribuire sono concetti strettamente connessi tra loro, e la partizione, detta anche Naming Context, è il basic-ground, la pietra angolare della logica architetturale distribuita di AD. Ogni buon servizio multiutente, accessibile da molte migliaia di persone e contenente potenzialmente molti di dati, deve avere un metodo di accesso e di gestione dati efficiente: un unico punto di accesso potrebbe creare una strozzatura nel traffico di rete, risorsa tipicamente critica; disporre le partizioni su più macchine aiuta a distribuire meglio il carico (load balancing). Un management eccessivamente centralizzato, nei grandi domini, potrebbe generare un carico amministrativo non facilmente gestibile, aumentando la complessità amministrativa, che cresce in modo non-lineare con il numero di dati che occorre gestire; separare i dati in partizioni diverse aiuta ad alleggerire il costo di ricerca ed inserzione. Partizionare un database distribuito che sia potenzialmente privo di limiti di crescita, è quindi un buon prerequisito architetturale.

3.4.1 Partizioni

La struttura della directory è quella di un albero, ma non quella di un albero in cui ad ogni nodo corrisponde una singola partizione: esistono differenti tipi di partizioni in AD (almeno 3) e più partizioni possono essere raggruppate su uno stesso Domain Controller (DC). In particolare su un DC Windows 2000 troviamo tre partizioni: le partizioni Schema e Configuration che raggruppano informazioni di tipo globale (riguardano tutta la foresta) e la partizione Domain che contiene informazioni locali relative al dominio a cui il DC appartiene.

In Windows .NET esiste un altro tipo di partizione detta Application Directory Partition (ADP) che può essere aggiunta ad AD per scopi applicativi; le ADP, permettendo all'amministratore di scegliere esplicitamente su quali DC della foresta debbano essere replicate, evitano di generare traffico di rete non necessario;

due di queste partizioni sono state usate da Microsoft per la distribuzione di informazioni relative alle zone DNS di dominio e di foresta (rispettivamente le partizioni DomainDnsZones, ForestDnsZones). In un Domain Controller .NET quindi troveremo almeno cinque partizioni: Schema, Configuration, Domain, DomainDnsZones, ForestDnsZones, più le eventuali altre Application Directory Partition.



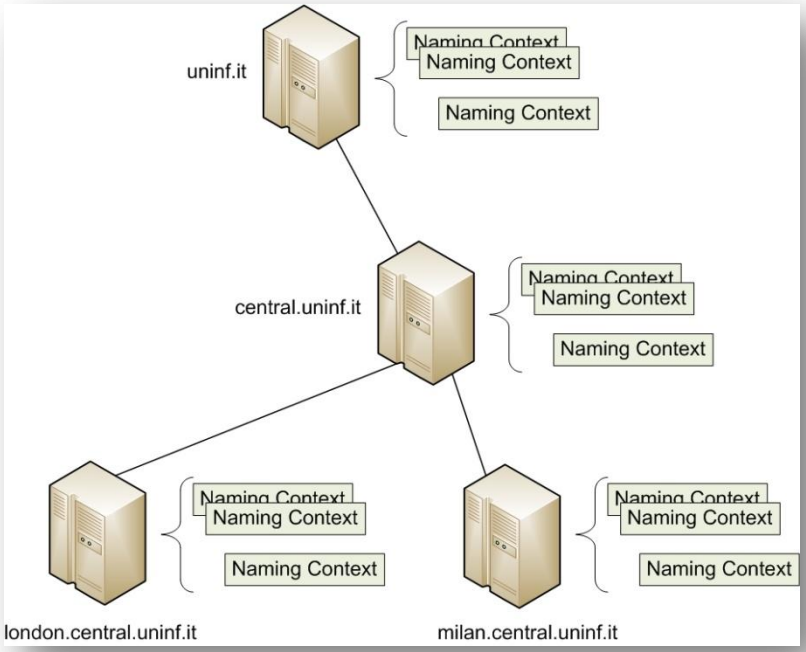
3.4.2 Schema e Configuration

Alcune informazioni del directory service interessano tutta la foresta e vengono quindi conservate all'interno di AD in partizioni specifiche di "tipo" globale: Schema e Configuration. La partizione Schema contiene la definizione delle classi e degli attributi che possono esistere nella foresta ed è unica per la directory; esistono, comunque, copie della partizione Schema su ogni DC della foresta, per motivi di efficienza. Anche l'architettura della directory, la sua topologia e ogni altro dato strutturale devono avere visibilità di tipo foresta; queste informazioni sono contenute nella partizione Configuration e, naturalmente, devono essere uguali in tutta la directory, e reperibili in modo efficiente; per questo motivo esiste una copia della partizione Configuration su ogni DC. Anche se esiste una partizione Schema su ogni DC della foresta, solo una di queste è scrivibile, le altre sono copie di sola lettura; i DC in linea di principio, sono dal punto di vista

funzionale identici tra loro, ma quello che detiene la copia scrivibile della partizione Schema ricopre una funzione unica nella foresta detta *Schema Master Role*; all'occorrenza, ad esempio in caso di failure del DC Schema Master, questo ruolo deve poter essere spostato su un qualsiasi altro DC della foresta, se non è possibile effettuare lo spostamento in modo transazionale (*transfer*), per esempio se il DC che detiene il ruolo di Schema Master è indisponibile, allora occorre effetuarlo in modo imperativo (*seizing*). Lo spostamento del ruolo Schema Master può essere attuato con lo *Schema Management snap-in* (*Microsoft Management Console*) o con il tool a linea di comando *ntdsutil.exe*.

3.4.3 Foreste e alberi

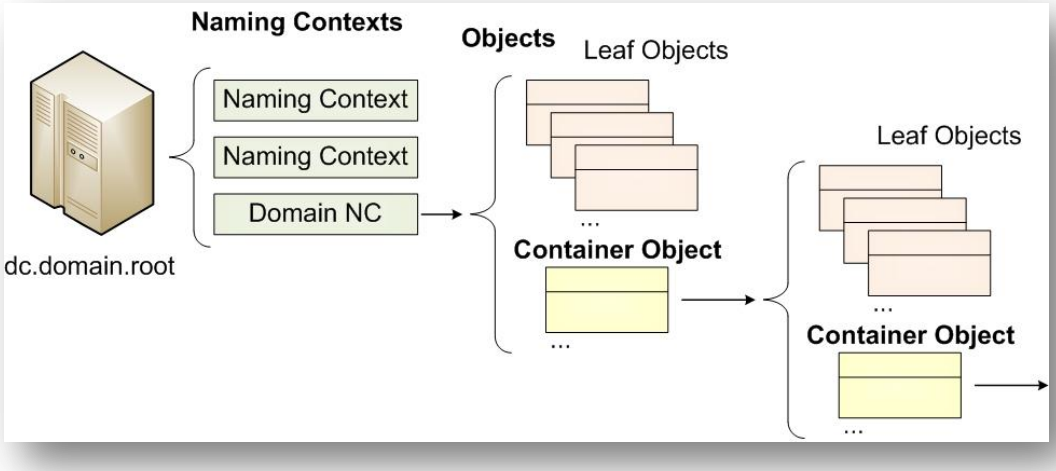
I domini Windows .NET e 2000 possono essere raggruppati in alberi e in foreste. La struttura della directory è quindi quella di un albero di domini che collezionano *Naming Context*, all'interno dei quali sono raccolte le informazioni dell'Active Directory; ad ogni dominio può corrispondere uno o più DC (DC di replica). Dal punto di vista del system engineer un albero è una collezione di domini posti in trust di autenticazione bidirezionale transitiva (*two way transitive trust*), ha quindi un significato connesso all'autenticazione e all'estensione del boundary fisico dei domini. Questa topologia ha anche uno specifico significato dal punto di vista LDAP: l'identificazione di un oggetto nella directory è legata alla sua collocazione nell'albero; questo ha a che fare ovviamente con la corretta formulazione di stringhe LDAP per la connessione e la manipolazione degli oggetti della directory.



3.4.4 Oggetti Container e Oggetti Leaf

Le informazioni contenute in AD sono rappresentate ad alto livello con una logica ad oggetti; alcuni di questi oggetti sono di tipo leaf altri di tipo container (oggetti che possono contenere altri oggetti). I container fungono da raccoglitori logici che permettono di suddividere il contenuto di una partizione in maniera ulteriore; container di uso comune sono, ad esempio, le Organizational Unit (OU). Una OU sostanzialmente è un container "specializzato", ovvero dedicato a particolari funzioni amministrative: serve a identificare in maniera chiara una zona del dominio che deve essere manipolata in modo coerente; ad una OU è possibile applicare, ad esempio, policy e DACL (Discretionary Access Control List) al fine di poter gestire certe zone del dominio secondo convenienza.

Un oggetto leaf può essere reso container rendendo la sua classe possible superior di un altra modificandone l'attributo *possSuperior*.



3.4.5 *Distinguished Name*

I Domain Controller formano quindi una rete di servizi, una foresta di ldap server, che conservano ed espongono un insieme di Naming Context della foresta, che a loro volta raggruppano al proprio interno oggetti container e oggetti leaf. Gli oggetti della AD sono individuabili univocamente nella directory secondo una sintassi che richiede di specificare precisamente la posizione dell'oggetto nell'albero della directory; la sintassi LDAP prevede di identificare un oggetto della directory tramite un vettore, detto Distinguished Name (DN). L'univocità del DN di un oggetto è garantita dal fatto che all'interno di un container il suo nome deve essere univoco; egualmente univoci sono i nomi dei Naming Context e dei DC all'interno della foresta.

Un Distinguished Name ha di norma una forma sintattica del tipo

```
CN=<value>,CN=<value>…,DC=<value>,DC=<value>…
```

oppure

```
CN=<value>…,OU=<value>…,DC=<value>,DC=<value>…
```

o altre analoghe a seconda dei *naming attribute* coinvolti.

L'oggetto *administrator* (classe *user*) presente nella OU (classe *organizationalUnit*) di nome *management*, posto nella partizione Domain del dominio *milan.central.uninf.it* avrà, ad esempio, il seguente Distinguished Name:

```
CN=administrator,OU=management,DC=milan,DC=central,DC=uninf,DC=it
```

mentre le partizione Configuration e Schema della foresta isqre.net hanno rispettivamente i seguenti Distinguished Name:

```
CN=configuration,DC=uninf,DC=it

CN=schema,CN=configuration,DC=uninf,DC=it
```

Dato che Schema e Configuration sono partizioni con visibilità di foresta, il Distinguished Name di queste due partizioni seguono la sintassi:

```
CN=schema,CN=configuration,<Root_Domain_DN>

CN=configuration,<Root_Domain_DN>
```

dove <Root_Domain_DN> corrisponde al Distinguished Name del primo dominio creato nella foresta; tale valore è reperibile nell'attributo *rootDomainNamingContext* dell'oggetto *RootDSE*. Se si desidera accedere alla copia Schema o di Configuration presente su un particolare DC, occorre seguire la seguente sintassi:

```
LDAP://<ServerName>[:<port>]/CN=schema,CN=configuration,<Root_Domain_DN>
```

Ad esempio,

```
LDAP://uninf.it:389/CN=schema,CN=configuration,DC=uninf,DC=it
```

o equivalentemente

```
LDAP://uninf.it/CN=schema,CN=configuration,DC=uninf,DC=it
```

3.4.6 Relative Distinguished Name

L'elemento più a sinistra di un Distinguished Name viene convenzionalmente definito Relative Distinguished Name (RDN); l'utente "alex" creato nella OU "studenti", del dominio "uninf.it", avrà un DN "CN=alex, OU=studenti, DC=uninf, DC=it" e un RDN "CN=alex". All'interno di uno stesso contenitore non è possibile avere due RDN identici, ma è possibile avere oggetti con stesso RDN se appartengono a contenitori diversi (hanno DN differenti).

Inoltre utenti e computer di uno stesso dominio non possono avere logon name uguali anche se creati in differenti container, perchè non possono possedere User Principal Name identici, nè tantomeno Donwlevel Name (*sAMAccountName*) eguali.

3.4.7 GUID

Dato che gli oggetti AD possono essere spostati da un container ad un altro e da un Dominio ad un altro o anche semplicemente rinominati, è fondamentale poter identificare in modo univoco gli oggetti all'interno dello spazio di nomi di AD; per questo motivo ad ogni oggetto della AD viene associato un numero univoco di 128 bit detto GUID (Global Unique Identifer), definito nell'attributo *objectGUID*, che assicura l'esistenza di un'identità univoca persistente.

Ora verrà descritto come questi elementi, precedentemente descritti vengono connessi tra loro e grazie a quali meccanismi la struttura della directory prenda consistenza architetturale, adeguando la rappresentazione logica della directory a quella fisica, lo vedremo qui di seguito.

3.5 AD, DNS e AD references

Il collante tra gli elementi costitutivi (DC, partizioni e oggetti) della directory sono esternamente il DNS, internamente gli AD references; gli AD reference contengono puntatori e sono di tre tipi: cross reference, continuation reference, superior reference. DNS, cross reference e continuation reference ricoprono un ruolo chiave nella definizione strutturale della AD e li esamineremo più a fondo.

3.6 Relazione tra AD e DNS

La prima cosa che deve fare un cliente AD che intenda interloquire con la directory è riuscire a contattare un servizio che espone un access point AD; quindi prima di tutto è necessario ottenere l'indirizzo IP di un DC (ldap server) per creare un circuito di comunicazione; a questo scopo i loro nomi simbolici vengono esposti su un DNS che deve rispondere alle specifiche RFC 2136, 2052, 1996. Queste RFC definiscono nuove caratteristiche che il DNS dovrebbe possedere:

- RFC 2136: introduce il *dynamic update*; permette l'aggiornamento dinamico dei record del DNS direttamente da parte del cliente DNS senza richiedere intervento manuale da parte dell'amministratore;

- RFC 2052: introduce i *service location resource record* (SRV RR); si tratta di un nuovo tipo di record DNS che permette la definizione di parametri non definibili con i normali host record (AA);

- RFC 1996: introduce un nuovo tipo di transazione detta *dns notify*; affronta il problema della propagazione di dati nuovi o modificati in una zona DNS; questa transazione permette ad un DNS server di informare i relativi partner che nella sua zona si è verificata una modifica.

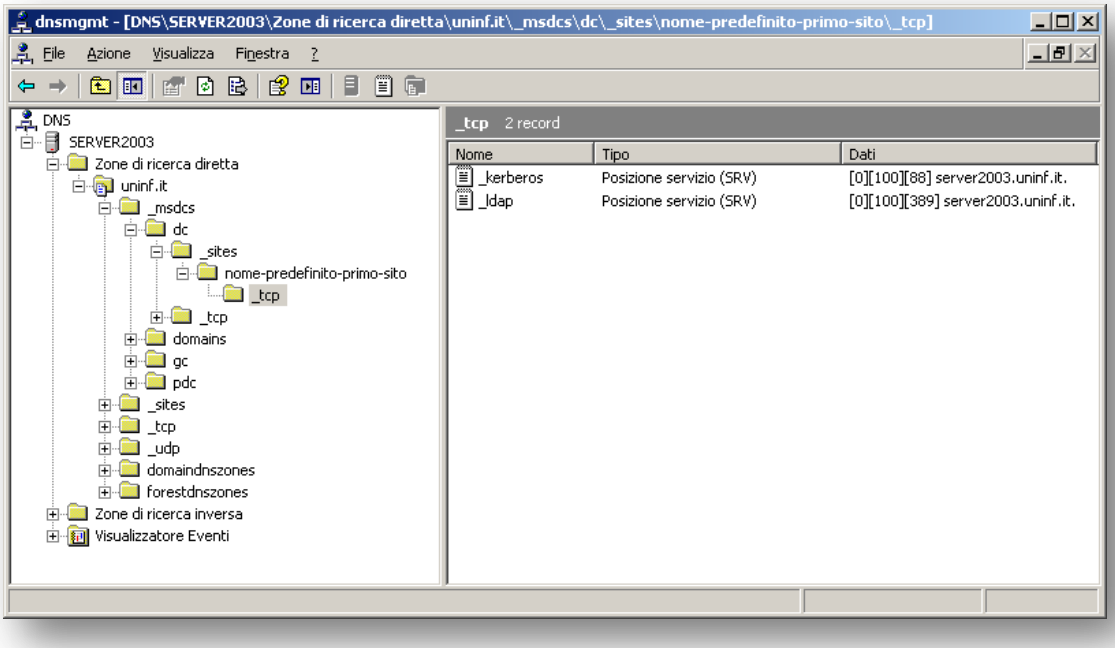
Mentre *dns notify* e *dynamic update* non sono requisti indispensabili (ma utili) per il funzionamento del domini .NET e 2000, la presenza dei SRV RR è assolutamente necessaria, i DC infatti sono pubblicati nei DNS come ldap server utilizzando questi tipi di record. I record SRV RR permettono non solo di definire il nome DNS di una macchina che esporta un servizio (come già fanno i record AA, CN), ma anche di indicare tre valori aggiuntivi: la priorità (<priority>) del servizio, il peso (<weight>) e la porta (<port>). La priorità indica quale endpoint (IP address) preferire per lo stesso tipo di servizio (un valore minore corrisponde ad una priorità più alta); il peso (quello a valore maggiore) specifica quale servizio utilizzare a parità di priorità; la porta indica ovviamente il numero di porta IP su cui il servizio è in ascolto. Un record SRV RR si rifà alla seguente sintassi (le parentesi quadre non indicano valori opzionali, sono parte della dicitura):

```
<name_of_service>, <type of record>, <[priority]> <[weight]> <[port]>,
<host_dns_name>
```

Ad esempio un DC è pubblicato su zone/domini DNS, in un record SRV con una espressione del tipo:

```
 _ldap, SRV, [0][100][386], dc.uninf.it
```

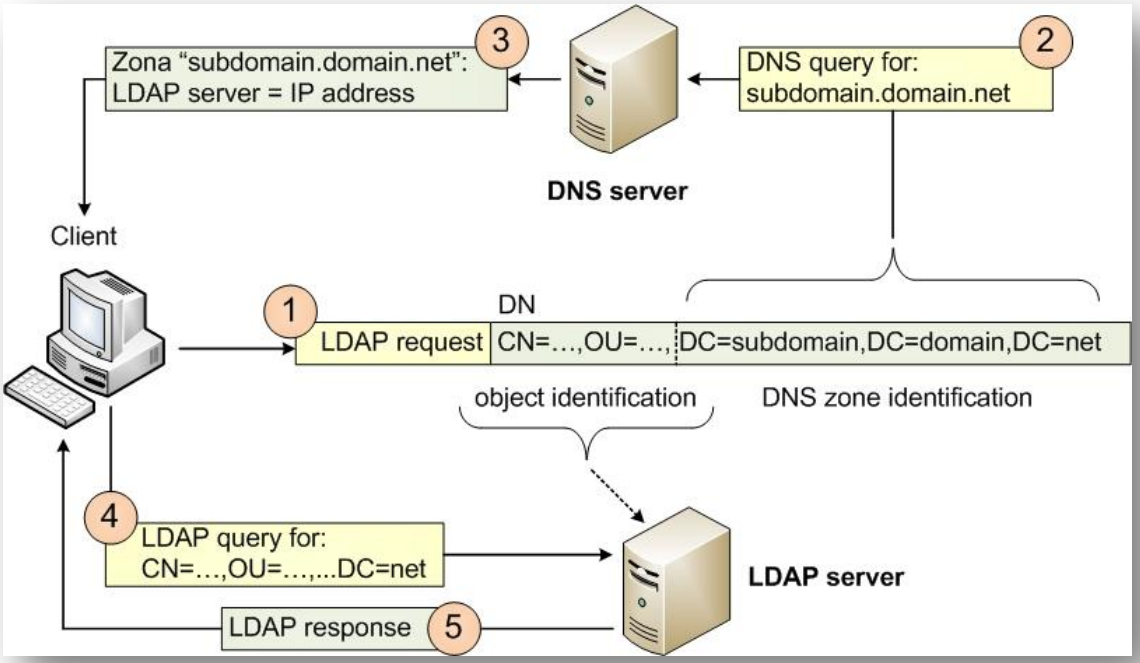
Quando si sta promuovendo un server a DC, vale a dire quando si sta installando l'AD su un particolare server, molti record di questo tipo vengono pubblicati in specifiche zone (correttamente, domini) del DNS; se al momento dell'installazione della AD un DNS rispondente alle specifiche RFC 2136, 2052 non fosse disponibile, queste zone vengono salvate nel file netlogon.dns (*%systemroot%\system32\config*), per poter essere inserite nel DNS in un secondo tempo. Queste zone DNS appositamente create per permettere il funzionamento della AD, sono facilmente riconoscibili perchè sono caratterizzate dal carattere prefisso "_" (underscore) come visibile nella figura successiva.



Grazie quindi alla pubblicazione dei DC della foresta sul DNS o, meglio, dei servizi ldap che espongono le partizioni della directory e tramite i Distinguished Name è possibile reperire un oggetto all'interno della AD.

CN=<…>,…, OU=<…>, …	DC=<sub domain>,DC=<domain>,DC=<root>
Object identification	**DNS zone identification**

Gli elementi "DC=" del Distinguished Name (DN) permettono di individuare la zona DNS ove è contenuto il nome di un ldap server che ospita una partizione della directory; hanno a che fare quindi con le tematiche di connessione e con l'architettura fisica della AD. Le componenti "CN=" ed "OU=" in generale, i naming attributes differenti da "DC=" servono ad identificare gli oggetti (container o leaf) contenuti all'interno della partizione specificata, permettono quindi di sfogliare il contenuto degli oggetti container (partizioni comprese) alla ricerca dell'oggetto desiderato.



3.7 AD Reference

Stando così la struttura, localizzato un DC, possiamo ovviamente accedere ai Naming Context locali; il cliente comunque deve essere in grado di reperire qualsiasi partizione della intera directory, ovvero qualsiasi Naming Context situato all'interno della foresta di domini (o anche esternamente, ad esempio in una foresta separata o in un LDAP server non Microsoft). A questo scopo deve esistere un meccanismo di riferimento ai vari Naming Context; questi riferimenti sono realizzati grazie agli oggetti di tipo cross reference e ai messaggi di referrals e di continuation.

3.7.1 Cross Reference

Nel Configuration Naming Context troviamo il container Partitions, dove sono elencati gli oggetti di tipo cross reference (classe *crossRef*). I cross reference sono il collante della directory: permettono di ottenere informazioni relative alla collocazione delle partizioni della directory presenti su altri DC.

Su ogni DC all'interno del container Partitions troveremo un cross reference object per ciascuno dei domini della foresta, e di ogni altra partizione riferita. Il contenuto del container Partitions rappresenta la *conoscenza* (*knowledge*) che l'AD possiede relativamente a tutte le partizioni della directory; ogni DC può attingere a questa conoscenza dalla copia locale del Configuration.

Tra gli attributi degli oggetti *crossRef* elenchiamo di seguito alcuni di particolare interesse:

- *cn*: il nome (Relative Distinguished Name) dello specifico cross reference object;
- *nCName*: il DN (Distinguished Name) della partizione riferita (ad es. DC=DomainDnsZones,DC=uninf,DC=it);
- *dnsRoot*: Il nome DNS della zona in cui è possibile reperire il server sui cui risiede la partizione riferita.
- *msDS-NC-Replica-Locations* (.NET): il Distinguished Name che identifica il DSA (Directory Service Agent, cfr. par. Error! Reference source not found.) dei DC dove la partizione ADP deve essere replicata (ad es. CN=NTDS Settings,CN=dc1,CN=Servers,CN=Default-First-Site-Name,CN=Sites, CN=Configuration,DC=uninf,DC=it); le partizioni ADP vengono replicate solo sui DC esplicitamente indicati in questo attributo.

E' possibile vedere i crossRef object usando *adsvw.exe* e connettendosi all'oggetto:

```
LDAP://cn=partition,cn=configuration,<Root_Domain_DN>
```

3.7.2 Utilizzare la conoscenza

Quando un cliente effettua una query in AD, LDAP invia ad un DC un

messaggio di tipo SearchRequest(3); a seconda del tipo di richiesta effettuata vengono generati differenti messaggi di risposta:

- Response;
- Referral;
- Continuation.

Response è un messaggio LDAP di tipo *SearchResultEntry(4)* che contiene una lista di Distinguished Name e di attributi che soddisfano la richiesta; Referral e Continuation sono invece messaggi che contengono riferimenti utili al proseguio della ricerca, questi riferimenti sono costruiti sulla base della *conoscenza* che il DC ha della AD. Nelle prossime due sezioni analizzeremo meglio gli scopi degli ultimi due messaggi.

3.7.3 Referrals

Quando un cliente chiede informazioni con scope base e queste informazioni non sono contenute in partizioni che risiedono sul particolare DC interrogato, viene generato un preciso messaggio di errore detto referral (RFC 2251); un referral è una struttura LdapResult con ResultCode 10 contenuto all'interno di un messaggio *SearchResultDone(5)*. Di seguito diamo lo schema della struttura LdapResult:

```
LdapResult {
    ResultCode ;  // integer; indica il tipo di risultato della
                  // SearchRequest
    matchedDN;    // optionale; dipende dal result code
    errorMessage; // una stringa descrittiva
    referral;     // optionale; sequence of LDAPURL
   }
```

Solo se il valore del resultCode è 10, il campo *LdapResult.referral* è presente; questo campo contiene uno o più riferimenti in forma di LDAP URL necessari per proseguire la ricerca su altri server. Un LDAP URL è una stringa del

tipo:

```
LDAP:// [Host [ ":" Port ]]/[DN]
```

dove host indica il DNS name (o l'IP address) del server ove è possibile proseguire la ricerca, port un numero di porta IP (di default la 389) e DN il Distinguished Name dell'oggetto ricercato. Se il cliente ha attivato l'opzione *chase referrals* ("segui le informazioni restituite dai referrals") la ricerca prosegue sui server indicati dagli LDAP URL restituiti.

3.7.4 Continuation Reference

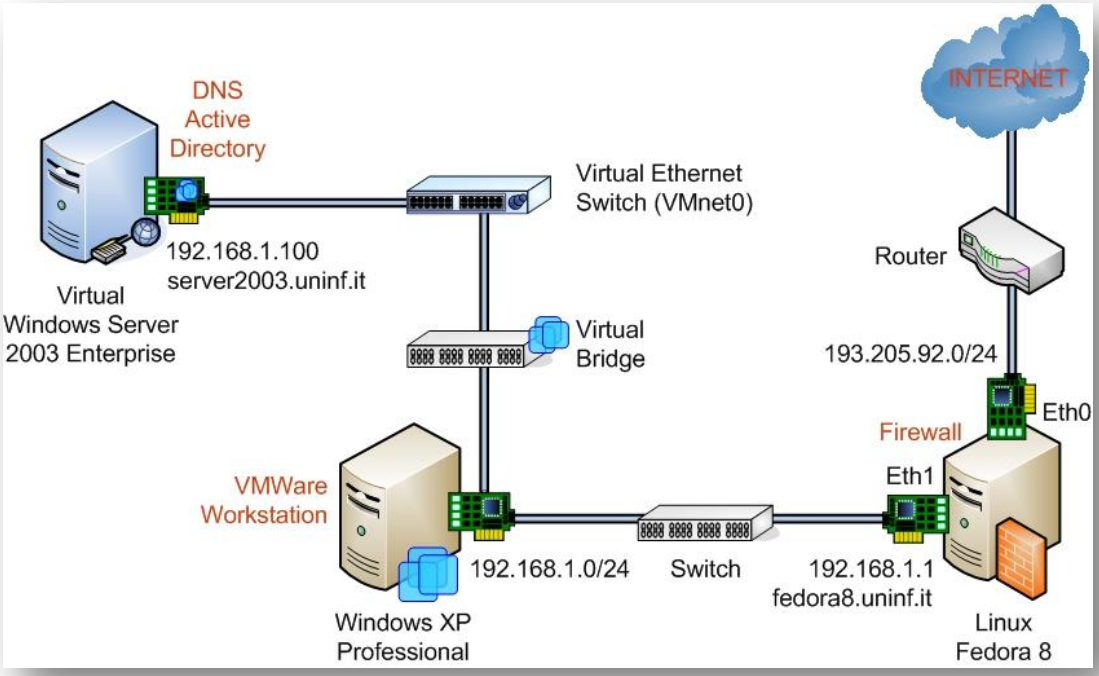
Se a seguito di una richiesta con scope one level o subtree, terminata la ricerca nel Naming Context riferito, il server determina che esistono altre partizioni subordinate, questi restituisce al cliente un segnale di continuation references; il continuation reference è un messaggio di tipo SearchResultReference(19), contenente uno o più LDAP URL; schematicamente:

```
SearchResultReference {
                 LDAP://<hostnameT>/<DistinguishedNameA>
                 LDAP://<hostnameS>/<DistinguishedNameB>
                 …
                }
```

Anche in questo caso gli LDAP URL indicano dove sia possibile proseguire la ricerca [13].

3.8 Installazione e Configurazione del DNS e di AD

Nell'immagine successiva viene riportato lo schema precedentemente configurato, con in più l'installazione e la configurazione di Active Directory e del DNS sulla macchina virtuale Windows 2003 server.



I sistemi Windows 2000/2003 vengono installati per default come sistemi autonomi o membri di dominio e solo ad installazione terminata è possibile elevare il ruolo degli stessi a controller di dominio tramite l'installazione guidata di Active Directory. Questo strumento fornisce una notevole flessibilità aggiuntiva agli amministratori poiché il ruolo del server può essere elevato o abbassato in qualsiasi momento, senza la necessità di re-installare il Sistema Operativo. I controller di dominio di Windows 2000/2003 sono "peer" in un sistema di replica a master multiplo. Questo significa che è possibile modificare i contenuti della struttura di Active Directory su qualsiasi server controller di dominio e il sistema replicherà le modifiche a tutti gli altri controller nel dominio. Questo è un grosso vantaggio rispetto al sistema di replica a master singolo di Windows NT 4, in cui le modifiche dovevano essere effettuate necessariamente sul controller primario di dominio (PDC) e successivamente venivano replicate a tutti i controller di Backup (BDC).

La funzione principale dell'installazione guidata di Active Directory è quella di configurare un server come controller di dominio ed inserirlo in una struttura di dominio già esistente oppure in una nuova struttura.

Prima di avviare l'installazione di Active Directory bisogna verificare che siano soddisfatti i seguenti prerequisiti:

- Una partizione o un volume NTFS;
- Spazio su disco adeguato per le informazioni di directory;
- TCP/IP installato e configurato per utilizzare il DNS;
- Un server DNS che supporti i *record SRV* (*Service Resource Records*) ed opzionalmente l'aggiornamento dinamico ed il trasferimento incrementale. Il *wizard* di installazione di Active Directory offre la possibilità di installare il DNS se si sta installando il primo controllore di domino e non esiste un DNS primario per tale dominio oppure esiste ma non supporta gli aggiornamenti dinamici;
- Le credenziali opportune di un utente con diritti da amministratore e con password regolarmente impostata.

In questo paragrafo descrivo come elevare il ruolo di un server autonomo a controller di dominio di un nuovo dominio in una nuova struttura di dominio.

Active Directory, necessita di un Server DNS già attivo per una corretta installazione. Se la procedura guidata non trova un Server DNS già attivo, installa e configura automaticamente il servizio DNS sul computer locale. Questa procedura, tuttavia, non sempre configura correttamente tale servizio ed è per questo motivo che preferisco effettuare alcune configurazioni manualmente prima dell'avvio dell'installazione guidata di Active Directory.

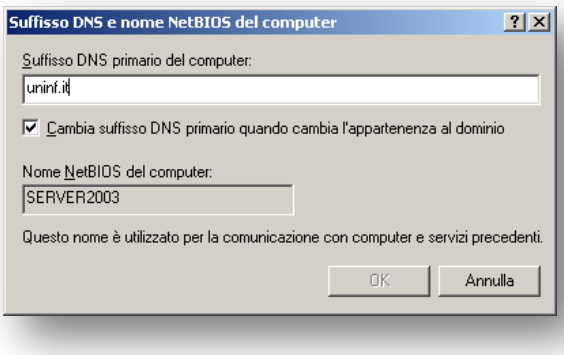
Windows 2003 fornisce un *Wizard* per l'installazione di Active Directory e dunque di un controllore di dominio. Tale *wizard* è costituito dall'eseguibile "`dcpromo.exe`". Tramite lo stesso eseguibile è possibile eseguire la disinstallazione di AD e quindi il declassamento del controllore di dominio a *Member Server*.

L'esecuzione di tale *Wizard* consente di realizzare una delle seguenti funzioni:

- Aggiunta di un controllore di dominio ad un dominio esistente;
- Creazione di un nuovo dominio figlio di un dominio padre in un albero esistente;
- Creazione di un nuovo albero in una foresta esistente;
- Creazione di una nuova foresta.

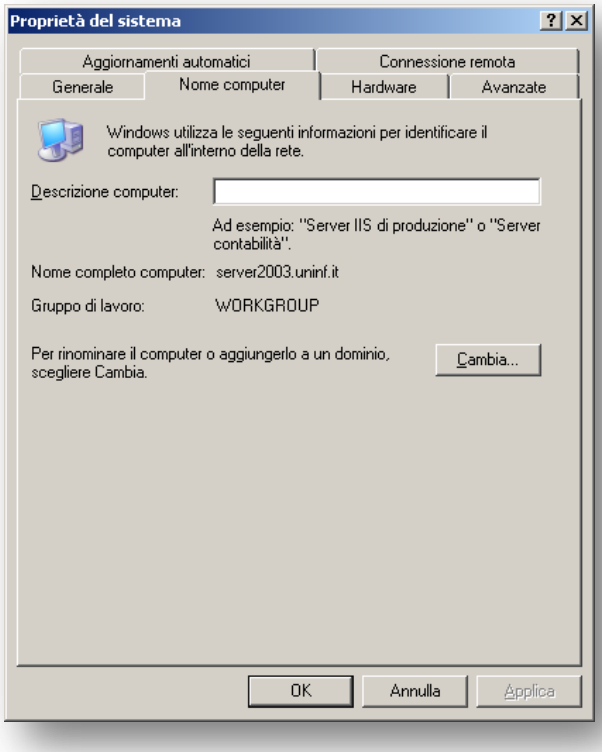
Durante l'installazione viene generato un file di log salvato nella cartella "`systeroot/debug`". Quando installiamo per la prima volta Active Directory sulla rete, si crea il primo controllore di dominio della foresta e dunque il dominio radice della foresta. Tale dominio contiene le informazioni relative allo *Schema* ed alla *Configurazione della foresta*. Di seguito verranno descritti i passaggi base per effettuare l'installazione e la configurazione del DNS e di Active Directory. Per prima cosa andiamo ad inserire il suffisso DNS primario dell computer.

Clicchiamo con tasto destro del mouse su "*Risorse del Computer*", andiamo su "*Proprietà*"→"*Nome Computer*"→"*Cambia…*"→"*Altro…*" su "*Suffisso DNS primario del computer:*" inserire: *uninf.it*, come evidente nella figura successiva:

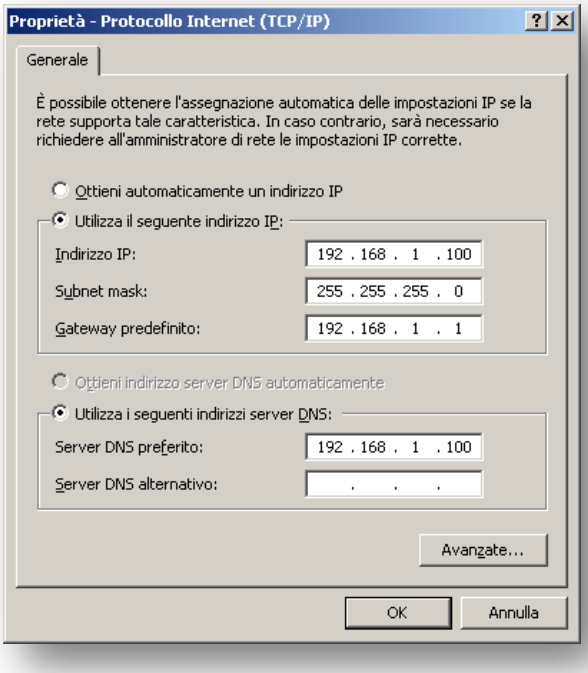


premere "*Ok*" e nuovamente "*Ok*" poi quando compare la finestra "*Per*

rendere effettive le modifiche, è necessario riavviare il computer", premere "*Ok*" e procedere con il riavvio del computer. Successivamente al riavvio del sistema, verificare il nome completo del computer andando su "*Nome Computer*" come precedentemente descritto, l'immagine successiva riporta l'esempio.



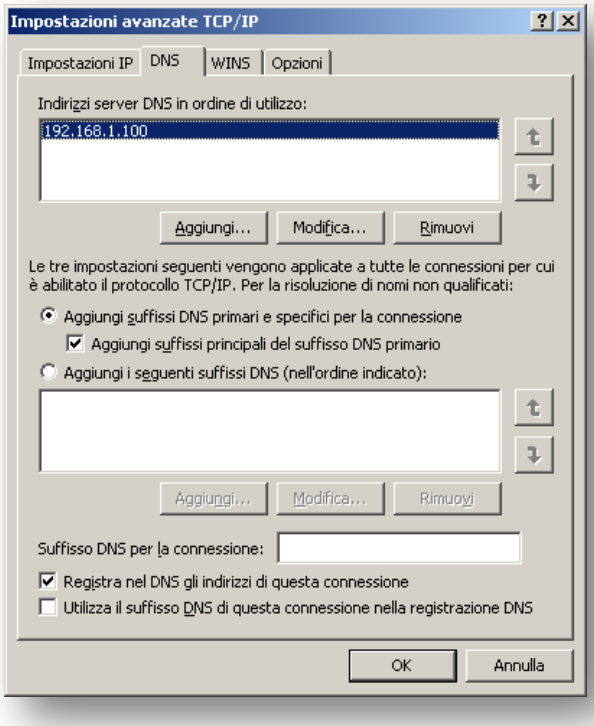
Il passo successivo è la modifica delle impostazioni TCP/IP della scheda di rete. Clicchiamo con il tasto destro del mouse su "*Risorse di Rete*" andare su "*Proprietà*" poi sull'icona "*Connessione sulla rete locale (LAN)*" tasto destro e poi di nuovo su "*Proprietà*" poi nella scheda "*Generale*" cliccare su "*Protocollo Internet (TCP/IP)"* e quindi su "*Proprietà*" compare la seguente immagine in cui vengono riporati gli indirizzi IP statici della macchina e del server DNS.



Come risulta evidente dall'immagine l'indirizzo IP del server DNS predefinito, corrisponde alla macchina stessa, questo perché il DNS, necessario per il funzionamento di Active Directory è stato configurato sulla stessa macchina. E le macchine connesse nella rete LAN privata, fanno riferimento a tale server DNS per la risoluzione dei nomi. L'indirizzo IP è ovviamente satico per il corretto funzionamento di tutta la rete LAN privata.

Più avanti descriverò il funzionamento di Active Directory con un server DNS non installato sullo stesso computer.

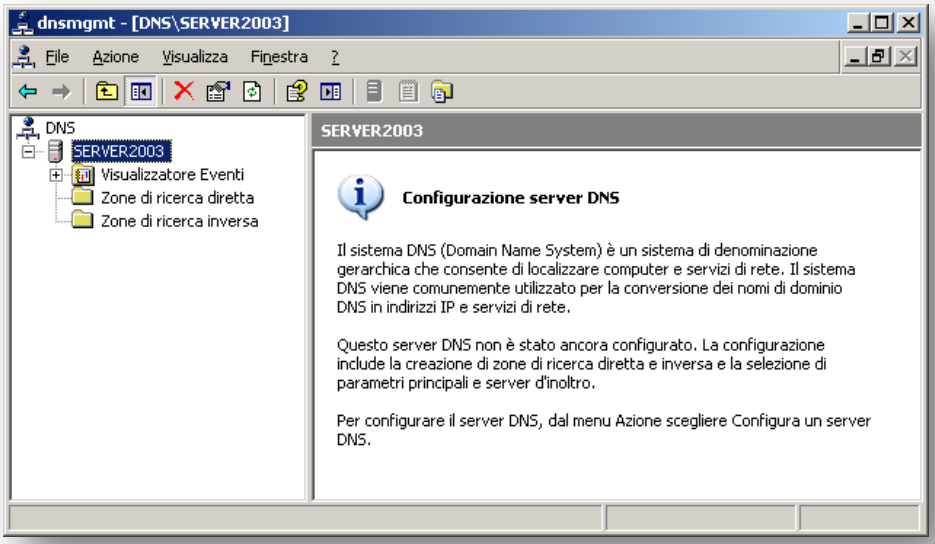
Una volta immessi gli indirizzi IP, clicchiamo su "Avanzare" e poi sulla scheda "*DNS*" e andiamo a verificare che le opzioni "*Aggiungi suffissi principali del suffisso DNS primario*" e "*Registra nel DNS gli indirizzi di questa connessione*" siano spuntate, come risulta evidente nell'immagine successiva.



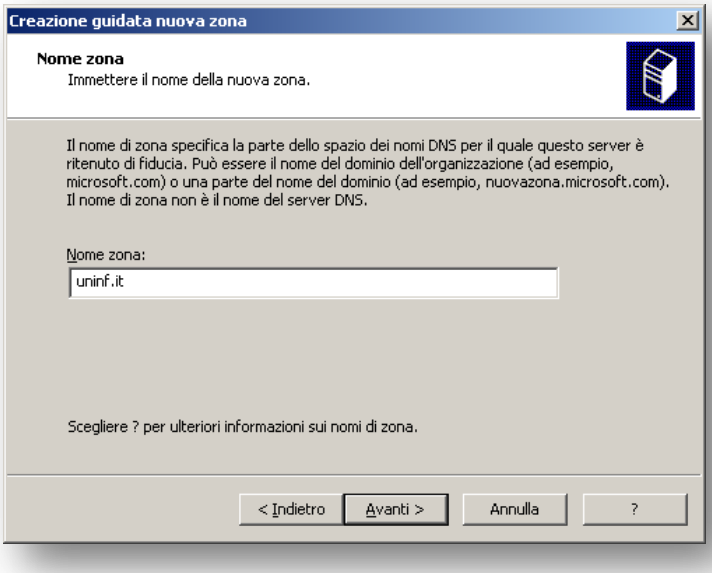
Una volta immessi verificato chidere le finestre aperte cliccando su "*Ok*" e poi su "*Chiudi*".

Procediamo quindi con i passi più importanti ossia l'installazione e la configurazione del servizio DNS. Andare su "*Start*"→"*Pannello di controllo*" →"*Installazione applicazioni*"→"*Installazione componenti di Windows*", scorrere l'elenco fino a "*Servizi di rete*" e cliccare su "*Dettagli…*" quindi spuntare "*Domain Name System (DNS)*" e cliccare su "*Ok*" →"*Avanti >*" per l'installazione effettiva, ovviamente avendo inserito nel lettore DVD il CD di Windows Server 2003. Una volta terminata l'installazione terminare la procedura cliccando su "*Fine*".

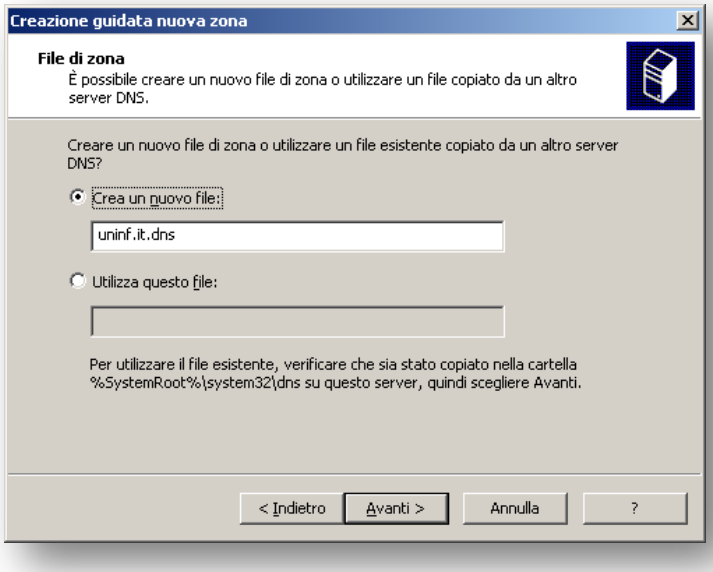
Per la configurazione del servizio DNS, andare su "*Start*"→"*Strumenti di amministrazione*" e quindi su "*DNS*" viene mostrata la seguente schermata.



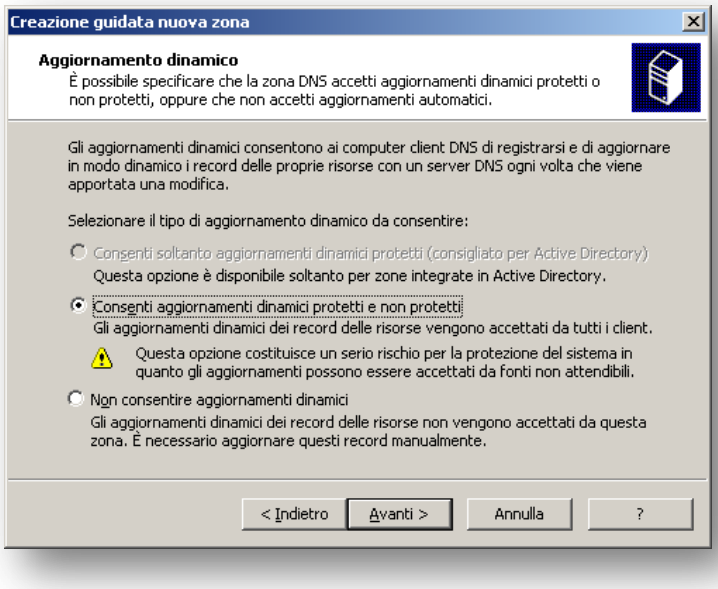
Proseguiamo creando una nuova zona primaria di ricerca, che è utilizzata per risolvere i nomi di dominio in indirizzi IP. Clicchiamo con il tasto destro su "*Zona di ricerca diretta*" poi su "*Nuova zona…*"→"*Avanti >*" selezioniamo "*Zona primaria*" e nuovamente su "*Avanti >*" compare la seguente schermata in cui inserire il nome della nuova zona.



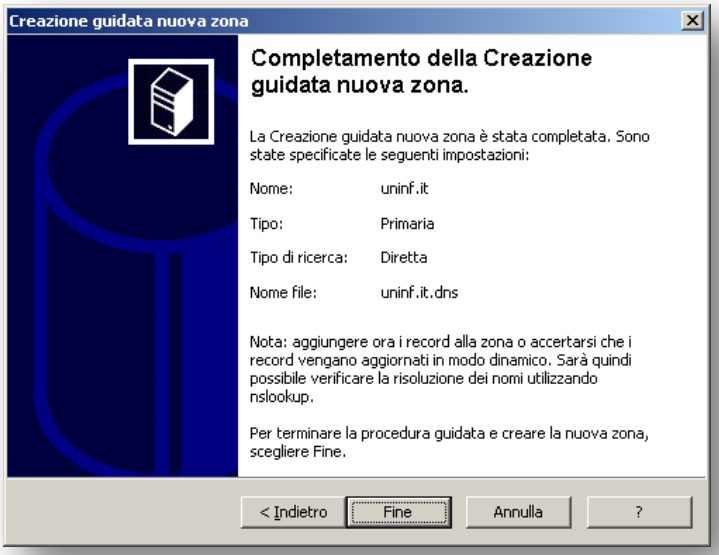
Una volta immesso il nome della nuova zona, clicchiamo su "*Avanti*" compare la seguente immagine in cui impostare il nome del nuovo file.



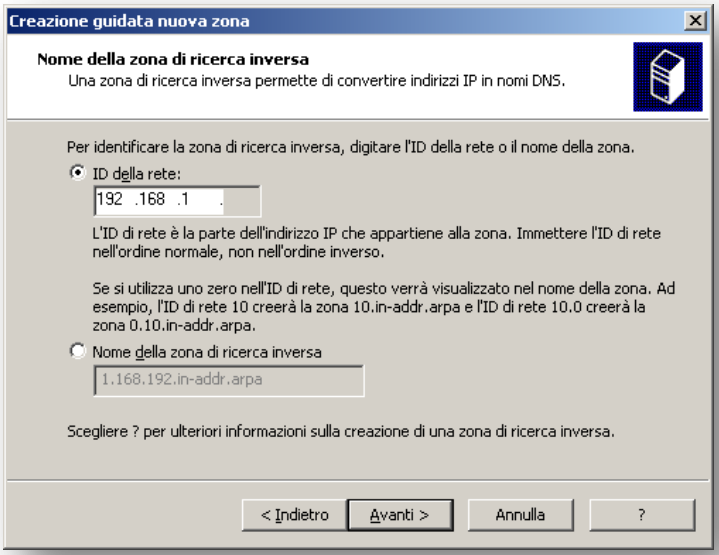
Lasciamo tutto come impostato in automatico e clicchiamo su "*Avanti*" compare la seguente schermata in cui spuntare "*Consenti aggiornamenti dinamici protetti e non protetti*" che permette a qualunque clients di aggiornare i record di risorse in DNS al verificarsi di variazioni. Tali clients possono essere protetti o non protetti.



Clicchiamo quindi su "*Avanti*" e ci viene mostrata la schermata visibile nell'immagine successiva in cui vengono riportate tutte le impostazioni effettuate.

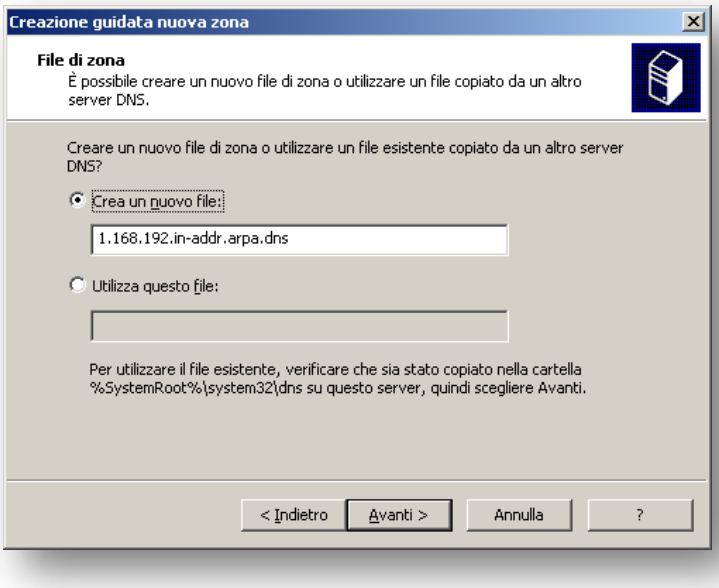


Per completare il processo clicchiamo su "*Fine*". Successivamente creiamo una nuova zona primaria di ricerca inversa. Clicchiamo con il tasto destro su "*Zona di ricerca inversa*" poi su "*Nuova zona…*"→"*Avanti >*" selezioniamo "*Zona primaria*" e nuovamente su "*Avanti >*" compare la seguente schermata in cui inserire l'ID della rete.

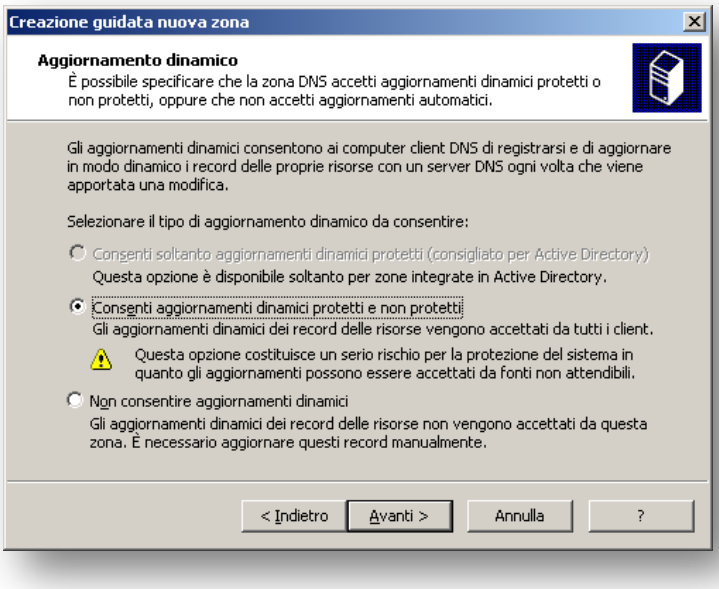


Le ricerche inverse svolgono il compito di autenticare le richieste DNS risolvendo gli indirizzi IP in nomi di dominio o host. Una volta immesso l'ID della

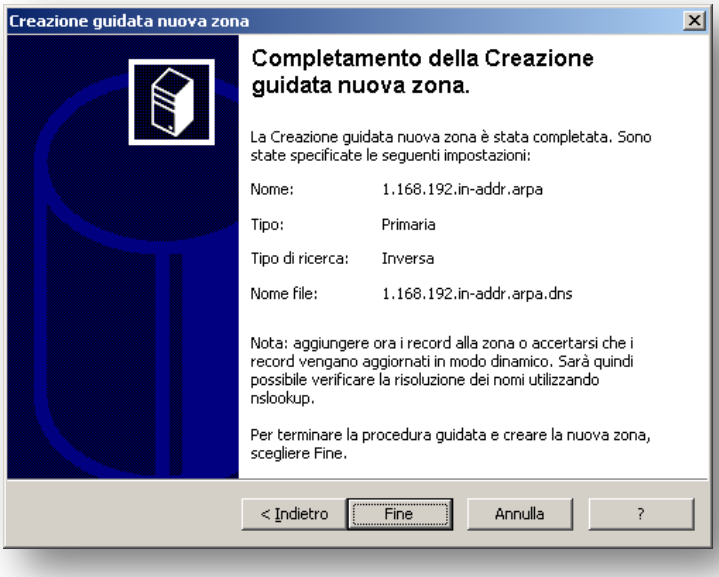
rete, clicchiamo su "*Avanti*" compare la seguente immagine in cui impostare il nome del nuovo file.



Lasciamo tutto come impostato in automatico e clicchiamo su "*Avanti*" compare la seguente schermata in cui spuntare "*Consenti aggiornamenti dinamici protetti e non protetti*". Per gli aggiornamenti dinamici dei record delle risorse.

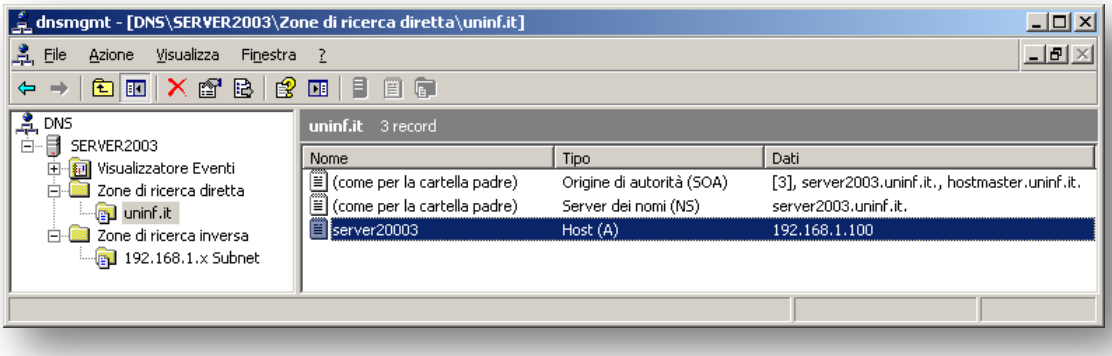


Clicchiamo quindi su "*Avanti*" e ci viene mostrata la schermata visibile nell'immagine successiva in cui vengono riportate tutte le impostazioni effettuate.

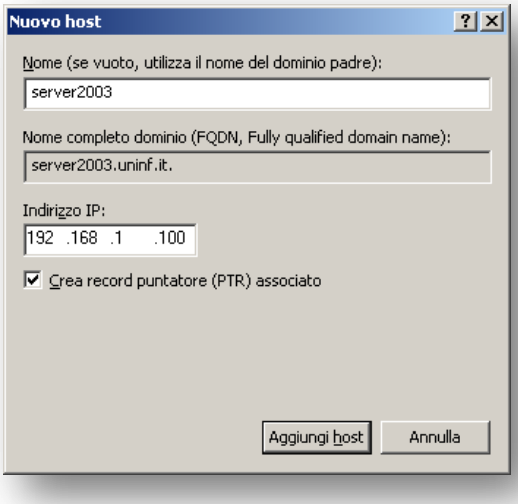


Per completare il processo clicchiamo su "*Fine*".

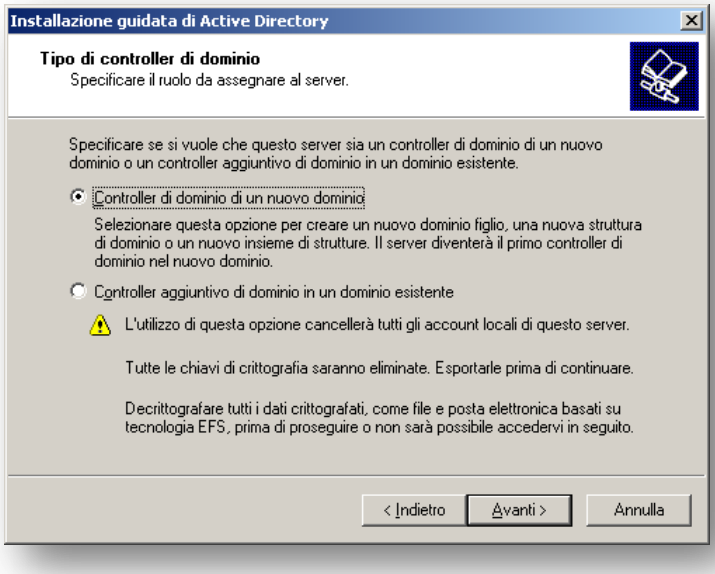
A questo punto cancelliamo e ricreiamo il file, evidenziato nell'immagine successiva, presente nella zona di ricerca diretta per aggiungere il record puntatore di quest'ultimo alla zona di ricerca inversa, qundi clicchiamo con il tasto destro sul suddetto file e quindi su "*Elimina*" poi alla richiesta di conferma clicchiamo su "*Si*".



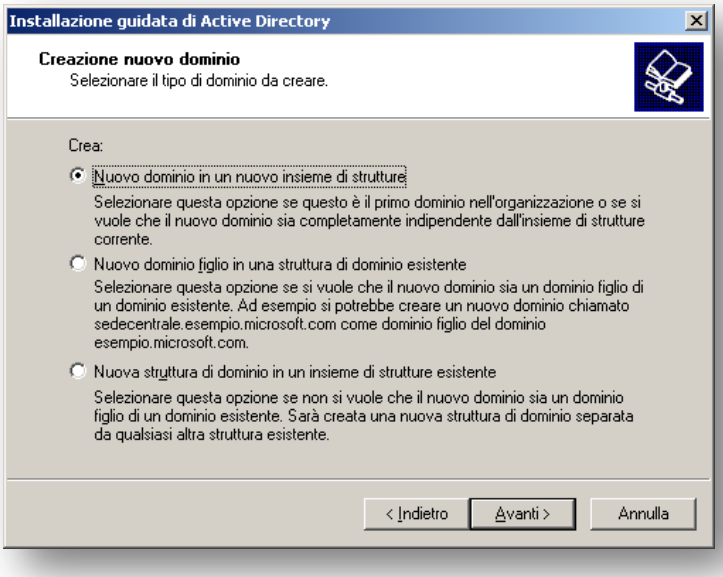
Una volta eliminato lo andiamo a ricreare cliccando ovviamente con il tasto destro su "*uninf.it*" compare un menù in cui selezionare "*Nuovo host (A)...*" e successivamente compare la seguente immagine in cui impostare i valori visibili.



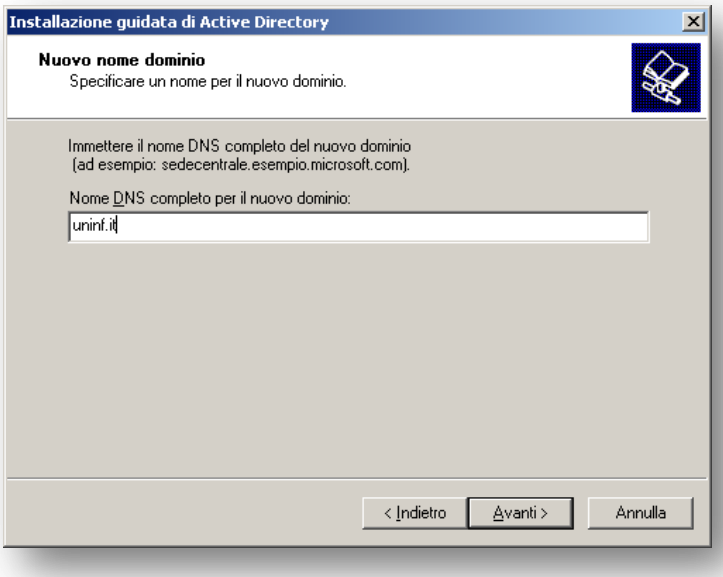
Per completa l'operazione cliccare su "*Aggiungi host*" poi su "*Ok*" e qunidi "*Fine*". Arrivati a questo punto la configurazioni del DNS è completa, quindi procediamo con l'installazione e la configurazione di Active Directory tramite l'utility "*dcpromo.exe*". Cliccare su "*Start*"→"*Esegui…"* inserire "*dcpromo*" e cliccare "*Ok*" quindi alle successive due schermate cliccare su "*Avanti* >" compare la seguente finestra.



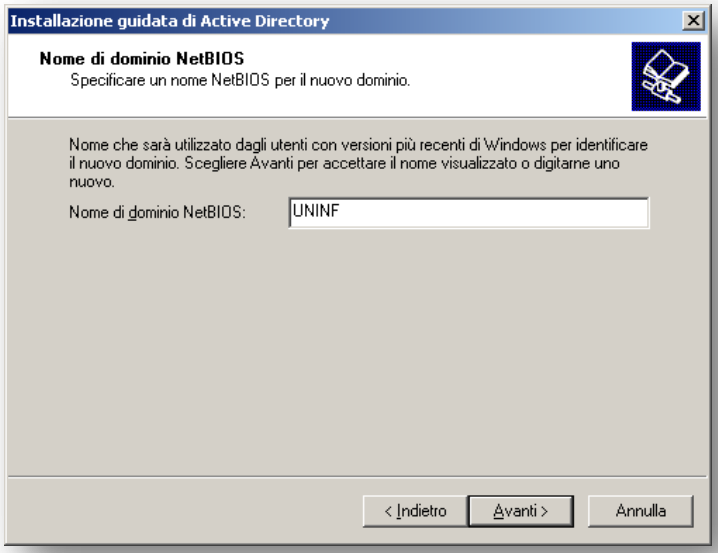
Lasciare l'impostazione su "*Controller di dominio di un nuovo dominio*" e cliccare su "*Avanti* >" compare la seguente schermata di richiesta.



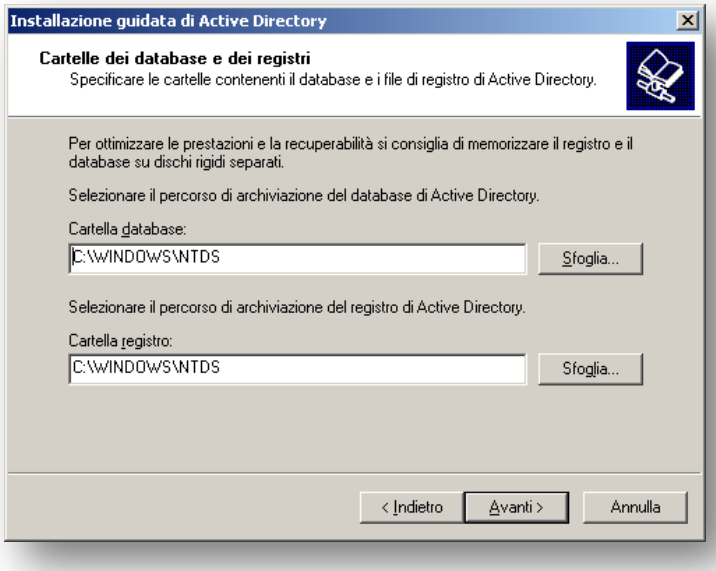
Lasciare, anche in questo caso, l'impostazione su "*Nuovo dominio in un nuovo insieme di strutture*" e cliccare su "*Avanti >*" compare la seguente schermata in cui inserire il "*Nome DNS completo per il nuovo dominio*".



Una volta immesso il nome DNS completo, clicchiamo su "*Avanti >*", ci viene mostrata la seguente immagine in cui impostare il "*nome di dominio netBIOS*", che permetterà a macchine Windows precedenti a Windows 2000 di identificare il nuovo dominio.

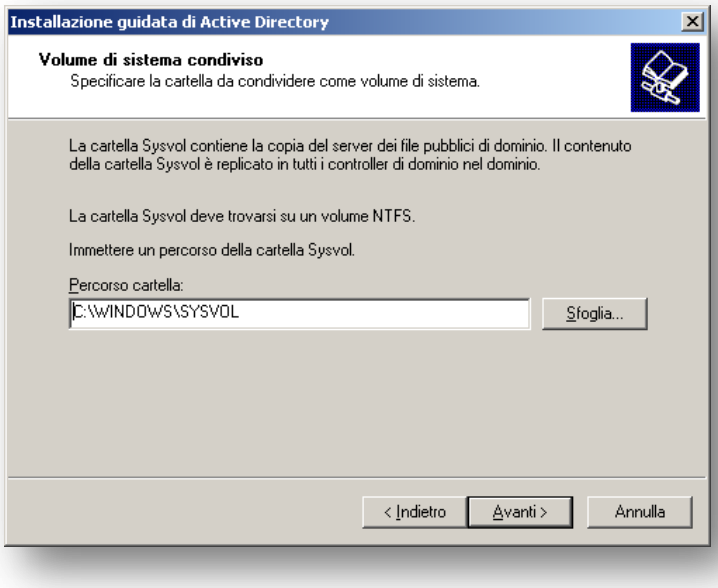


A questo punto clicchiamo su "*Avati* >" e viene mostrata la seguente schermata in cui impostare la "*cartella database"*e la "*Cartella registro*" che specifica la locazione del database di Active Directory e i relativi file di Log.



Poi cliccando su "*Avanti* >" ci compare la scermata successiva in cui impostare il "*Percorso cartella*" per il Sysvol (*Shared System Volume*) che specifica la locazione della condivisione di sistema SYSVOL. Tale struttura risiede su tutti i controllori di dominio, server ad ospitare files ed informazioni relative al

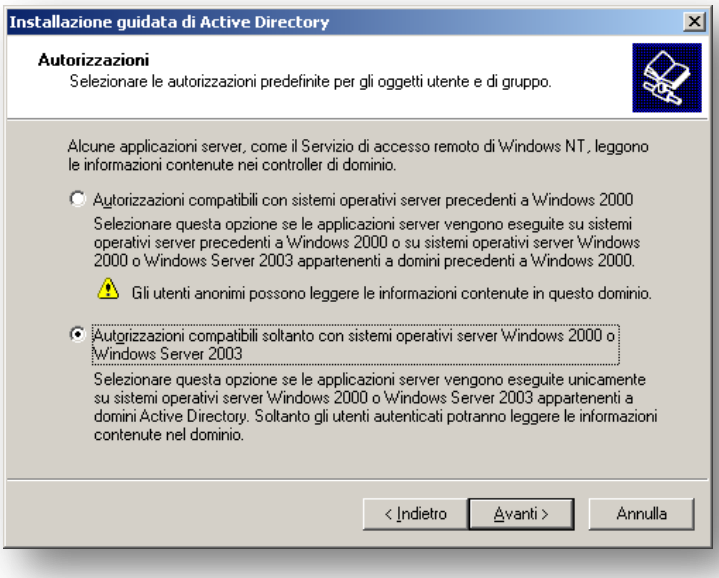
Group Plicies che vengono replicate tra tutti i controllori di dominio e la partizione che la ospita deve essere NTFS.



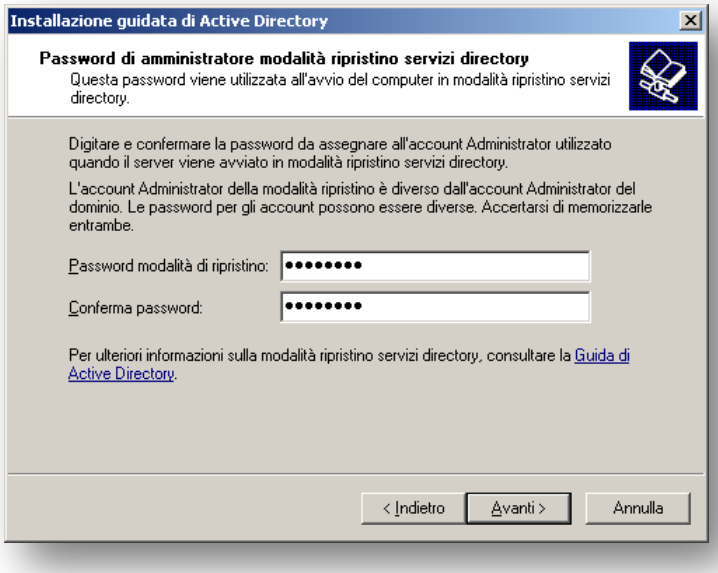
Cliccando su "*Avanti >*" ci compare la scermata di diagnostica.

Come risulta evidente dall'immagine precedente il server DNS risulta configurato a dovere. A questo punto cliccando su "*Avanti* >" ci viene mostrata la seguente schermata in cui specificare se i permessi impostati di default su utenti e gruppi sono compatibili solo con server Windows 2000 o 2003 o anche con

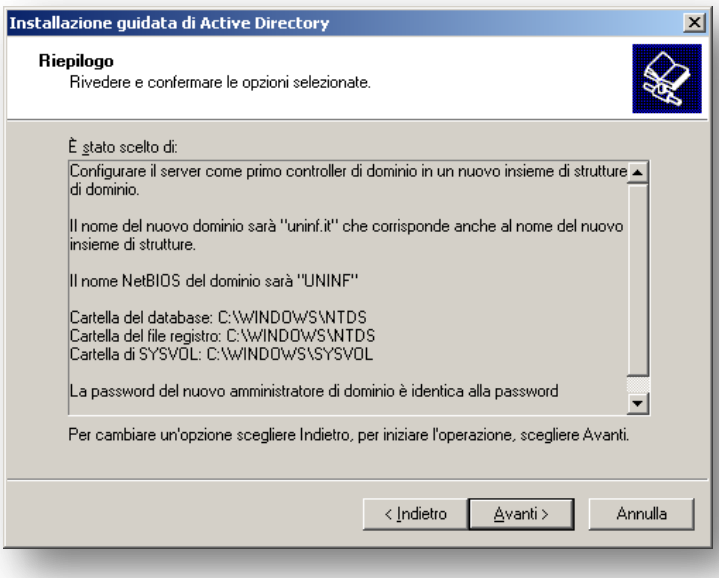
precedenti versioni di Windows.



Cliccando su "*Avanti* >" possiamo specificare la password utilizzata dall'amministratore per eseguire l'opzione di *startup Directory Restore Mode*.



A questo punto cliccando su "*Avanti* >" possiamo avere una immagine di riepilogo della configurazione applicata.



Nuovamente cliccando su "*Avanti* >" viene installato Active Directory.

Una volta completata la procedura cliccare su "*Fine*" e poi alla richiesta di riavviare il computer, cliccare su "*Riavvia*".

Il Wizard una volta impostati i valori visti precedentemente, effettua le seguenti operazioni.

- Installa Active Directory;
- Converte il server a controllore di dominio;

- Aggiunge al gruppo di programmi "*Strumenti di amministrazione*" e i seguenti *Tools*:

  - "*Domini e trust di Active Directoy*", per la gestione delle relazioni di fiducia;
  - "*Siti e servizi di Active Directory*", per la gestione dei siti e delle repliche tra controllori di dominio;
  - "*Utenti e computer di Active Directory*", per la gestione di oggetti (utenti, gruppi, computer) e per il passaggio del dominio da modalità Mista a modalità Nativa.

Applicate le impostazione precedentemente descritte abbiamo la certezza che il DNS e Active Directory funzionano correttamente [14][15[16][17].

3.9 Configurazione del Servizio SSL di Active Directory

A questo punto il servizio di directory fornito da Active Directory funziona utilizzando la porta standard 389. Tutte le comunicazioni che avvengono attraverso questa porta sono in chiaro. Qualsiasi malintenzionato connesso alla stessa rete LAN può tranqulllamente catturare tutte le informazioni che si scambiano il server, in cui è installato Active Directory, e un eventuale client.

Per evitare questo e altri problemi di sicurezza, le transazioni digitali all'interno delle singole LAN o tra le varie LAN richiedono protezione da diversi pericoli, tra cui l'intercettazione di messaggi, lo spoofing delle identità e il ripudio dei messaggi. Per formire tale protezione Windows Server 2003 fornisce tutti i componenti necessari per creare un'infrastruttura PKI.

Una *infrastruttura PKI* è una raccolta di componenti software e criteri operativi che gestiscono la distribuzione e l'utilizzo delle chiavi pubbliche private tramite i certificati digitali. Per proteggere i dati trasmessi in rete, i computer utilizzano vari tipi di crittografia per codificare i messaggi e creano firme digitali

che ne verificano l'autenticità. Affinchè un computer possa crittografare un messaggio e un altro, computer, possa decrittografarlo, è necessario che entrambi posseggano una chiave.

Per utilizzare la crittografia con chiave pubblica, è necessario disporre di un certificato emesso da un'entità amministrativa denominata *Autirità di Certificazione* (*CA, Certificatio Autority*). Una CA può essere un'azienda di terze parti considerata affidabile per la verifica delle identità di tutti i soggetti coinvolti in una transazione digitale, oppure un software in un computer su cui è in esecuzione Window Server 2003 o un altro sistema operativo. Il tipo di CA utilizzata per la propria rete LAN dipende dai soggetti convolti nelle transazioni protette.

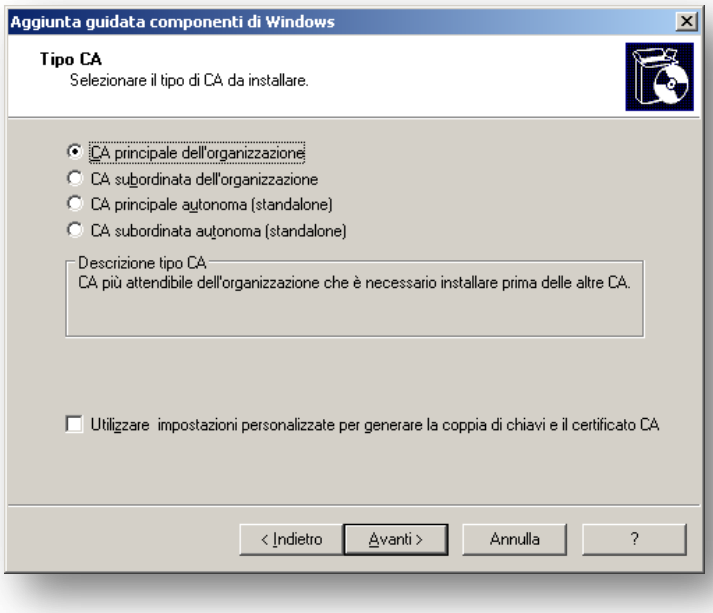
Per ottenere un certificato da una CA è possibile eseguire una procedura manuale, vale a dire che un utente richiede esplicitamente a una CA il rilascio di un certificato, oppure una procedura automatica, in cui un'applicazione richiede e ottiene un certificato in back-ground come parte delle normali funzioni. Indipendentemente dalla procedura scelta, la CA emette una chiave pubblica e una chiave privata come coppia di chiavi. La chiave privata viene memorizzata nel computer dell'utente in forma crittografata mentre la chiave pubblica viene emessa come parte di un certificato. Il certificato è essenzialmente un un vettore per una chiave pubblica e le relative informazionie, in quanto tale, facilita la distribuzione della chiave agli utenti appropriati.

Nel nostro caso siccome vogliamo proteggere efficacemente le comunicazioni interne alla rete LAN privata, la scelta migliore è l'installazione di una CA personalizzata. Windows Server 2003 include i servizi certificati che forniscono le stesse funzioni di una CA. Tutti gli utenti della rete LAN privata possono considerare affidabile tale CA per verificare le identità degli altri utenti.

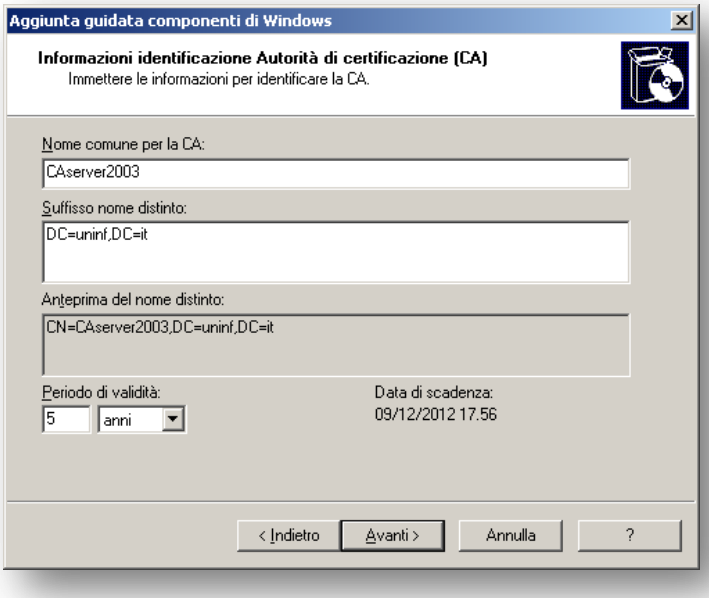
Vediamo come installare e configurare il servizi certificati che fornisce Windows Server 2003. Per prima cosa, dopo aver opportunamente installato Active

Directory, occorre installare la CA nel modo seguente.

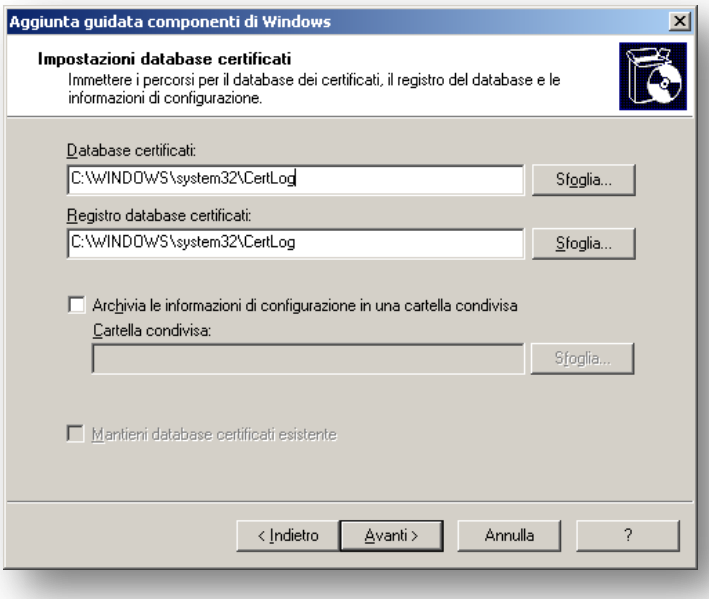
Clicchiamo su "*Start*"→"*Pannello di controllo*"→"*Installazione applicazioni*" e poi su "*Installazione componenti di Windows*" a questo punto scorrere l'elenco trovare e spuntare "*Servizi certificati*" a questo punto ci compare una finestra che ci avverte che non è più possibile cambiare il nome del computer e il dominio di apparteneza, a causa del legame tra il nome del computer e l'autorità di certificazione archiviato in Active Directory. Infatti se andassimo a cambiare il nome del computer o il dominio di appartenenza renderemmo invalidi i certificati emessi dall'autorità di certificazione installata. A questo punto clicchiamo su "*Si*" poi su "*Avanti >*" e ci compare la seguente schermata. In cui definire il tipo di autorità di certificazione.



Lasciare le impostazioni su "*CA principale dell'organizzazione*" e clicchiamo su "*Avanti >*" a questo punto ci compare la seguente finestra in cui inserire il nome della CA.



Inseriamo per il nome "*CAserver2003*" e clicchiamo su "*Avanti* >" successivamente viene creata la chiave crittografica e poi mostrata la seguente finestra in cui definire la locazione del "*Database dei certificati*" e il "*Registro database certificati*".



Lasciamo di default i percorsi, e clicchiamo su "*Avanti* >" per completare l'installazione della CA, alla visualizzazione della finestra, che ci avverte del

completamento dell'installazione, clicchiamo su "*Fine*".

Arrivati a questo punto Active Directory e la CA sono installate correttamente. Quindi è possibile interrogare Active Directory usando la crittografia SSL (*Secure Sockets Layer*) utilizzando la porta standard 636. L'unica requsito necessario è quello di installare il certificato sulla macchina client che vuole comunicare con Active Directory.

Inoltre è possibile richiedere informazioni utilizzando il protocollo LDAPS che prevede l'utilizzo di una URL estesa che consenta di eseguire in maniera generale una richiesta ad un server LDAPS, questa URL ha una forma generica del tipo:

```
ldaps://server/base?attributi?profondità?filtro
```

dove la prima parte, specifica l'indirizzo del server da contattare, è identica a quella di una URL consueta, mentre la seconda parte, che indica la ricerca da effettuare, ha una sua sintassi specifica, come descritto precedentemente [16][18].

Come vederemo più avanti l'abilitazione della comunicazione crittografata di Active Directory, servirà per poterla mettere in comunicazione e qundi sincronizzare i dati, con Fedora Directory Server.

CAPITOLO 4

FEDORA DIRECTORY SERVER COME DIRECTORY SERVICE

4.1 Directory Service

Il termine Directory Service vuole dire una raccolta di software, hardware, e processi che immagazzinano le informazioni su un'impresa, sugli abbonati, o entrambi e mette tali informazioni a disposizione degli utenti. Un Directory Service consiste di almeno un'istanza Directory Server e alcuni o più programmi client della directory. I client possono accedere ai nomi, ai numeri telefonici, agli indirizzi, e ad altri dati immagazzinati nella directory.

Un comune servizio di directory è un server DNS (*Domain Name System*). Un server DNS mappa un nome host di un computer con un indirizzo IP. Così, tutte le risorse di calcolo (hosts) diventano clients del server DNS. Il mappaggio dei nomi host permette agli utenti di localizzare facilmente computer nella rete e ricordare più facilmente i nomi di hosts piuttosto che i loro indirizzi IP numerici.

Comunque, il server DNS immagazzina solo due tipi di informazioni: nomi ed indirizzi IP. Un vero servizio di directory può memorizzare, virtualmente, una quantità illimitata di tipi di informazioni.

Il server di directory memorizza tutte le informazioni in una singola locazione accessibile tramite la rete. Di seguito sono riportati alcuni esempi del tipo di informazioni che si possono memorizzare in una directory:

- Le informazioni di apparecchiature fisiche, come i dati sulle stampanti nell'organizzazione (dove loro risiedono, se loro sono a colori o in bianco e nero, il loro fabbricante, la data d'acquisto, ed il numero di serie).

- Le informazioni pubbliche sugli impiegati, come nome, indirizzo e-mail, ed il loro reparto.

- Le informazioni private sugli impiegati, come salario, i numeri di identificazione di governo, domicili, numeri di telefono e il loro grado di servizio.

- Contratto o informazioni di account, come il nome di un cliente, la data di consegna finale, informazioni su un'offerta, numeri di contratto, e date dei progetti.

Directory Server è necessario per una larga varietà di applicazioni. Esso è provvisto anche di un protocollo standard e API (*Application Programming Interfaces*) per accedere alle informazioni che contiene.

Il server di directory è provvisto di servizi di directory globali, per dire che provvede a fornire informazioni ad una larga varietà di applicazioni. Fino a poco tempo fa, molte applicazioni erano legate ai loro database di proprietà riservate. Mentre un database di proprietà riservata può essere conveniente se si usa solo un'applicazione, i database multipli sono convenienti se si uniscono per dividersi il carico amministrativo trattando le stesse informazioni.

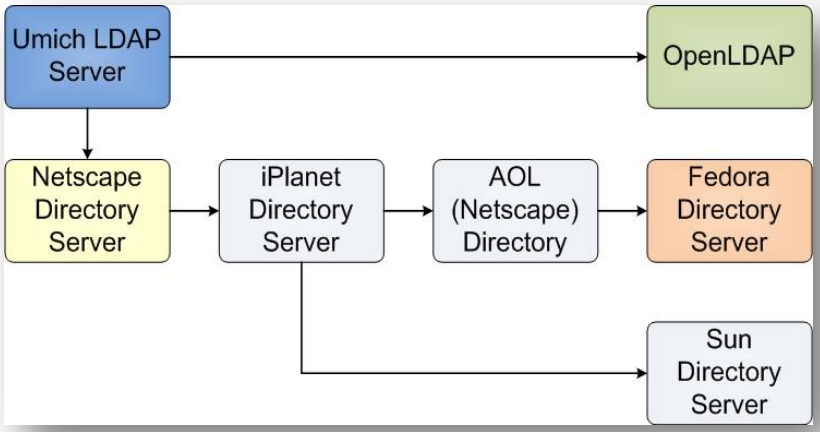
Ad esempio, si supponga che una rete supporta tre differenti sistemi di e-mail proprietarie e ogni sistema ha il suo proprio servizio di directory di proprietà riservata. Se gli utenti cambino le loro parole d'ordine in una directory, i cambiamenti non sono replicati automaticamente negli altri. Maneggiare istanze multiple delle stesse informazioni aumenta notevolmente il costo per l'hardware e per il personale.

Un servizio di directory globale risolve il problema con l'impiego di una singola e centralizzata directory che contiene tutte le informazioni, a cui può accedere ogni applicazione.

Comunque, una larga varietà di applicazioni che accedono alla directory, richiedono un collegamento di comunicazione tra le applicazioni e la directory. Il servizio di directory usa il protocollo LDAP (*Lightweight Directory Access Protocol*) per dare alle applicazione la possibilità di accedere al suo servizio di directory globale.

4.2 Fedora Directory Server

Fedora Directory Server e OpenLDAP sono entrambi derivati dal progetto *slapd* realizzato nell'Università del Michigan. Nel 1996 gli sviluppatori di *slapd* divennero dipendenti Netscape e svilupparono Netscape Directory Server, che appartiene ora a Fedora Directory Server. Quindi ha iniziato la vita come Netscape Directory Server (NDS), poi è diventato iPlanet Directory Server, da cui si è diviso in SunONE directory server e AOL Directory, da quest'ultimo è nato Fedora Directory Server.



Di seguito sono riportare alcune delle caratteristiche presenti in Fedora Directory Server e non presenti in OpenLDAP:

- Abbondante, documentazione;
- Comunità di utenti molto estesa;

- Replica multi master;
- Affidabili backup e ripristina a caldo;
- Utility di integrazione con Active Directory per gli utenti e gruppi;
- Autenticazione e trasporto sicuri tramite Mozilla NSS;
- La maggior parte dei cambiamenti non hanno bisogno di riavviare il server;
- Console grafica per la gestione;
- Amministrazione basato su server HTTP.

Il server di directory include la directory stessa, il software del server implementa il protocollo LDAP e un'interfaccia grafica che permettono agli utilizzatori finali di cercare e cambiare le entry memorizzate nella directory. E' possibile acquistare un programma client che utilizza LDAP o utilizzare un client SDK incluso nel Directory Server.

Senza aggiungere altri programmi client che utilizzano LDAP, il Directory Server può provvedere alla fusione per della intranet o extranet. Ogni Directory Server e applicazioni compatibili con il server, usano la directory come un deposito centrale per condividere le informazioni, come impiegati, clienti, fornitori, e dati dei partner.

E' possibile usare il Directory Server per maneggiare le autenticazioni di utenti della extranet, creare controlli di accesso, impostare le preferenze dell'utente, e centralizzare la gestione degli utenti. I partner, i clienti, e i fornitori possono maneggiare le loro proprie porzioni di directory, riducendo i costi amministrativi.

Un server di directory è provvisto delle seguenti caratteristiche:

- *Replicazione Multi-Master*: Fornisce un servizio di directory altamente

disponibili per entrambe le operazioni di lettura e scrittura. Repliche Multi-Master possono essere semplicemente combinate con scenari di replica a cascata e fornire un elevato grado di flessibilità e scalabilità in un'ambiente di replica.

- *Concatenamenti e referenze*: Aumenta la potenza dell'indice per la memorizzazione della completa vista logica della directory su un unico server, per mantenere trasparente i dati, di un gran numero di Directory Server, ai client.

- *Ruolo e classe di servizio*: Fornisce un meccanismo flessibile per raggruppare e condividere gli attributi tra entries in modo dinamico.

- *Miglior meccanismo di controllo d'accesso*: Fornisce il supporto per le macro che riducono drasticamente il numero di dichiarazioni di controllo di accesso utilizzato nella directory e aumentare la scalabilità di controllo di accesso.

- *I limiti delle risorse da impegnare per il DN*: Dà la possibilità di controllare la quantità di risorse, del server, allocate per ricercare operazioni impegate sul DN del client.

- *Database multipli*: Fornisce un modo semplice per dividere la directory di dati, per semplificare l'implementazione della replicazione e del concatenamento nel servizio di directory.

- *Politica delle password e del blocco degli account*: Permette di definire un insieme di regole che disciplinano come le password e gli account utente sono gestiti nel server di directory.

- *SSL*: Fornisce comunicazioni sicure attraverso la rete, grazie a cifre di criptazione fino a 168 bit.

Di seguito invece vengono riportati i maggiori componenti inclusi in un Directory Server:

- *Un server LDAP*: Il cuore del Directory Server, è provvisto del demone `ns-slapd` e compatibile con gli standards internet LDAPv3.

- *Console del Directory Server*: Una migliore gestione della console che riduce lo sforzo di creare e mantenere il Directory Server. La console di directory è parte di Fedora Console, il comune framework per la gestione dei servizi di directory LDAP.

- *Un Agente SNMP*: Che permette di controllare il server di directory in tempo reale, usando il Simple Network Management Protocol (SNMP).

- *Online backup e restore*: Consente di creare copie di backup e di ripristinare da backup, mentre il server è in esecuzione.

- *Tools a linea di comando*: Consentono di avviare e fermare il server, importare ed esportare i dati nel database, reindicizzare il database, attivare e disattivare gli account, unire gli LDIF e mettere a punto il kernel.

4.2.1 Architettura del Directory Server

L'installazione del Directory Server contiene i seguenti componenti:

- Un server front-end responsabile per le comunicazioni di rete.

- Plug-ins per il funzionamento del server, come il controllo d'accesso e la replicazione.

- Un albero di directory di base che contiene i dati all'interno del server.

4.2.1.1 Server Front-End

Un server front-end del directory server gestisce la comunicazioni con i programmi client della directory. Il Directory Server funziona come un demone su un sistema Unix o come un servizio su un sistema Windows. Più programmi client possono parlare con il server di directory tramite il protocollo LDAP. Quindi possono comunicare usando il protocollo LDAP su TCP/IP.

La connessione può essere anche protetta con SSL/TLS, dipendere se il client negozia l'uso del TLS (*Transport Layer Security*) per la connessione.

Quando la connessione avviene con il supporto del TLS, la comunicazione è di solito criptata. In futuro, quando sarà presente la sicurezza del DNS, TLS usato in congiunzione con i DNS sicuri provvederanno alla conferma delle applicazioni client che si connettono al server corretto. Se i clients sono forniti di certificati, il TLS può essere usato dal Directory Server per confermare che il client ha la possibilità di accedere al server.

TLS e il suo predecessore SSL sono usati per realizzare altre attività sicure come, controlli di integrità di comunicazione, firme digitali, e mutua autenticazione tra i servers.

Più client possono connettersi al server nello stesso tempo sulla stesso rete, perché il server di directory può rispondere contemporaneamente a più richieste. Quando i server diventano grandi, includendo un grande numero di entry o un grande numero di clients sparpagliati geograficamente, essi includono anche multipli Directory Servers posizionati in luoghi strategici in giro per la rete.

4.2.1.2 Server Plug-ins

Il Directory Server dipende dai plug-ins. Un plug-ins è un modo per aggiungere funzionalità al nucleo del server. Questo è importante perché permette

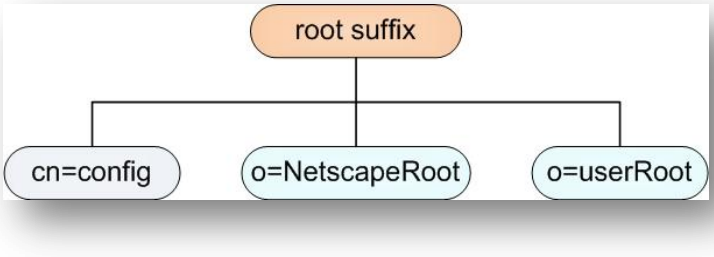
al server di fornire nuove funzionalità. Ad esempio, un database è un plug-in. Un plug-in può essere disabilitato. Quando è disabilitato, le informazioni di configurazione del plug-in rimangono nella directory, ma la sua funzione non verrà usata dal server. Dipende da cosa si scegli di far fare alla directory, si può scegliere di abilitare alcuni plug-ins forniti con il Directory Server.

Quando un plug-in è installato, esso verrà richiamato soltanto per assolvere ad alcune funzioni. Per esempio un plug-in che vuole essere sicuro che gli attributi soddisfano determinati criteri (es. verificare se le password hanno 8 caratteri) verrà richiamato soltanto quando verranno eseguite le operazioni di ADD o MODIFY.

4.2.1.3 Albero base della Directory

L'albero della directory, anche cognosciuto col nome di DIT (*Directory Information Tree*), rispecchia il modello usato da molti file system, con la radice dell'albero, o prima entry, che appare nella parte superiore della gerarchia. Durante l'installazione, il Directory Server crea un albero di directory di default.

L'albero di directory di default appare come segue:



La directory contiene fino a quattro sottoalberi sotto il suffisso di radice:

- `cn=config`: questo sottoalbero contiene le informazioni sull'intera configurazione del server;
- `o=NetscapeRoot`: questo sottoalbero contiene le informazioni di configurazione di altri server, come il server di amministrazione. Il

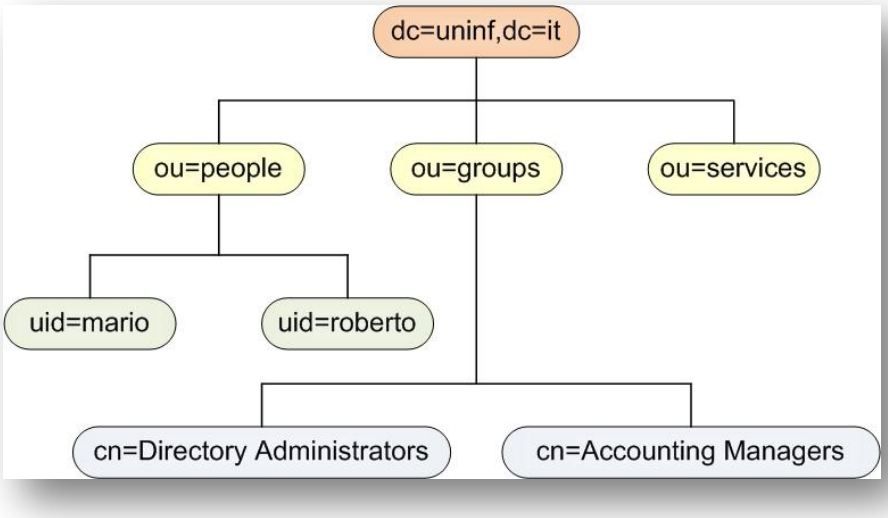
server di amministrazione ha cura dell'autenticazione e di tutte le azioni a cui non si può dare una rappresentazione attraverso il protocollo LDAP (come inizio o arresto);

- `o=userRoot`: durante installazione, un database utente viene creato di default. Il suo nome di default è `o=userRoot`. Si può scegliere di

popolarelo durante l'installazione, o in seguito.

E' possibile creare l'albero di directory di default ed aggiungere alcune dati attinente ad una propria installazione di directory.

Un esempio di albero di directory per la società `uninf.it` è il seguente:



4.2.2 Memorizzazione dei Dati all'Interno del Directory Server

I dati nella directory sono immagazzinati in un database LDBM. Il database LDBM è implementato come un plug-in viene automaticamente installato insieme alla directory e abilitao di default.

Il database è l'unità di base di memorizzazione, prestazione, replicazione, e indicizzazione. Si possono fare operazioni di importazione, esportazione, ritorno

indietro, ripristino, e indicizzazione nel database.

Di default, il directory server usa un singolo database per contenere un albero di directory. Questa database può trattare milioni di entries. Il database di default supporta dei metodi avanzati per tornare indietro e ripristinare i dati, così i dati non sono a rischio.

Si può scegliere di usare più database per sostenere il sistema di directory. Si può distribuire i dati attraverso i database, permettendo al server di tenere più dati rispetto a quelli memorizzabili in un singolo database.

Le sezioni seguenti descrivono come una database di directory memorizza i dati.

4.2.2.1 Entries della Directory

L'LDIF è un formato standard basato sul testo per descrivere le entries delle directory. Un'entry è un gruppo di linee nel file LDIF che contiene informazioni su un oggetto, come una persona nell'organizzazione o uno stampante nella rete. Le informazioni sulle entries sono rappresentate nel file LDIF da una collezione di attributi e dei i relativi valori. Ogni entry ha una classe oggetto di attribuiti che specifica il tipo di oggetto che l'entry descrive e definisce la collezione di attributi supplementari. Ogni attributo descrive un particolare tratto di un'entry.

Ad esempio, un'entry potrebbe essere di una classe `OrganizationalPerson`, indicando che l'entry rappresenta una persona dentro una particolare organizzazione. Questa classe accetta gli attributi `givenname` e `telephoneNumber`. I valori assegnati a questi attributi forniscono il nome e il numero di telefono della persona rappresentata dalla l'entry.

Il directory server usa gli attributi di solo lettura che sono calcolati dal server. Questi attributi sono chiamati attributi operativi. Ci sono anche alcuni

attributi operativi che possono essere specificati dall'amministratore, per il controllo d'accesso e altre funzioni del server.

Le entries sono memorizzate in una struttura gerarchica nell'albero della directory. Con LDAP, si può consultare un'entry e richiedere tutte le entries sotto essa, nell'albero della directory. Questo sottoalbero si chiama *base distingished name*, o base DN. Ad esempio, se si fa un ricerca LDAP, si specifica un DN `ou=people,dc=uninf,dc=it`, l'operazione di ricerca esamina sola il sottoalbero `ou=people` nell'albero della directory `dc=uninf,dc=it`.

Comunque, tutte entry non sono automaticamente ritornate in risposta ad una ricerca con LDAP. Questo perché il server di directory supporta un nuovo tipo di entry, della classe `ldapsubentry`. Un'entry `ldapsubentry` rappresenta un oggetto amministrativo; per esempio, le entries usate per definire un ruolo o una classe di servizio sono del tipo `dapsubentry`. Le entry del tipo `ldapsubentry` non sono restituite in risposta a una ricerca normale. Per ricevere queste entries, i clients hanno bisogno di cerca specificamente le entries della classe `ldapsubentry`.

4.2.2.2 Distribuire i dati della Directory

Quando si memorizza vari parti dell'albero in database separati, la directory può elaborare le richieste dei client in parallelo, migliorando le prestazioni. Si può memorizzare anche i database su macchine diverse, per migliorare le prestazioni.

Per connettere i dati distribuiti, si può creare un'entry speciale in un sottoalbero della directory. Tutte le operazioni LDAP eseguite sotto questa entry si mandano ad una macchina remota dove l'entry è davvero memorizzata. Questo metodo si chiama *chaining*.

Chaining è implementato nel server come un plug-in. I plug-in si abilitano di default. Usando questo plug-in, si crea un collegamento al database, le entry

speciali puntano ai dati memorizzati in locazioni remote. Quando un'applicazione client richiede i dati in un collegamento del database, il collegamento del database recupera i dati dal database remoto e lì rertituisce al client.

4.3 Distinguished Names

Un Distinguished Nanes (DN) è una stringa di testo che identifica uno specifico ramo della directory o una voce. Ogni utente e gruppo nella Directory Server è rappresentata da un DN. Ogni volta che si apporta modifiche alle informazioni degli utenti e dei gruppi, nella directory, si utilizza il Distinguished Nanes (DNs). Ad esempio, è necessario specificare un DN ogni volta che si esegue una delle seguenti operazioni:

- Creare o modificare le entries nella directory;
- Impostare i controlli di accesso;
- Imposta di account utente per le applicazioni quali la posta elettronica o la pubblicazione;

Dunque un Distinguished Nanes (DN) è la stringa di rappresentazione del nome di una entry e la sua posizione in una directory LDAP. Un DN descrive il percorso di una directory. Ogni DN è composto da un numero di componenti chiamati Relative Distinguished Nanes (RDNs). Ogni RDN identifica una specifica voce nella directory. Al fine di garantire che ogni voce è unica, LDAP, impone un unico genitore non può avere due identici RDNs sotto di essa.

Abitualmente, un DN per un utente o un gruppo contiene almeno tre tipi di RDN:

- Un user name, user ID, o nome di gruppo (identificato da parola chiave `cn`);

- Un nome di organizzazione (identificato da parola chiave `o`);
- Un nome di dominio o di componente.

Altri RDNs comuni sono unità organizzativa (`o`), Stato (`st`), e il paese (`c`).

L'esatta composizione di un DN dipende dalla struttura delle directory. La maggior parte delle directory sono organizzate da più categorie dalla designazione del paese e dal nome di organizzazione. Di conseguenza, il DNs è utilizzato per identificare le entries che sono più lunghe e contengono più specifiche RDNs. Per esempio, il DNs per tre dipendenti o utenti nella stessa azienda può apparire come segue:

```
cn=Ben Hurst, ou=Operations, o=Klondike Corp, st=CA, c=US
cn=Jeff Lee, ou=Marketing, o=Klondike Corp, st=CA, c=US
cn=Mary Smith, ou=Sales, o=Klondike Corp, st=MN, c=US
```

In questi esempi, tutti e tre gli utenti lavorano in diversi dipartimenti o unità organizzative (`o`), per la stessa società o organizzazione (`o`) Klondike Corp Il terzo utente lavora in un altro stato (`st`) rispetto ai primi due utenti.

LDAP permette a organizzazioni o unità organizzative di contenere altre organizzazioni e unità organizzative, per consentire la rappresentazione di complesse imprese. Per esempio, il DN di un gruppo all'interno di una grande società potrebbe apparire come segue:

```
cn=Technical Publications, ou=Super Server Group, ou=Server Division,
o=Example Corporation, o=MegaCorp, dc=megacorp, dc=com
```

La tabella successiva riporta le parole chiave utilizzabili in un RDN [26].

Parola chiave RDN	Significato in un DN	Descrizione
`c`	Paese	Paese in cui l'utente o il gruppo risiede.
`cn`	Nome comune o nome completo	Nome completo della persona o oggetto definito dalla entry.

dc	Componente di dominio	Parte di un dominio DNS. Questa parola chiave è tipicamente utilizzato in cima ai livelli di un albero di directory.
l	Località	Nella località in cui l'utente o il gruppo risiede. Questo può essere il nome di una città, paese, o di altre regioni geografiche.
o	Organizzazione	Organizzazione a cui l'utente o il gruppo appartiene.
ou	Unità organizzativa	Unità all'interno di una organizzazione.
sn	Cognome	Cognome dell'utente.
st	Stato o provincia	Stato o provincia in cui l'utente o il gruppo risiede.

4.4 Standard Schema

Nella directory lo schema mantiene l'integrità dei dati memorizzati nella directory, e impone vincoli alle dimensioni, al range, e al formato dei valori assunti dai dati. Decide quali tipi di entry, la directory può contenere (le persone, i dispositivi, le organizzazioni, e così via) e gli attributi disponibili per ogni entry. Lo schema predefinito incluso con Directory Server, contiene sia lo schema LDAP standard, che lo schema di altre applicazioni specifiche.

4.4.1 Formato dello Schema

Il formato dello schema del Directory Server è basato su quello del protocollo LDAPv3. Questo protocollo richiede il server di directory per pubblicare il loro schema attraverso il protocollo LDAP, permettendo alle applicazioni client della directory di recuperare lo schema programmatico e di adattare il proprio comportamento basandolo su di esso. Lo schema per il Directory Server può essere trovata nella entry chiamata `cn=schema`.

Lo schema del Directory Server differisce leggermente dallo schema di LDAPv3, in quanto utilizza una sua classe oggetto di proprietà e di attributi.

Inoltre, esso utilizza un settore privato nell'entry dello schema chiamato `X-ORIGINE`, che descrive dove l'entry dello schema è stato definito originariamente. Per esempio, se l'entry dello schema è definito nello schema standard LDAPv3 il campo `X-ORIGINE` si riferisce alla RFC 2252.

Per esempio, la classe oggetto standard `person` appare nello schema come segue:

```
objectclasses: ( 2.5.6.6 NAME 'person' DESC 'Standard Person
Object Class' SUP top MUST (objectlass $ sn $ cn) MAY
(description $ seealso $ telephoneNumber $ userPassword)
X-ORIGIN 'RFC 2252' )
```

Nella righe precedenti è riportato l'identificativo dell'oggetto dello stato dell'entry schema, o OID, per la classe `(2.5.6.6)`, il nome della classe oggetto `(person)`, una descrizione della classe `(standard person)`, l'elenco degli attributi necessari `(objectclass, sn,` e `cn)`, e gli attributi permessi `(description, seealso, telephoneNumber,` e `userPassword)`.

4.4.2 Attributi standard

Gli attributi mantengono i dati, come un nome o un numero di fax. Il Directory Server rappresenta i dati come coppie di dati, un attributo descrittivo associato ad una specifica parte dell'informazione. Per esempio, la directory è in grado di memorizzare i dati, come un nome di persona in un attributo standard, in questo caso `commonName` (`cn`). Così, un'entry per il nome di una persona "Roberto Carli" ha la seguente coppia di valori:

```
cn: Roberto Carli
```

In realtà, l'intera voce è rappresentata da una serie di coppie attributo-dato. L'intera voce per Roberto Carli, può apparire come segue:

```
dn: uid=mrossi, ou=people, dc=uninf,dc=it
objectClass: top
objectClass: person
```

```
objectClass: organizationalPerson
objectClass: inetOrgPerson
cn: Roberto Carli
sn: Carli
givenName: Roberto
givenName: Giorgio
mail: mrossi@uninf.it
```

L'entry per Roberto contiene più valori, per alcuni degli attributi. L'attributo `givenName` appare due volte, ogni volta con un valore unico.

Nello schema, ogni definizione di attributo contiene le seguenti informazioni:

- Un nome unico;
- Un'identificativo dell'oggetto (OID) per l'attributo;
- Un testo descrittivo dell'attributo;
- L'OID della sintassi dell'attributo;
- Indicazioni del fatto che l'attributo ha un valore singolo oppure un valore multiplo, se l'attributo è per l'uso della directory, l'origine del attributo, e di qualsiasi altra corrispondenza delle regole associate con l'attributo.

Per esempio, la definizione dell'attributo `cn` appare nello schema come segue:

```
attributetypes: ( 2.5.4.3 NAME 'cn' DESC 'commonName Standard
Attribute' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

La tabella sottostante contiene una lista dei più comuni attributi utilizzati, nella directory, per gli utenti e i gruppi.

Parola chiave Attributo	Nome dell'attributo	Descrizione
giveName	Nome	Il primo nome utente.
mail	Indirizzo email	Indirizzo e-mail per l'utente o il gruppo.
streetAddress	Strada	Indirizzo di strada e dell'utente o del gruppo definito dall'entry.
telephoneNumber	Telefono	Numero di telefono per l'utente o il gruppo.
title	Titolo	Titolo del lavore odell'utente.
uid	User ID	Nome che identifica in modo univoco la persona o l'oggetto definito dalla entry.
userPAssword	Password	Password dell'utente.

4.4.3 Classi oggetto standard

Le classi oggetto sono utilizzate per raggruppare le informazioni correlate. In genere, un classe oggetto rappresenta un vero e proprio oggetto, ad esempio una persona o un fax. Prima di poter utilizzare una classe oggetto e i suoi attributi nella directory, devono essere identificati nello schema. La directory riconosce un elenco delle classi oggetto di default.

Ogni entry di directory appartiene ad una o più classi oggetto. Una volta che un oggetto è messo nella classe oggetto è identificato nello schema da un'entry; l'entry del Directory Server può avere un certo insieme di valori di attributi e devono avere un altro insieme, di solito più piccoli, di valori degli attributi.

La definizione della classe oggetto contiene le seguenti informazioni:

- Un nome unico;
- Un'identificativo dell'oggetto (OID) che nomina l'oggetto;
- Un insieme di attributi obbligatori;
- Un insieme di attributi consentiti.

Come è in questo caso per tutti gli schema del Directory Server, le classi

oggetto sono definite e memorizzate direttamente nel Directory Server. Ciò significa che è possibile interrogare e cambiare lo schema della directory con operazioni LDAP standard.

4.5 Cosa può e non può Includere la Directory

I dati che si possono inserire nella directory sono:

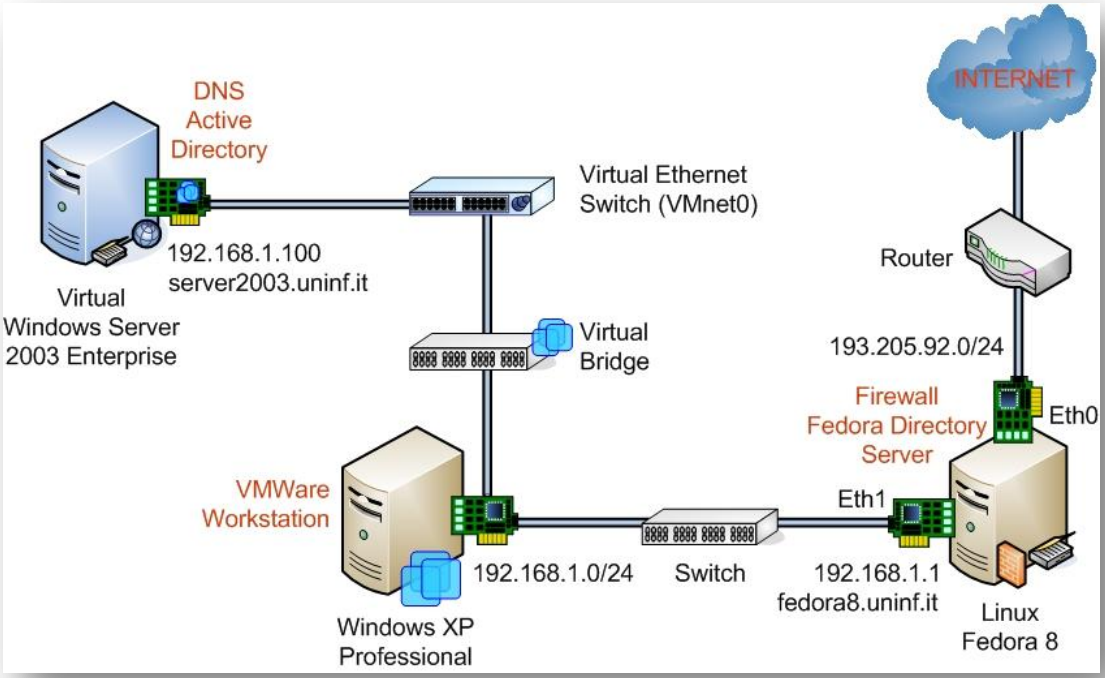
- Informazioni di contatto, come numeri di telefono, indirizzi fisici e indirizzi e-mail.
- Informazioni descrittive, come il numero dell'impiegato, il titolo di lavoro, l'identificazione del direttore o dell'amministratore, e gli interessi collegati al lavoro.
- Informazioni per contattare l'organizzazione, come il numero di telefono, indirizzo fisico, l'identificazione dell'amministratore, e la descrizione degli affari.
- Informazioni relative alle apparecchiatura, come l'ubicazione fisica della stampante, il tipo di stampante, ed il numero di pagini per minuto che la stampante può produrre.
- Contatti e informazioni collegate per i partner accreditati, clienti e commercianti.
- Informazioni di contratto, come il nome del cliente, date di scadenza, descrizione del lavoro e informazioni sul prezzo.
- Preferenze dei software individuali o informazioni di configurazione del software.

- Siti di risorse, come puntatori a web server o il file system di un certo file o applicazione.

Il server di directory è eccellente per trattare grandi quantità di dati che le applicazioni client possono legga e scrivere, ma non è designato per trattare, grandi, oggetti non strutturati, come immagini o altri media. Questi oggetti si devono memorizzare in un filesystem. Comunque, la directory può memorizzare i puntatori a questi tipi di applicazioni attraverso l'uso di FTP e HTTP, o altri tipi di URL [19] [20] [21].

4.6 Installazione e Configurazione di FDS

Vediamo nell'immagine successiva l'evoluzione dello schema relativo ai dispositivi software configurati nella rete privata LAN, in particolare notiamo l'installazione e la configurazione di Fedora Directory Server.



Per avere un completo sistema Fedora Directory Server, occore soltanto installare il file `fedora-ds-1.0.4-1.FC6.i386.opt.rpm`, reperibile sul sito http://directory.fedoraproject.org/wiki/Download dedicato esclusivamente all'FDS.

I componenti software contenuti in un'installazione di FDS sono:

- *Fedora Console*: Fornisce l'interfaccia utente per le applicazioni Directory Server. Da essa, è possibile svolgere le funzioni di amministrazione del server così come lo spegnimento e la partenza del server, l'installazione di una nuova istanza del server, e la gestione delle informazioni utente e di gruppo. Fedora Console può essere installato come applicazione stand-alone su qualsiasi macchina. È inoltre possibile installare sulla rete e utilizzarlo per la gestione remota dei server.

- *Fedora Administration Server*: Administration Server è un front-end a tutti I Directory Server. Che riceve le comunicazioni da Fedora Console e passa tali comunicazione all'opportuno Directory Server. Quindi il sito avrà almeno un Administration Server per ciascun server di directory root.

- *Directory Server*: Directory Server è un'implementazione di Fedora LDAP. Il Directory Server viene eseguito come il processo `ns-slapd`. Questo è il server che gestisce il database della directory e risponde alle richieste dei clients. Il Directory Server è un componente necessario.

Le risorse hardware necessarie per il funzionamento del FDS sono:

Versione O.S.	Fedora con relativie patch e aggiornamenti
CPU	500 Mhz o più, compatibile con il PIII.
Memoria RAM	256 MB, per un'ottimo utilizzo consigliati 1 GB
Memoria Disco Fisso	Approssimativamente 300 MB per una minima installazione, per un sistema di produzione sono raccomandati 2 GB per mantenere i binari, il database e files di log. 4 GB sono richiesti per Directory di grossa dimensione.
Altri Requisiti	È necessario installare come root per poter utilizzare i numeri di porta noti (ad esempio, 389) che si trovano al di sotto di 1024. Se non si prevede di utilizzare numeri di porta inferiori a 1024, non si ha

	bisogno di installare come root. Se si prevede di eseguire come root, si dovrebbe installare anche come root.

È possibile utilizzare uno dei numerosi processi di installazione per installare il Directory Server. Ognuno di essi guida l'utente attraverso il processo di installazione e garantisce che l'installazione di vari componenti avvenga nell'ordine corretto.

Innanzitutto andiamo ad installare l'rpm relativo al FDS, utilizzando la shell bash, da utente root, nel seguente modo:

```
rpm –ivh fedora-ds-1.0.4-1.FC6.i386.opt.rpm
```

Una volta installato l'rpm ci viene indicato che per la configurazione del FDS, e quindi per la creazione di un'istanza del Directory Server, occorre avviare lo script di setup presente nel percorso `/opt/fedora-ds/setup/setup`.

Quindi per l'esecuzione dell'utility, occorre spostarsi nella seguente directory:

```
/opt/fedora-ds/setup
```

A questo punto da utente root, avviamo lo script:

```
./setup
```

ci vengono mostrati i temini di licenza, che ovviamente dobbiamo accettare, per poter utilizzare il FDS:

```
Do you accept the license terms? (yes/no) yes
```

Quindi alla richiesta digitiamo `yes` se si accettano i temini di licenza, oppure `no` nel caso contrario. Nel caso vengano accettati i termini di licenza, vengono mostrate le seguenti informazioni:

```
==========================================================================
                        Fedora Directory Server 1.0.4
==========================================================================
```

```
The Fedora Directory Server is subject to the terms detailed in the
license agreement file called LICENSE.txt.
Late-breaking news and information on the Fedora Directory Server is
available at the following location:

    http://directory.fedora.redhat.com

Continue (yes/no) yes
```

Quindi digitare `yes` per continuare con la configurazione. Successivamente vengono mostrate alcune notizie e avvertiemti sulla configurazione del sistema:

```
Fedora Directory Server system tuning analysis version 04-APRIL-2005.

NOTICE : System is i686-unknown-linux2.6.23.8-63.fc8 (2 processors).

WARNING: 1008MB of physical memory is available on the system. 1024MB is
recommended for best performance on large production system.

NOTICE : The net.ipv4.tcp_keepalive_time is set to 7200000 milliseconds
(120 minutes).  This may cause temporary server congestion from lost
client connections.

WARNING: There are only 1024 file descriptors (hard limit) available,
which
limit the number of simultaneous connections.

WARNING: There are only 1024 file descriptors (soft limit) available,
which
limit the number of simultaneous connections.

Continue? (yes/no) yes
```

Digitare `yes` per continuare, a questo punto ci viene chiesto che tipo di installazione vogliamo effettuare:

```
Please select the install mode:
  1 - Express - minimal questions
  2 - Typical - some customization (default)
  3 - Custom - lots of customization

Please select 1, 2, or 3 (default: 2) 2
```

Per procedere con un'istalazione tipica digitiamo `2`, e di seguito ci viene

chiesto di inserire il nome host che sarà utilizzato per la macchina in cui è installato FDS:

```
Hostname to use (default: localhost.localdomain) fedora8.uninf.it
```

Il nome host assegnato, sarà `fedora8.uninf.it`. Successivamente ci viene richiesto di inserire un utente e un gruppo non privilegiati per il server LDAP:

```
Server user ID to use (defaults: nobody)
```

Premere invio per confermare l'utente di default, e alla richiesta del gruppo:

```
Server group ID to use (defaults: nobody)
```

Premere invio per confermare il gruppo di default. A questo punto verrà chiesto se si desidera memorizzare le informazioni di configurazione per questo server in un altro Fedora Directory Server di installazione:

```
Do you want to register this software with an existing Fedora
configuration directory server? [No]:
```

Premere invio, per installare la configurazione sulla macchina locale. Verrà chiesto se si vuole utilizzare un altro directory server, per memorizzare i dati:

```
Do you want to use another directory to store your data? [No]:
```

Premere invio, per accettare l'impostazione di default, per poter memorizzare i dati nella directory sul computer che si stà configurando.

In seguito verrà richiesto di inserire la porta su cui è in esecuzione il Directory Server:

```
Directory server network port [389]:
```

Premere invio, per confermare la porta di default 389, per le interazione con il Directory Server, utilizzando il protocollo LDAP. A questo punto verrà richiesto

di immettere l'identificativo del Directory Server:

```
Directory server identifier [fedora8]:
```

Premere invio per confermare il nome di default, o immetterer un nome diverso. E' usato per creare il nome dell'istanza, in questo caso "`slapd-fedora8`", è impossibile cambiare più tardi tale nome. Di default è il nome della macchina locale in cui è in esecuzione il FDS.

Successivamente verrà richiesto di immettere il nome per l'utente Amministratore del FDS:

```
Fedora configuration directory server
Administrator ID [admin]:
```

Premere invio per confermare la scelta di default, o immettere un ID utente diverso. A questo punto ci viene chiesto di inserire la password per tale utente:

```
Password: ********
Password (again): ********
```

Successivamente ci viene chiesto di specificare il suffisso per la l'albero della directory:

```
Suffix [dc=uninf, dc=it]:
```

Premere invio per confermare la scelta di default, o immettere un suffisso diverso. Successivamente ci viene chiesto di inserire il distinguished name per poter amministrare la directory:

```
Directory Manager DN [cn=Directory Manager]:
```

Premere invio per confermare la scelta proposta, oppure inserirne una diversa. Ci viene chiesta quindi la password da assegnare all'utente che ha la possibilità di amministrare la directory.

```
Password: ********
Password (again): ********
```

Arrivati a questo punto ci viene chiesto di fornire il dominio di amministrazione:

```
Administration Domain [unif.it]:
```

Anche in questo caso premere invio, o immettere una dominio di amministrazione differente. Quindi in seguito ci viene chiesto di inserire la porta per il server di amministrazione:

```
Administration port [28324]:
```

Premere invio per confermare la scelta proposta, oppure inserirne un nuovo valore per la porta. Ci viene chiesta se eseguire il server di amministrazione come root, in modo tale da avere ogni privilegio sulla macchina in esecuzione:

```
Run Administration Server as [root]:
```

Premere invio per confermare, oppure inserirne un nuovo utente. Arrivati a questo punto ci viene chieta l'ultima informazione, prima della fine della procedura di configurazione, che riguarda la locazione in cui si trova l'eseguibile per Apache:

```
Apache Directory [/usr/sbin]:
```

Premiamo invio, in quanto l'eseguibile, si trova proprio nel percorso fornitoci di default.

A questo punto l'utility avrà configurato il database, e avvierà il server LDAP (`ns-slapd`) e il server di amministrazione (`httpd`):

```
Hostname to use (default: localhost.localdomain) fedora8.uninf.it

Server user ID to use (default: nobody)

Server group ID to use (default: nobody)
```

```
[slapd-fedora8]: starting up server ...
[slapd-fedora8]:        Fedora-Directory/1.0.4 B2006.312.1539
[slapd-fedora8]:        fedora8.uninf.it:389 (/opt/fedora-ds/slapd-
fedora8)
[slapd-fedora8]:
[slapd-fedora8]: [22/Dec/2007:14:08:46 +0100] - Fedora-Directory/1.0.4
B2006.312.1539 starting up
[slapd-fedora8]: [22/Dec/2007:14:08:47 +0100] - slapd started.
Listening on All Interfaces port 389 for LDAP requests
Your new directory server has been started.
Created new Directory Server
Start Slapd Starting Slapd server configuration.
Success Slapd Added Directory Server information to Configuration
Server.
Configuring Administration Server...
Setting up Administration Server Instance...
Configuring Administration Tasks in Directory Server...
Configuring Global Parameters in Directory Server...
You can now use the console.  Here is the command to use to start the
console:
cd /opt/fedora-ds

./startconsole -u admin -a http://fedora8.uninf.it:28324/

INFO Finished with setup, logfile is setup/setup.log
```

A questo punto si dovrebbe essere in grado di connettere al server LDAP con "`cn=Directory manager`", utilizzando la password che è stata fornita precedentemente [19][22][23]. Una configurazione completa è riportata nell'appendice B.

4.6.1 Scripts SysV Init per Fedora DS

Arrivati a questo punto installiamo gli script SysV Init per rendere più agevole le operazioni di avvio e stop del Fedora DS e del Amministratore del Fedora DS. Per prima cosa scarichiamo gli strips dal sito http://directory.fedoraproject.org/ eseguendo i seguenti comandi, da shell, ovviamente da utente root:

```
wget http://www.directory.fedora.redhat.com/download/fedora-ds.init.d

wget http://www.directory.fedora.redhat.com/download/fedora-ds-admin-
```

```
init.d
```

Successivamente effettuiamo le seguenti operazioni per poter installare gli scripts nella directory contenete tutti gli Init scripts (`/etc/init.d/`):

```
chmod 755 FedoraDirectoryServer-init.d
cp FedoraDirectoryServer-init.d /etc/init.d/fedora-ds
chkconfig fedora-ds on

chmod 755 fedora-ds-admin-init.d
cp fedora-ds-admin-init.d /etc/init.d/fedora-ds-admin
chkconfig fedora-ds-admin on
```

Tramite l'installazione di tali scripts è possibile eseguire automaticamente all'avvio della macchina, il Fedora Directory Server. Come risulta evidente dall'immagine successiva tali impostazioni è possibile effettuarle tramite l'interfaccia grafica Webmin.

L'immagine precedete ci riporta la configurazione dei demoni che partono all'avvio della macchina, tra cui è possibile vedere i demoni relativi al Fedora Directory Server.

Tali scripts possono essere richiamati anche da shell, per gestire l'avvio, lo stop e il restart, del Fedora DS [24] [25].

```
[root@uninf mario]# /etc/init.d/fedora-ds stop
```

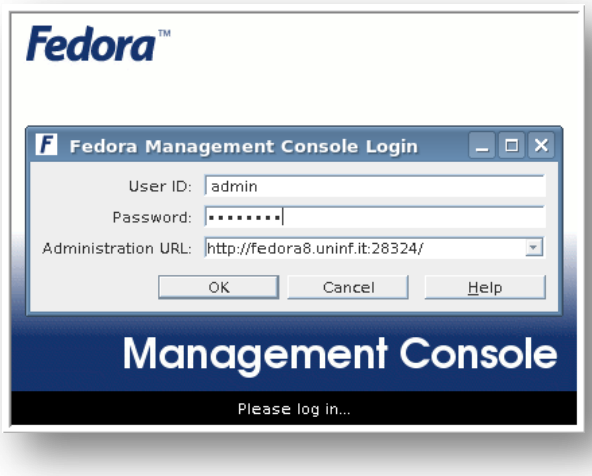
```
Stopping slapd trying: fedora8                             [  OK  ]
[root@uninf mario]# /etc/init.d/fedora-ds start
Starting slapd trying: fedora8                             [  OK  ]
[root@uninf mario]# /etc/init.d/fedora-ds-admin  restart
Riavvio di Fedora-DS Admin:                                [  OK  ]
```

4.7 Avvio e Configurazione della Console di FDS

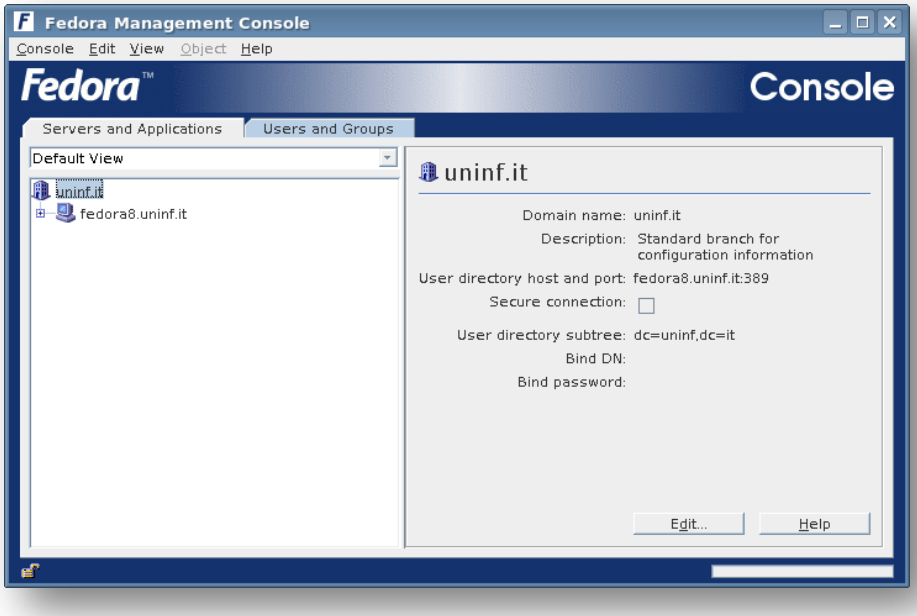
A questo punto siamo pronti per la prima esecuzione della console del Fedora Directory server. Quindi da shell digitiamo il seguente comando, che ci è stato fornito al momento in cui è terminata la configurazione del FDS, tramite script:

```
./startconsole –u admin –a http://fedora8.uninf.it:28324/
```

La directory per l'esecuzione del commando precedente ovviamente è `/opt/fedora-ds/`. Successivamente verrà mostrata la seguente immagine, in cui per poter accedere effettivamente alla Console, occorrerà fornire la password:



Inseriamo quindi la password relativa all'utente *admin*, ossia l'utente creato per la gestione del Fedora Directory Server, ed entriamo nella console cliccando su "*Ok*". Quindi la schermata principale, per la gestione del Fedora Directory Server, viene mostrata nell'immagine successiva:



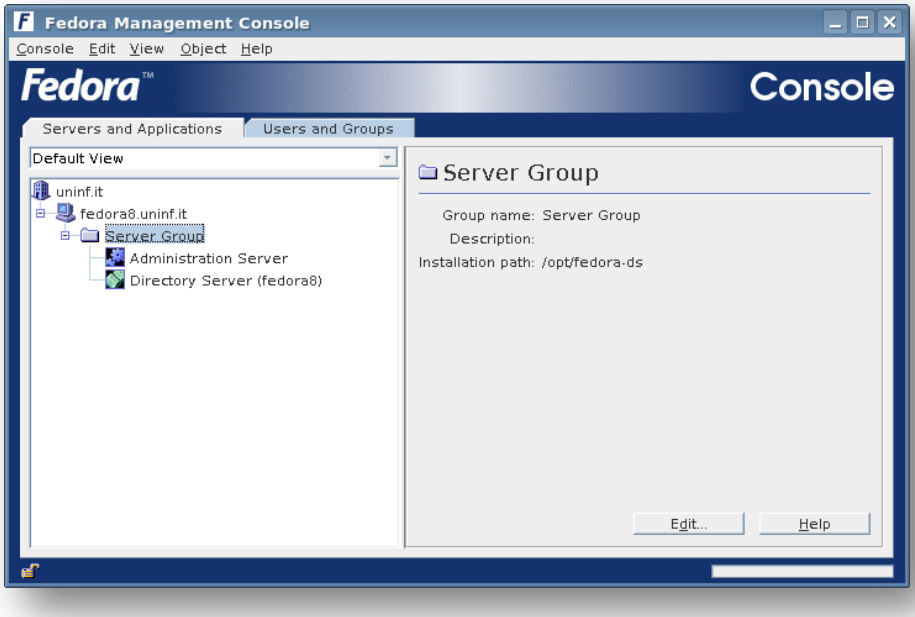
Dopo aver eseguito l'accesso al Server di Amministrazione, viene mostrata la console di Fedora Directory Server. La schermata principale della console presenta cinque menù (*Console*, *Edit*, *View*, *Object* e *Help*), nella tabella seguente è riportata una breve descrizione di tali funzioni.

Console	Aggiunge o rimuove elementi dall'albero di navigazione.
Edit	Imposta le preferenze generali per la Fedora Console.
View	Modificare l'aspetto principale delle finestre della Fedora Console.
Object	Svolgere le attività connesse alla gestione delle risorse, quali domini amministrativi, server di gruppi, e servers.
Help	Ottenere assistenza online mentre si usa la Fedora Console.

Come è possibile vedre nell'immagine precedente, la finestra principale della console di Fedora Console ha due schede: "*Server e Application*" e "*Users and Groups*". La scheda "*Server e Application*" contiene un albero di navigazione e

un pannello di informazioni. Invece la scheda "*Users and Groups*" ha un'interfaccia per gestire le entry nella directory utente.

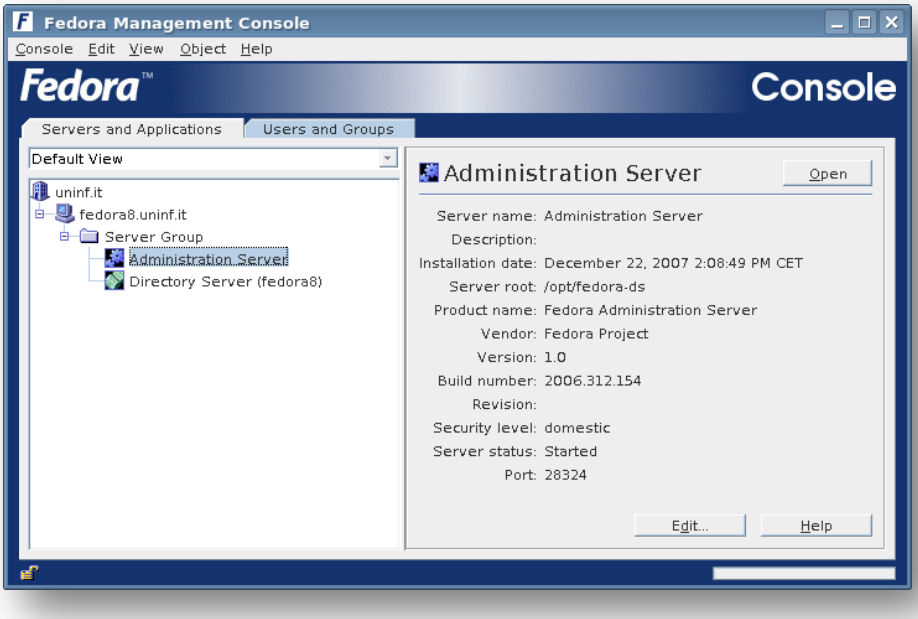
La scheda "*Server e Application*" consiste in un albero di navigazione e in un pannello di informazioni. L'albero di navigazione rappresenta una *topologia*. Una topologia è una struttura gerarchica che rappresenta tutte le risorse, o gli oggetti (ad esempio, i server, le applicazioni e gli host), che vengono registrati in una directory di configurazione. Si può utilizzare l'albero di navigazione per cercare le risorsa con cui si desidera lavorare. Un tipo di risorsa in una topologia è un *dominio di amministrazione*. Un dominio di amministrazione è un insieme di sistemi host e server che condividono la stessa directory utente.



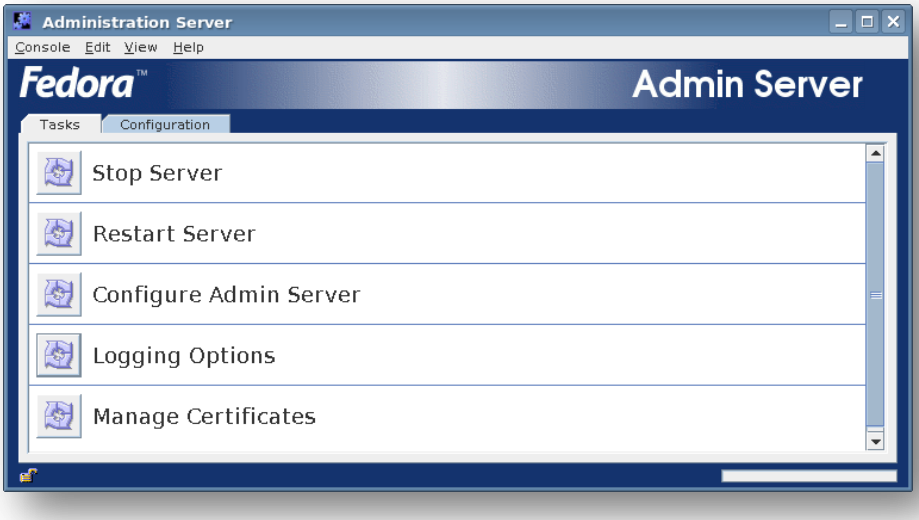
Un certo numero di *gruppi di server* possono esistere all'interno di un dominio di amministrazione. Un gruppo di server è costituito da tutti i server che sono gestiti da una comune istanza di un Server di Amministrazione e condividono una cartella root nel server. I singoli *servers* in un gruppo di server sono istanze di server, che forniscono servizi specifici, come servizi di directory database, la messaggistica, e la pubblicazione. Sul lato destro della scheda "*Server e Application*" c'è il *pannello di informazioni*. Quando si seleziona

un'amministratore di dominio, host, e gruppo di server, o un'istanza del server nell'albero di navigazione, il pannello visualizza le relative informazioni dettagliate. A seconda della risorsa selezionata, è possibile modificare tutti o alcuni di questi dettagli.

Nell'immagine successiva sono visibili le impostazioni relative al server di amministrazione. Cliccando su "*Open*" viene mostrata la schermata di gestione del Server di Amministarazione, visibile nell'immagine seguente. Come evidente sono presenti due schede "*Tasks*" e "*Configuration*" analizzandole più attentamente è possibile notare che le impostazioni sono le medesime, l'unica differenza è che con la scheda "*Configuration*" è possibile anche visualizzare i log di accesso e di errore.



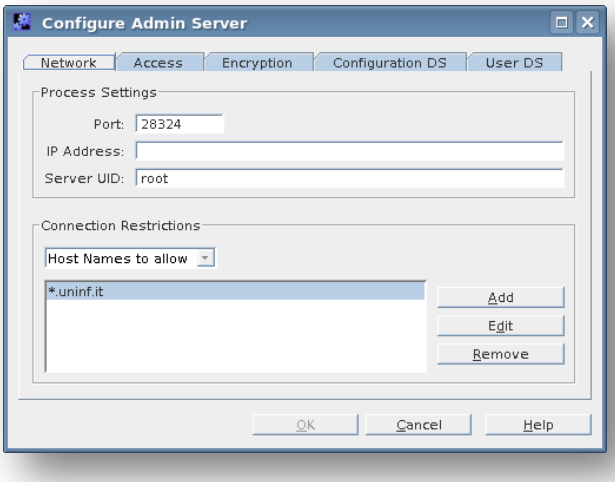
Descriverò soltanto le opzioni messe a disposizione della scheda "*Tasks*" che sono identiche a quelle della scheda "*Configuration*". Aperta la scheda "*Tasks*" sono presenti le opzioni per: fermare il server, riavviarlo, configurare il server di amministrazione, impostare le opzioni per il logging, e gestire i certificati digitali.



Cliccando su "*Stop Server*" viene semplicemente fermato il server, su "*Restart Server*" invece riavviato. E' possibile effettuare le stesse operazioni tramite shell, invocando i seguenti comandi:

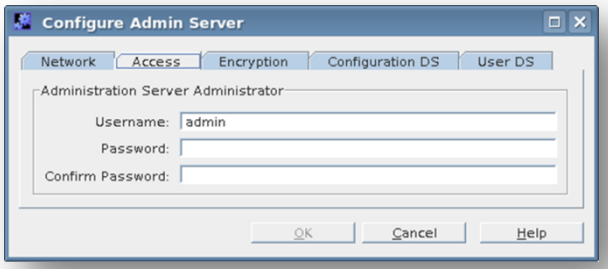
```
[root@uninf fedora-ds]# ./stop-admin
[root@uninf fedora-ds]# ./restart-admin
```

Cliccandi su "*Configure Admin Server*" sia apre la seguente schermata, in cui è possiblie impostare diversi paramentri di configurazione del Server di Amministrazione.



La scheda "*Network*" riporta le imostazioni che sono state configurare

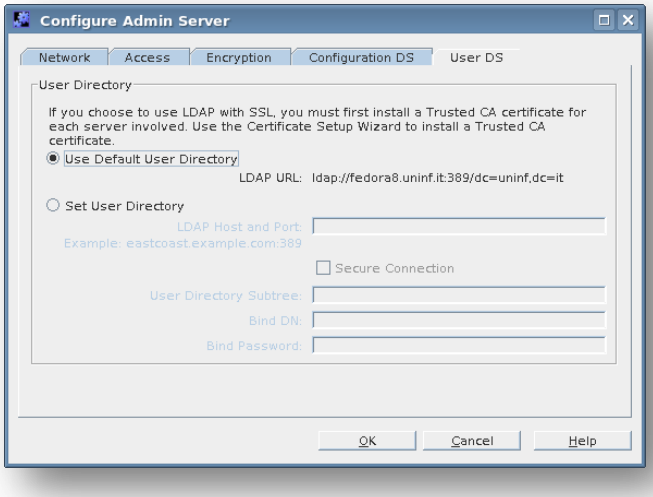
tramite l'utility di configurazione iniziale e tramite tale scheda è possibile quindi cambiare il "*Port Number*" ossia il numero di porta su cui è in esecuzione il server di amministrazione e il "*Connection Restrictions*" con il quale è possibile impostare gli hosts che hanno la possbilità di connettersi con l'istanza del server di amministrazione. Nella scheda "*Access*", visibile nell'immagine successiva, è possibile cambiare la password per l'utente admin, ossia l'utente amministratore.



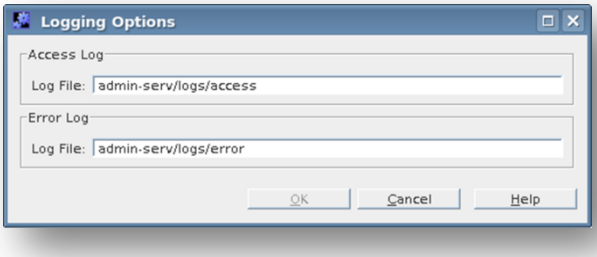
Nella scheda "*Encryption*", viene abilitata la crittografia basata su SSL, per il server e impostate le preferenze per il client, come risulta evidente nell'immagine seguente.

La scheda "*Configuration DS*" visibile nell'immagine successiva, ci permette di cambiare il nome host e la porta in cui è in esecuzione una directory LDAP. In questo caso vengono lasciati i valori visualizzati, in quando noi lavoriamo con una directory LDAP in esecuzione sul computer locale.

L'ultima scheda disponibile è "*User DS*", con il quale è possibile impostare l'URL LDAP di partenza, con il quale l'utente può interrogare la directory. L'asciamo la configurazione di default, come visibile nell'immagine seguente.

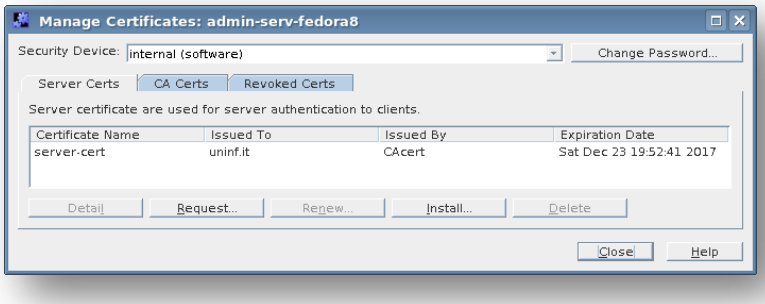


Tornando nella schermata principale, cliccando su "*Logging Options*" è possibile impostare i percorsi per i log di accesso e di errore.

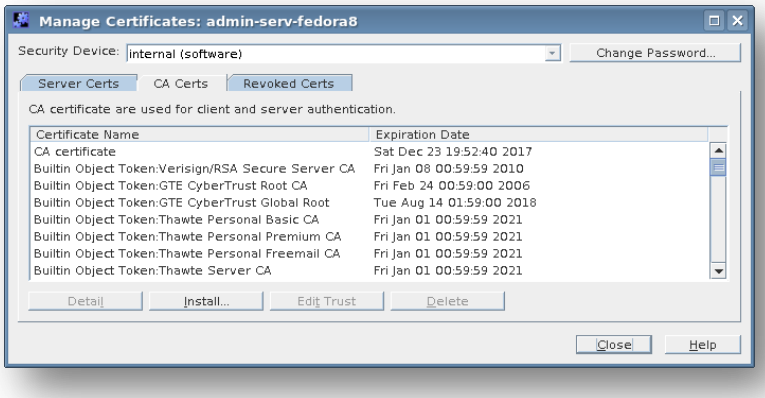


Mentre cliccando su "*Manage Certificates*" è possibile gestire i certificati

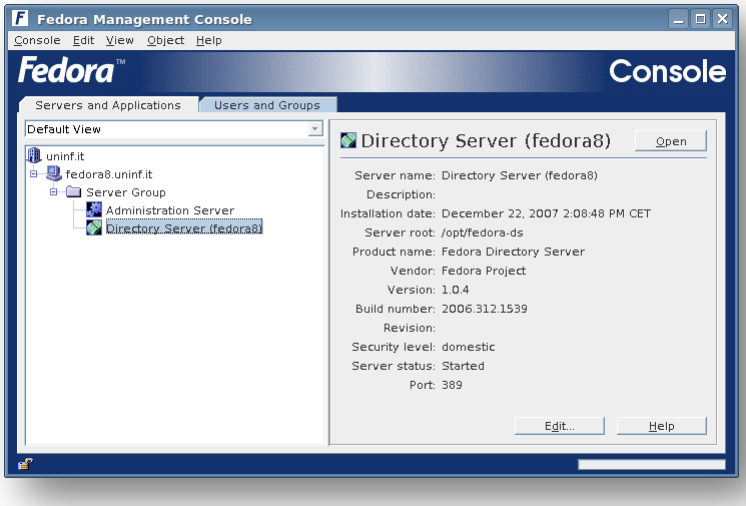
digitali.



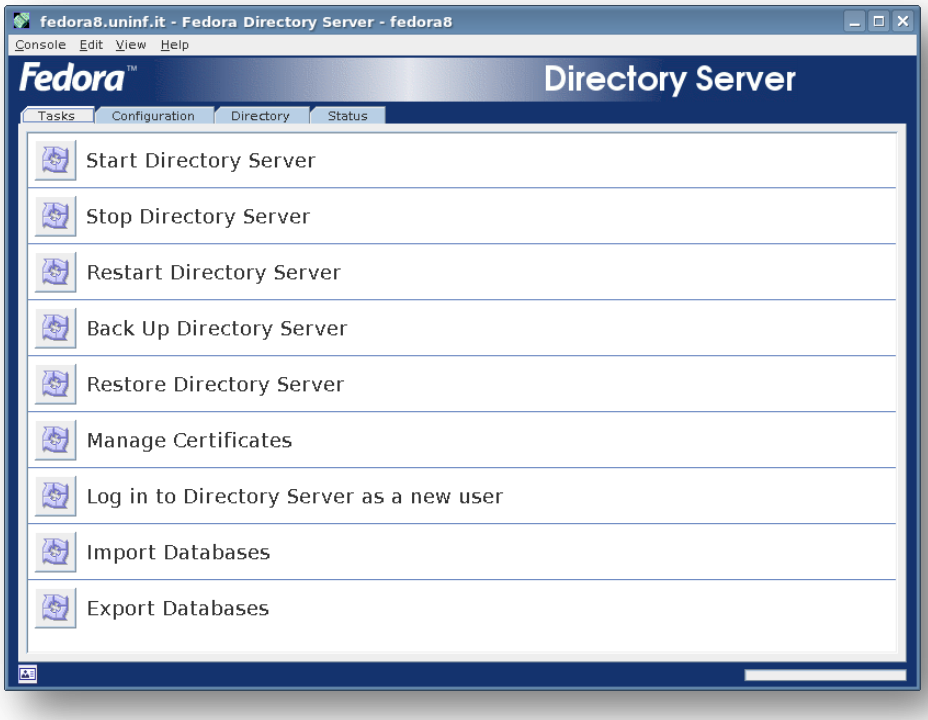
Nell'immagine precedente è visibile il certificato del server che è possibile utilizzare per l'autenticazione del server ai clients. L'immagine successiva invece mostra i certificati utilizzati per le autenticazioni dei clients e dei servers.



Nell'immagine successiva sono visibili le impostazioni relative al server di directory (fedora8).

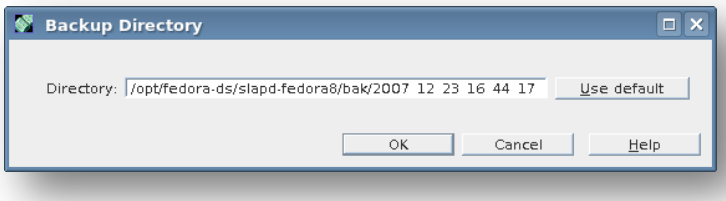


Cliccando su "*Open*" viene mostrata la schermata di gestione del Server di Directory, visibile nell'immagine seguente.

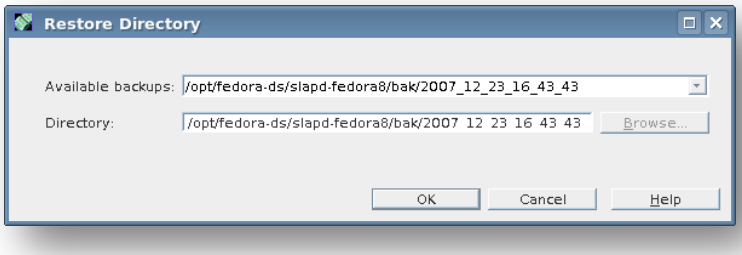


Come risulta evidente anche dall'immagine sono presenti quattro schede: "*Tasks*", "*Configuration*", "*Directory*", "*Status*" di seguito verrano descritte più dettagliatamente, partiamo con la descrizione della scheda "*Tasks*". Essa presenta le opzioni visibile nell'immagine. Iniziamo con il descriverle. Le prime tre sono

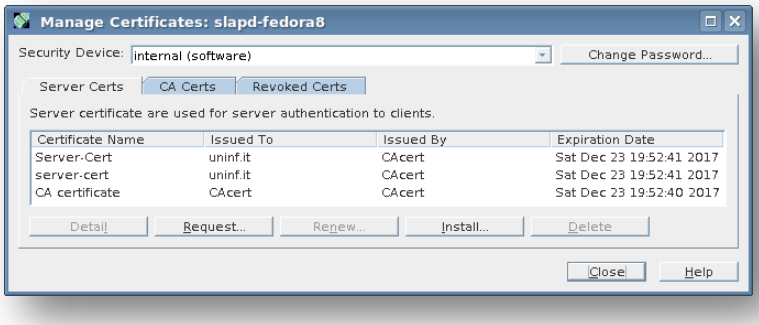
abbastanza semplici e ci permettono di avviare il server di Directory, cliccando su "*Start Directory Server*", fermarlo cliccando su "*Stop Directory Server*" e riavviarlo cliccando su "*Restart Directory Server*". La quarta opzione "*Back Up Directory Server*", visibile nell'immagine, ci permette di effettuare il backup dell'intera directory.



Mentre la quinta opzione "*Restore Directory Server*", visibile nell'immagine successiva, ci permette di ripristinare l'intera directory, precedentemente salvata.

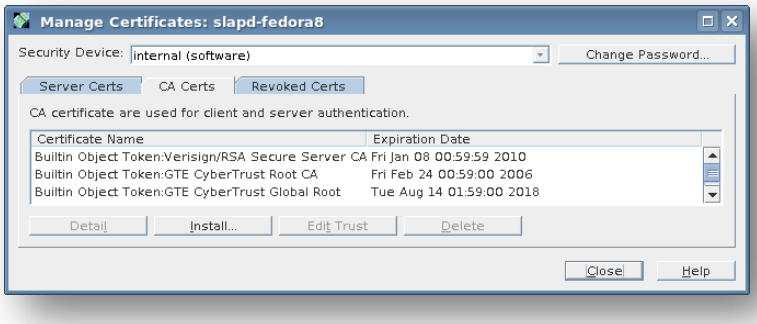


La sesta opzione "*Manage Certificate*" ci permette di gestire i certificati digitali.

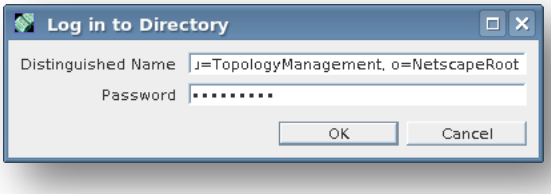


L'immagine precedente riporta i certificati del server che è possibile utilizzare per l'autenticazione del server ai clients. L'immagine successiva invece

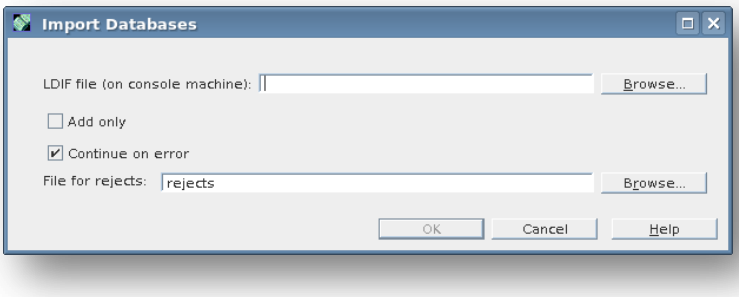
mostra i certificati utilizzati per le autenticazioni dei clients e dei servers.



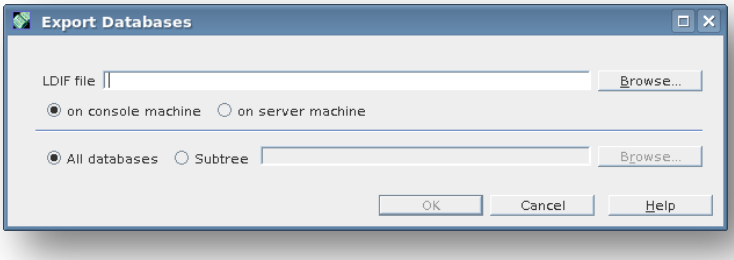
La settima opzione "*Log in to Directory Server as a new user*" ci permette di loggarci alla directory, con un diverso utente.



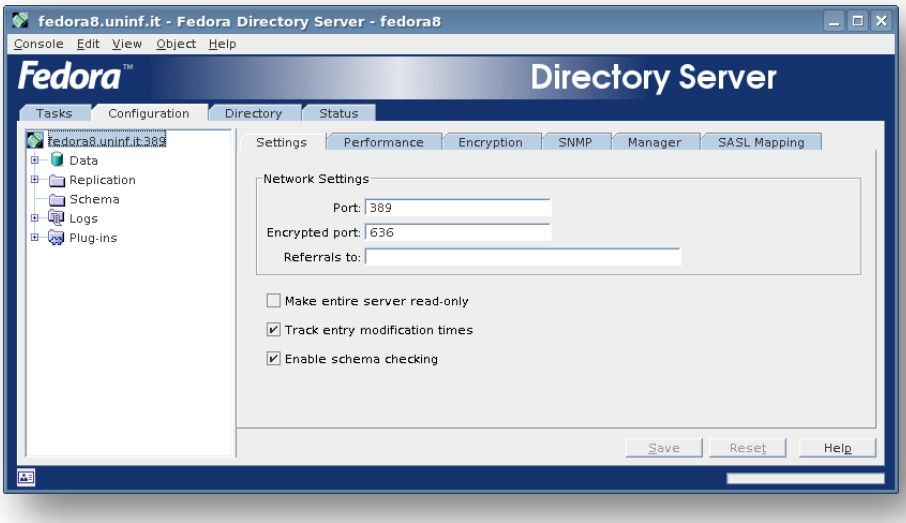
L'ottava opzione "*Import Databases*" ci permette di importare un nouvo database utilizzando un file LDIF.



La nona e ultima opzione "*Export Databases*" ci permette di esportare il database presente sulla macchina corrente, utilizzando un file LDIF.



Sulla scheda principale "*Configuration*" è possibile impostare parecchi paramentri relativi alla directory locale. Come risulta evidente anche dall'immagine, l'interfaccia è divisa in due parti, la parte di sinistra in cui è presente un'albero di navigazione e la parte di destra che riporte le informazioni relative all'elemento selezionato nell'albero di navigazione.



Come risulta evidente anche dall'immagine sono presenti sei schede: "*Settings*", "*Performance*", "*Encryption*", "*SNMP*", "*Manager*" e "*SALS Mapping*".

- La scheda "*Settings*" ci permette di impostare le porte per il protocollo LDAP e LDAPS, per interrogare la directory. E altre opzioni relative alle entries memorizzate nella directory e allo schema.

- La scheda "*Performance*" ci permette di impostare alcuni paramentri, per

ottimizzare le prestazioni, relativi al numero di entries memorizzabili nella directory, il tempo limite, il tempo idle, e il numero massimo di file descrittori.

- La scheda "*Performance*" ci permette di impostare alcuni paramentri, relativi al numero di entries memorizzabili nella directory, il tempo limite, il tempo idle, e il numero massimo di file descrittori.

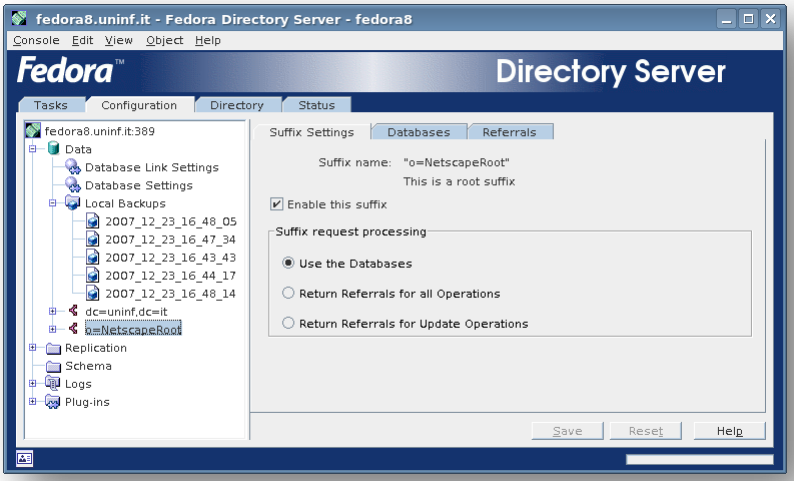
- La scheda "*Encryption*" ci permette di impostare i paramentri relativi ai certificati digitali, per comunicazioni crittografate tra il server di directory e i clients.

- La scheda "*SNMP*" ci permette di impostare i paramentri per monitorare il Fedora Directory Server tramite l'SNMP.

- La scheda "*Manager*" ci permette di impostare il DN per il gestore della directory, l'algoritmo di criptazione per la password, e la password stessa.

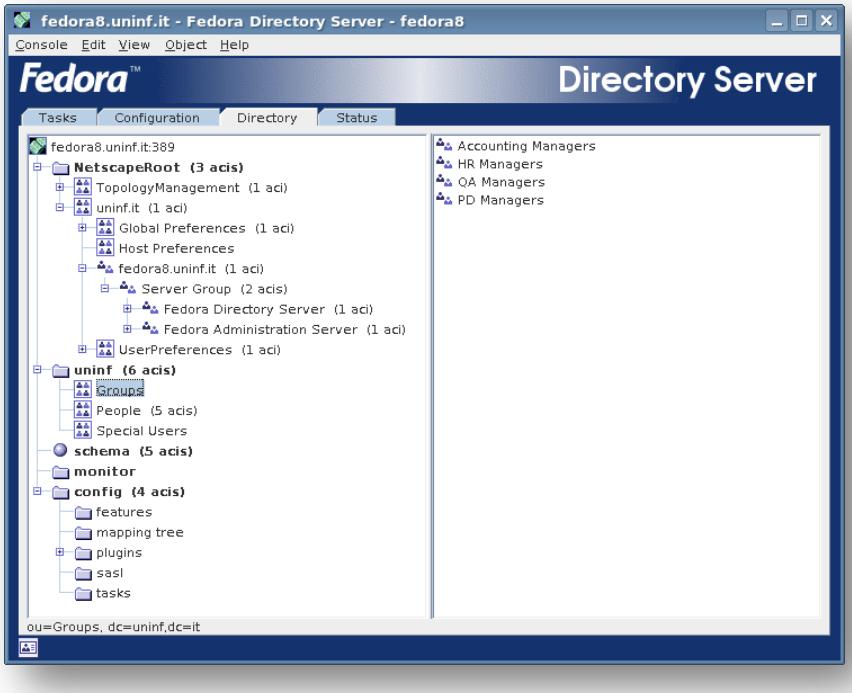
- La scheda "*SASL Mapping*" ci permette di impostare i parametri relativi all'autenticazione tramite ticket Kerberos5.

Comunque per ogni elemento presente nell'albero di navigazione è possibile applicare delle impostazioni personalizzate in base alle proprie esigenze. Ad esempio si ha le seguenti informazioni relative al suffisso radice della directory.

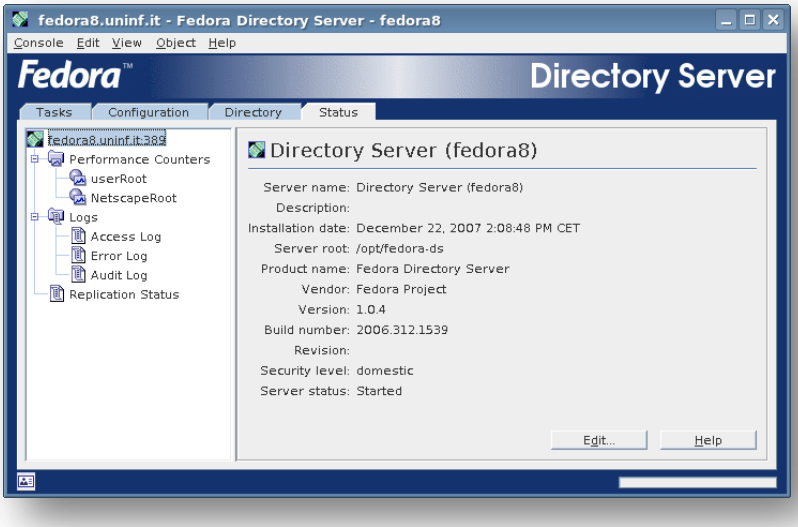


Come risulta evidente è possibile abilitare o meno tale suffisso e impostare altre opzioni realtive ad esso. Nel albero di navigazione sono anche evidenti i backup della directory locale e altri elementi "*Replication*", "*Schema*", "*Logs*", e "*Plug-ins*", a cui è possibile personalizzare la configurazione a seconda delle proprie esigenze.

Tornando sulla schermata principale è possibile cliccare sulla scheda "*Directory*", visibile nell'immagine sottostante, che ci permentte di navigare nella struttura gerarchica dell'albero che costituisce la directory locale.



Come risulta evidente, nel albero di navigazione a sinistra, è stato selezionata l'entry *Groups*, quindi a destra ci viene mostrato il contenuto di tale entry. Infine l'ultimo scheda presente è "*Status*" che ci mostra tutte le informazioni relative alla directory, comprendente i valori di prestazioni della directory, i file di log e lo stato della replicazione.

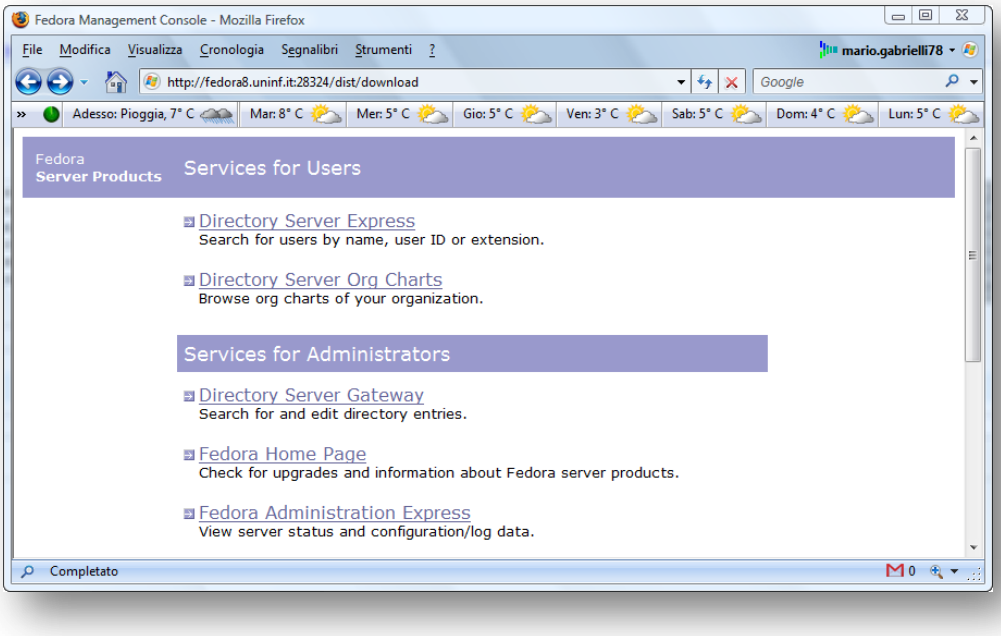


4.8 Amministrazione del FDS Tramite HTTP

L'amministrazione espressa è una pagina HTML basata sulla versione di Fedora Console, che fornisce accesso rapido al server. L'amministrazione espressa è accessibile comodamente tramite browser web, il qualsiasi computer della rete che ha l'accesso al Fedora Directory Server. L'URL per accedere a tale interfaccia è la seguente:

```
http://fedora8.uninf.it:28324/
```

Se l'istanza del server di amministrazione a cui si ha accesso utilizza SSL, è possibile che venga richiesto di confermare l'accettazione del certificato. Inoltre, se il server è configurato per richiedere l'autenticazione dei client, può essere richiesto di presentare un certificato client. Tipicamente, l'accettazione dei certificati server avviene attraverso le finestre di dialogo, mentre per i certificati client comporta una selezione da un elenco a discesa. L'immagine successiva riporta la pagina iniziale in cui sono riassunte tutte le operazioni gestibili, tramite tale interfaccia.



Di seguito viene riportato il riassunto delle opzioni utilizzabili:

- **Directory Server Express**: con tale opzione è possible ricercare utenti, con i rispettivi valori, memorizzati all'interno di FDS.

- **Directory Server Org Charts**: con la tale opzione è possibile ricercare gli utenti e visualizzare un grafico relativo all'organizzazione dell'azienda.

- **Directory Server Gateway**: con tale opzione è possibile ricercare in modo più dettagliato, ogni elemento memorizzato nell'albero di directory, modificarlo e aggiungerne di nuovi.

- **Fedora Home Page**: con tale opzione è possibile accedere immediatamente alla paginaweb principale di FDS presente in Internet.

- **Fedora Administration Express**: tale opzione è la più interessante in quanto ci permette di gestire diversi aspetti dell'amminstrazione del server.

Tramite il collegamento "*Fedora Administration Express*", è possibile eseguire quattro compiti, principali di amministrazione:

- Avvio del server (ad eccezione del caso in cui il server di amministrazione, è fermo, deve essere avviato da riga di comando);

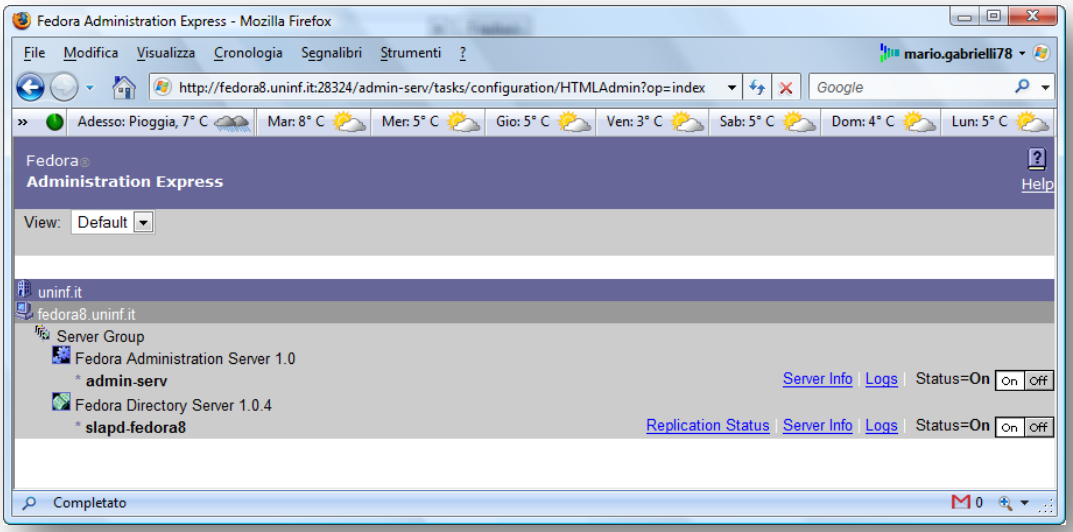
- Stop di server;

- Visualizzazione delle informazioni di base del server, come il nome, la descrizione, e la cartella di installazione;

- Visualizzazione dei log.

Per poter accedere all'amministrazione occorre comunque fornire le credenziali, login e password, vediamo un esempio, del server di amministrazione, nell'immagine seguente.

Se l'istanza del server di amministrazione utilizza SSL, è possibile che venga richiesto di confermare l'accettazione del certificato. Inoltre, se il server è configurato per richiedere l'autenticazione dei client, può essere richiesto di presentare un certificato da parte del client. Tipicamente, l'accettazione dei certificati server avviene attraverso le finestre di dialogo, mentre per i certificato client comporta una selezione da un elenco a discesa.



In alternativa all'interfaccia web "*Administration Express*", per poter gestire e amministrare da remoto il FDS, è possibile scaricare dal sito http://directory.fedoraproject.org/wiki/Download il file: *FedoraConsole.msi*. L'installazione di tale file, ci fornisce la possibilità di utilizzare la stessa console precedentemente descritta del FDS, sotto qualsiasi sistema Windows, e quindi connettersi al server FDS per qualsiasi gestione [26].

4.9 Configurazione del Servizio SSL di Fedora DS

Arrivati a questo punto il Fedora Directory Server è configurato per accettare interrogazioni LDAP in chiaro sulla porta 389. Per aumentare la sicurezza delle

comunicazioni tra il server di directory e i clients, è possibile abilitare una comincazione crittografata LDAPS sulla porta 636. Per automatizzare il più possibile la procedura è possibile scaricare lo script *setupssl.sh* dalla pagina web: http://directory.fedoraproject.org/download/setupssl.sh. Tale script crea tutti i certificati necessari. Questa procedura memorizza tutte le chiavi-certificati dei databases di tutti i servers, all'interno della directory "`/opt/fedora-ds/alias/`" e identifica ognuno di essi, tramite un unico prefisso. Vediamo come effettuare l'operazione. Innanzitutto eseguiamo lo script come segue:

```
[root@unif fedora-ds]# ./setupssl.sh
```

Durate la creazione dei certificate, ci viene chiesto di fornire la password per LDAP, inseriamo la password relativa al Directory Manager, come segue:

```
Enter LDAP Password:********
```

A questo punto lo script termina e ci restituisce alcune informazioni, relative alle modifiche e all'aggiunta fatta nell'albero della directory, visibile di seguito:

```
modifying entry "cn=encryption,cn=config"

modifying entry "cn=config"

adding new entry "cn=RSA,cn=encryption,cn=config"
```

Infine per rendere effettive le modifiche occorre far ripartire il server di amministrazione e il server di directory, eseguendo i seguenti comandi da shell [27].

```
[root@unif fedora-ds]# /etc/init.d/fedora-ds restart
[root@unif fedora-ds]# /etc/init.d/fedora-ds-admin restart
```

CAPITOLO 5

INTERAZIONE CON I DIRECTORY SERVICES

5.1 Gestione Utenti e Gruppi in Active Directory

5.1.1 Creazione e modifica di account utente

Prima di poter accedere alle risorse di rete, Active Directory richiede la verifica dell'identità della persona che desidera accedere, un processo più comunemente noto come autenticazione. Alla base dell'autenticazione vi è l'account utente, con i relativi nome di accesso utente, password e identificativo di protezione (SID) univoco. Durante l'accesso, Active Directory autentica un utente utilizzando il nome utente e la password forniti. Ad autenticazione avvenuta, il sottosistema di protezione di Windows Server 2003 crea un token di accesso di protezione che rappresenta l'utente autenticato sulla rete. Questo token di accesso contiene il SID dell'account utente e i SID dei gruppi a cui appartiene l'utente.

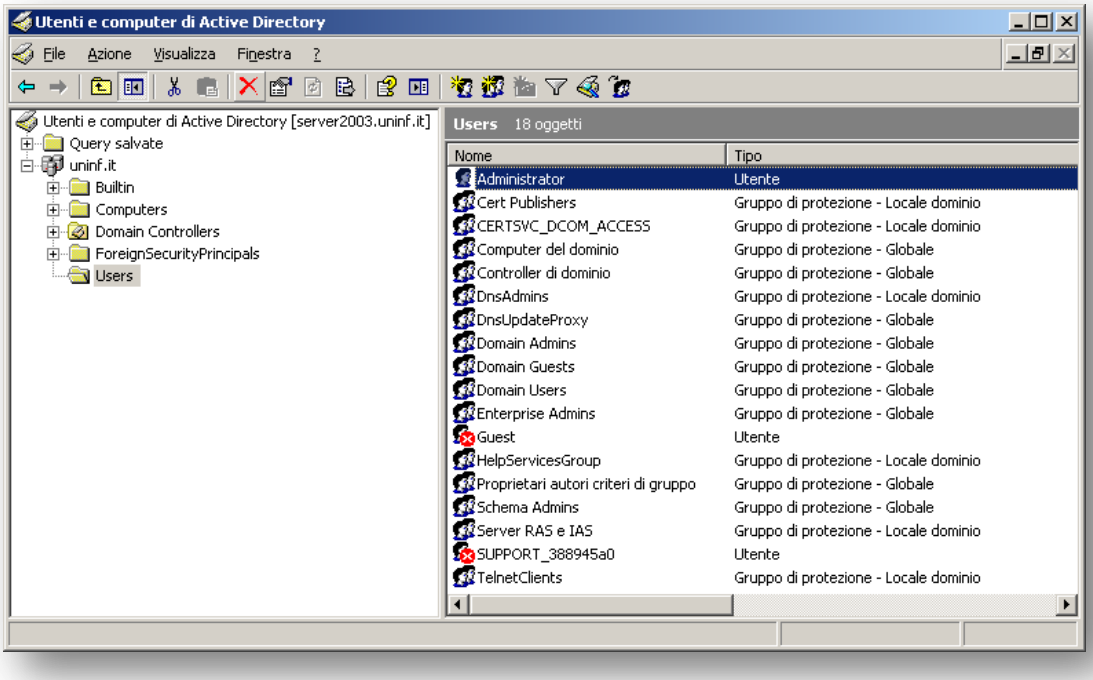
Questo token viene utilizzato per verificare le assegnazioni dei diritti utente e per autorizzare l'accesso alle risorse protette dagli elenchi di controllo di accesso (ACL).

In Active Directory, un utente viene rappresentato mediante un oggetto utente. Un oggetto utente include, oltre al nome utente, alla password e al SID, anche informazioni personali, come numeri telefonici e indirizzi, informazioni sull'appartenenza ai gruppi, impostazioni di ambiente e altro ancora.

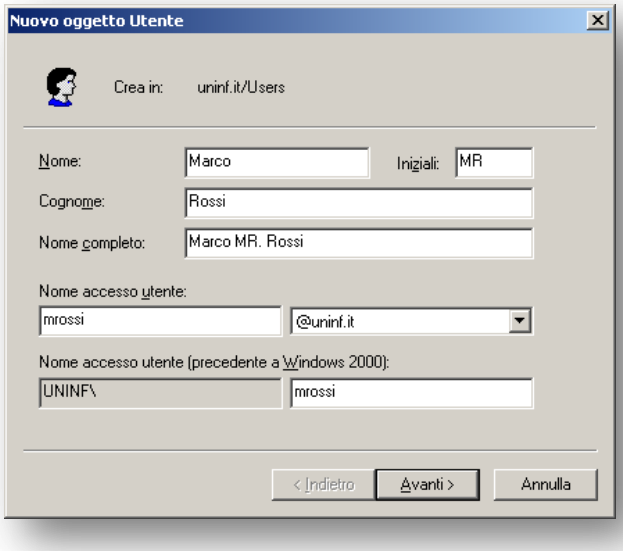
IL principale strumento utilizzato per la creazione di oggetti utente è lo snap-in Utenti e computer di Active Directory. Sebbene sia possibile creare oggetti utente nella directory principale di un dominio, oppure di qualsiasi contenitore predefinito, di solito è consigliabile inserire gli oggetti utente in un unità

organizzative per sfruttare a pieno la possibilità di delegare l'autorità amministrative e di distribuire le impostazioni dei Criteri di gruppo.

L'immagine successiva riporta la schermata principale che riporta tutti gli utenti registrati in Active Directory, raggiungibile cliccando su "*Start*"→"*Strumenti di amministrazione*"→"*Utenti e computer di Active Directory*" e poi selezionando nell'albero di sinistra la cartella "*Users*".



Per creare un oggetto utente, si clicca con il pulsante destro del mouse sul contenitore in cui si desidera creare l'oggetto, si seleziona "*Nuovo*", quindi si clicca su "*Utente*". Viene visualizzata la finestra di dialogo "*Nuovo oggetto Utente*", come illustrato nell'immagine successiva.



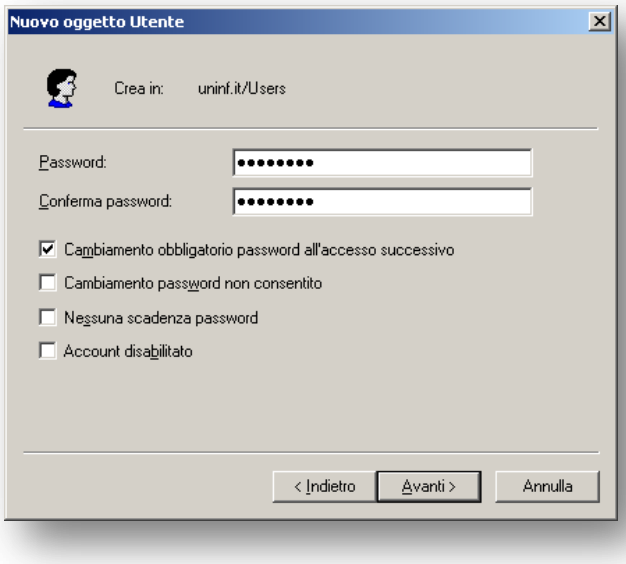
Tale immagine riporta la creazione dell'utente Marco Rossi. Quindi la prima pagina di questa finestra di dialogo contiene proprietà relative al nome utente. Descriviamo di seguito il significato di ogni campo della finestra.

- Nome: Il nome dell'utente.
- *Iniziali*: Le iniziali del nome dell'utente.
- *Cognome*: Il cognome dell'utente.
- *Nome Completo*: Il nome completo dell'utente. Se si specifica un valore per il nome o il cognome, questo campo viene completato automaticamente. Questo campo è obbligatorio. Il nome digitato in questo campo definisce l'impostazione di numerose proprietà dell'oggetto utente, il particolare *CN* (nome comune), *DN* (nome distinto), nome e *NomeVisualizzato*. Poiché CN deve essere un nome univoco all'interno del contenitore, il nome fornito in questo campo deve essere univoco rispetto a tutti gli altri oggetti dell'unità organizzative (o in un contenitore) in cui si crea l'oggetto utente.
- *Nome accesso utente*: Il nome principale dell'utente (UPN) è formato da un nome di accesso e da un suffisso UPN che, per impostazione predefinita, è il

nome Domain Name Syste (DNS) del dominio in cui si crea l'oggetto. Questa proprietà è obbligatoria e l'intero UPN, nel formato *nome-accesso@UPN-suffisso*, deve essere univoco all'interno dell'insieme di strutture di Active Directory. L'UPN può essere utilizzato per effettuare l'accesso da qualsiasi computer sul quale sia in esecuzione Windows 2000, Windows XP o Windows Server 2003.

- *Nome accesso utente (Precedente a Windows 2000)*: Questo nome di accesso viene utilizzato per accedere da client sui quali sono in esecuzione versioni precedenti del sistema operativo Windows. Si tratta di un campo obbligatorio e il valore specificato deve essere univoco all'interno del dominio.

Dopo aver immesso tali valori si clicca su "Avanti >" e compare la seconda pagina della finestra di dialogo, visibile nell'immagine successiva, in cui è possibile specificare la password utente e impostare i flag per l'account.



Descriviamo di seguito il significato di ogni campo della finestra.

- *Password*: La password utilizzata per autenticare l'utente. Per motivi di sicurezza,

occorre sempre assegnare una password. Quando si digita la password, questa non viene visualizzata in chiaro.

- *Conferma password*: Conferma la password digitandola una seconda volta, senza commettere errori di digitazione.

- *Cambiamento obbligatorio password all'accesso successivo*: Seleziona questa casella di controllo se si desidera che l'utente cambi la password immessa la prima volta che effettua l'accesso. Non è possibile selezionare questa opzione se si è selezionato *Nessuna scadenza password*. Selezionado questa opzione, verrà automaticamente deselezionata l'opzione *Cambiamento password non consentito*: infatti, le due opzioni si escludono a vicenda.

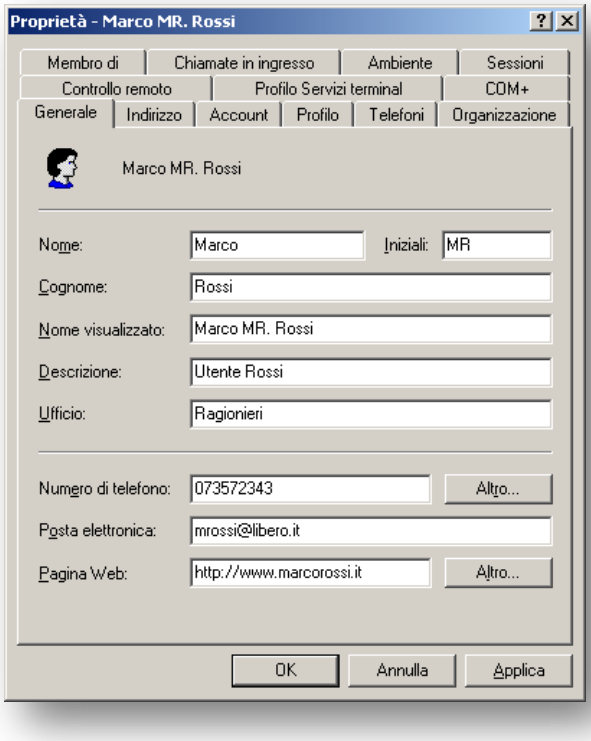
- *Cambia password non consentito*: Selezionare questa casella di controllo se ci sono più persone che utilizzano lo stesso account utente di dominio, oppure per esercitare un controllo sulle password degli account utente. Questa opzione viene comunemente utilizzata per gestire la password degli account di servizio. Non è possibile selezionare questa opzione se si è selezionato *Cambiamento obbligatorio password all'accesso successivo*.

- *Nessun cambiamento password*: Selezioanre questa casella di controllo se si desidera che la password non abbia nessuna scadenza. Questa opzione deselezionerà automaticamente l'impostazione Cambbbligatorio password all'accesso successivo, in quando le due opzioni si escludono a vicenda. Questa opzione viene comunemente utilizzata per gestire le password degli account di servizio.

- *Account disabilitato*: Selezioanre questa casella di controllo per disabilitare l'account utente: ad esempio, quando si crea un oggetto per un dipendente appena assunto che ancora non ha bisogno di accedere alla rete.

Quando si crea un nuovo utente, viene inizialmente richiesto di configurare le proprietà più comuni per l'oggetto utente, tra cui i nomi di accesso e una password. Tuttavia, gli oggetti utente supportano molte altre proprietà, che possono essere configurate in qualsiasi momento utilizzando "*Utenti e computer di Active Directory*". Questa proprietà agevola l'amministrazione degli oggetti utente e consentono inoltre di ricercare oggetti attraverso query LDAP.

Per configurare le proprietà di un oggetto utente, clicchiamo con il tasto destro del mouse su di esso, e scegliere "*Proprietà*", viene visualizzata la finestra di dialogo relativa alle proprietà dell'utente, visibile nell'immagine.



Le pagine di questa finestra di dialogo contengono le impostazioni configurabili, che si suddividono nelle seguenti categorie:

- **Proprietà dell'account: scheda Account**. Questa scheda consente di configurare le impostazioni che sono state originariamente definite durante la creazione di un nuovo oggetto utente, compresi i nomi di accesso, la

password e i flag per l'account.

- **Informazioni personali: scheda Generale, Indirizzo, Telefoni e Organizzazione**. La scheda Generale espone le proprietà relative ai nomi che vengono configurate quando si crea un oggetto utente. Le schede Indirizzo, Telefoni e Organizzazioni consentono di configurare impostazioni che si prevede queste schede contengano.

- **Gestione della configurazione utente: scheda Profilo.** Questa scheda viene utilizzata per configurare il percorso del profilo, lo script di accesso e il percorso della home directory relativi a un utente.

- **Appartenenza ai gruppi: schema membro di.** Questa scheda viene utilizzata per configurare i gruppi di protezione ai quali l'utente appartiene.

- **Servizi terminal: schede Profilo Servizi terminal, Ambiente, Controllo remoto e Sessioni.** Queste quattro schede consentono di configurare e gestire le impostazioni dell'ambiente utente per sessione di Servizi terminal.

- **Accesso remoto: scheda Chiamate in ingresso.** Questa scheda consente di abilitare e configurare l'autorizzazione di accesso remoto per utente.

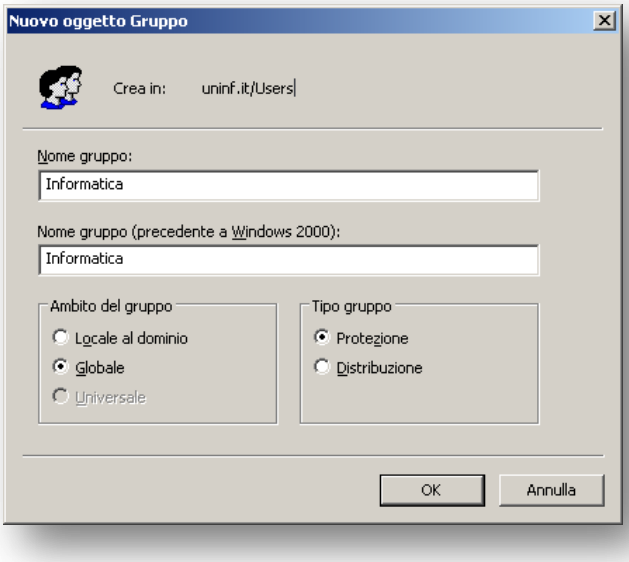
- **Applicazioni: scheda COM+.** Questa scheda, nuova in Windows Server 2003, agevola la gestione di applicazioni distribuite assegnando all'utente set di partizioni COM+ di Active Directory.

5.1.2 Creazione e modifica dei gruppi di protezione

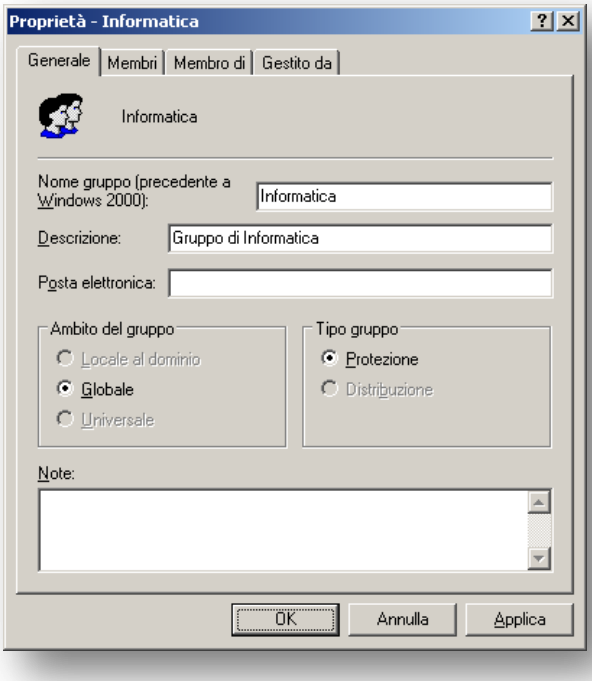
Il principale strumento utilizzato per creare gruppi in Windows Server 2003 è lo snap-in "*Utenti e computer di Active Directory*". Analogamente agli utente, è possibile creare nuovi oggetti gruppo nella directory principale del dominio, in uno qualunque dei contenitori predefiniti oppure nelle unità organizzative che sono state definite. Per creare un nuovo gruppo, è sufficiente fare clic con il pulsante destro

del mouse sul contenitore in cui si desidera creare il gruppo, selezionare "*Nuovo*", quindi fare clic su "*Gruppo*".

Quando il dominio è configurato per il livello di funzionalità di dominio Windows 2000 nativo o Windows Server 2003, nella finestra "*Nuovo oggetto Gruppo*" vengono impostati automaticamente l'ambiente globale e il tipo protezione. Se il livello di funzionalità di dominio è impostato su Windows 2000 misto o Windows Server 2003, non è possibile selezionare l'ambiente gruppo universale, come visibile nell'immagine seguente.



Quando si crea un nuovo gruppo di qualunque tipo di ambiente, è necessario fornire un nome che sia univoco all'intero del dominio. Quando si digita questo nome nel campo "*Nome gruppo*", lo stesso nome viene automaticamente inserito nel campo "*Nome gruppo (precedente a Windows 2000)*". Dopo aver creato un gruppo, è possibile visualizzare e modificare le proprietà, e le impostazioni di configurazione o di appartenenza ai gruppi. Nella figura seguente la scheda "*Generale*" di un gruppo globale consente, se necessario, la modifica del tipo di gruppo da protezione a distribuzione, mentre l'ambito del gruppo può essere modificato solo in universale.



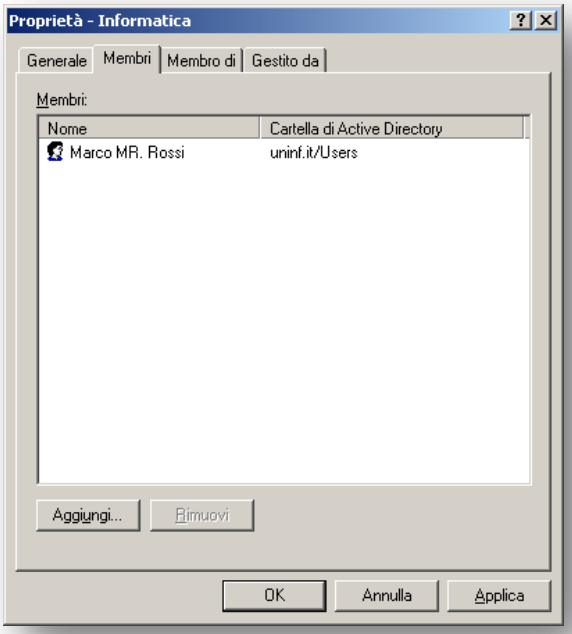
Dopo aver creato un nuovo gruppo, è possibile aggiungervi dei membri utilizzando una vasta gamma di metodi disponibili in "*Utenti e computer di Active Directory*". Riporto un elenco dei metodi utilizzati con maggiore frequenza:

- Fare clic con il pulsantre destro del mouse su un oggetto utente e selezionare "Aggiungi a un gruppo".

- Accedere alle proprietà di un utente, di un computer o di un gruppo, selezionare la scheda "*Membro di*" quindi fare clic su "*Aggiungi*".

- Accedere alle proprietà di un gruppo, selezionare la scheda "*Membri*" quindi fare clic su "*Aggiungi*".

Nella figura successiva viene riportato la scheda "*Membri*" relativa a un gruppo globale denominato "*Informatica*"



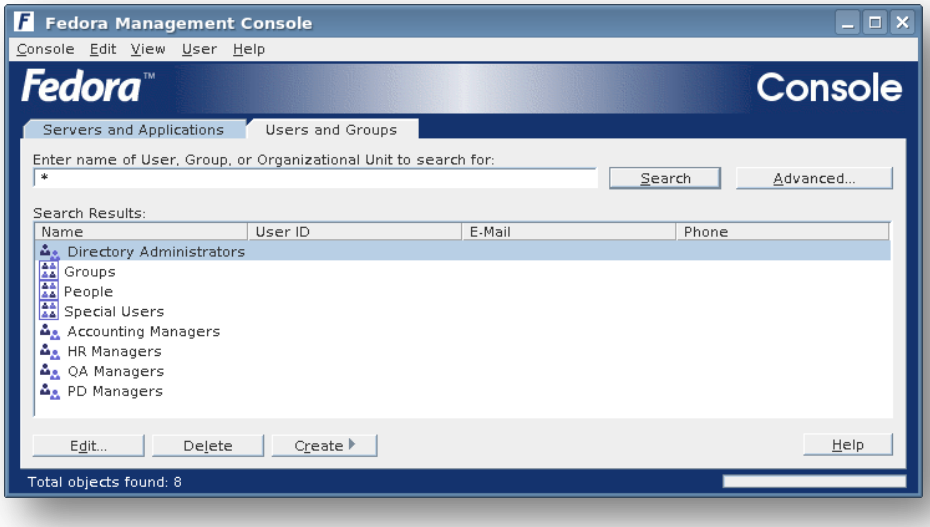
Come risulta evidente l'utente "*Marco Rossi*" è stato aggiunto al gruppo globale denominato "*Informatica*" [16] [17].

5.2 Gestione Utenti e Gruppi in Fedora Directory Server

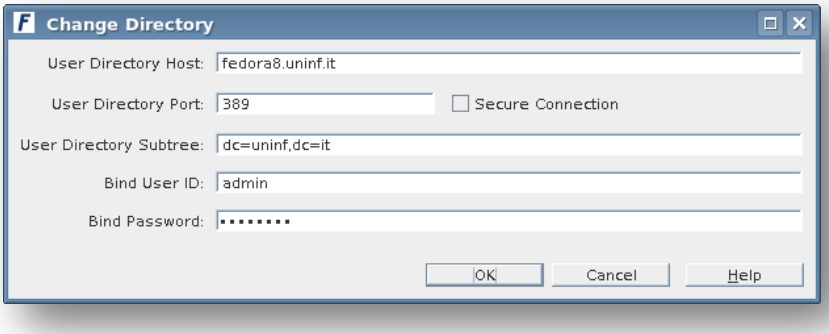
5.2.1 Creazione e modifica di account utente

Il metodo più semplice per poter aggiungere nuovi utenti e gruppi in Fedora Directory Server, è quello di avvalersi della console, in cui è presente una specifica schede per queste operazioni.

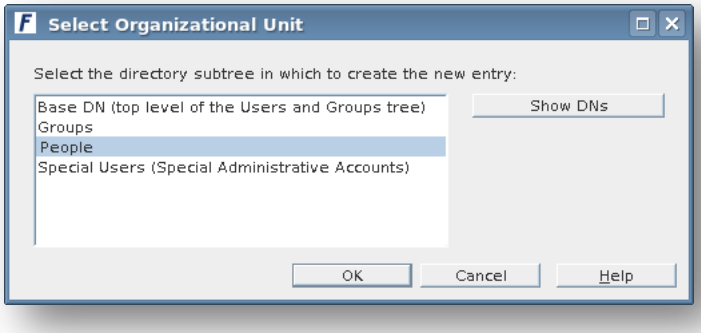
Quindi per prima cosa, si va a cliccare sulla scheda "*User and Group*", si apre la seguente schermata in cui è possibile effettuare operazioni di ricerca o di gestione delle entries, nella directory.



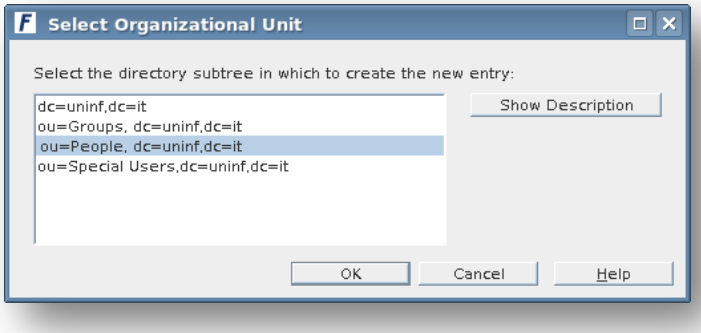
Innanzitutto, si va a cambiare il "*User Directory Subtree*" in quanto di default è impostato su "*o=NetscapeRoot*". Quindi si va a specificare il suffussi del sottoalbero in cui sono contenuti gli utenti e i gruppi che è "*dc=uninf, dc=it*". Per effettuare tale impostazione si clicca su "*User*"→"*Change Directory…*", viene mostrata la seguente schermata in cui si va a modificare il valore. Una volta cambiato si clicca su "*Ok*" per confermare la modifica.



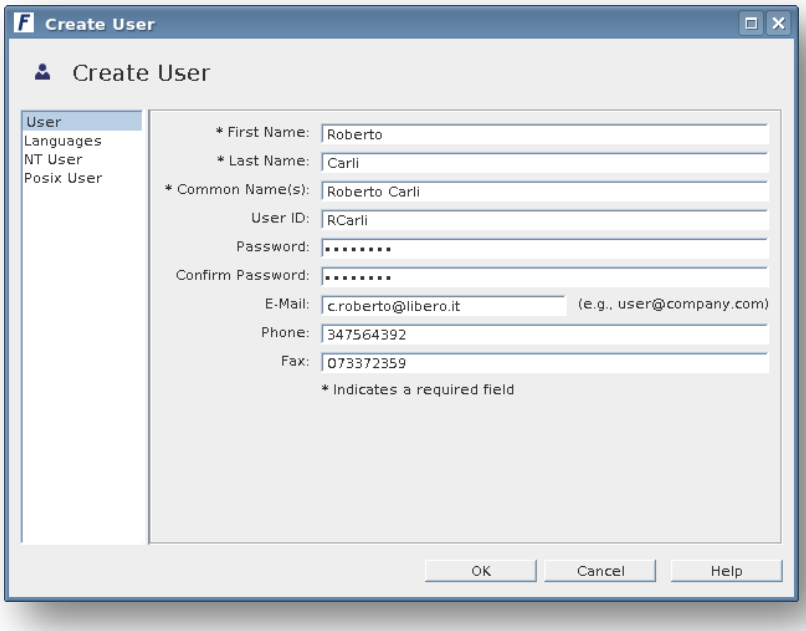
A questo punto si va a creare gli utenti cliccando su "*Create >*"→"*User…*" compare la seguente schermata in cui selezionare l'unità organizzativa.



E' possibile visualizzarer anche i relativi Distinguished Name cliccando su "*Show DNs*" come visibile nell'immagine seguente.



A questo punto, cliccando su "*Ok*", viene mostrata la seguente schermata in cui definire tutte le impostazioni relative al nuovo utente.

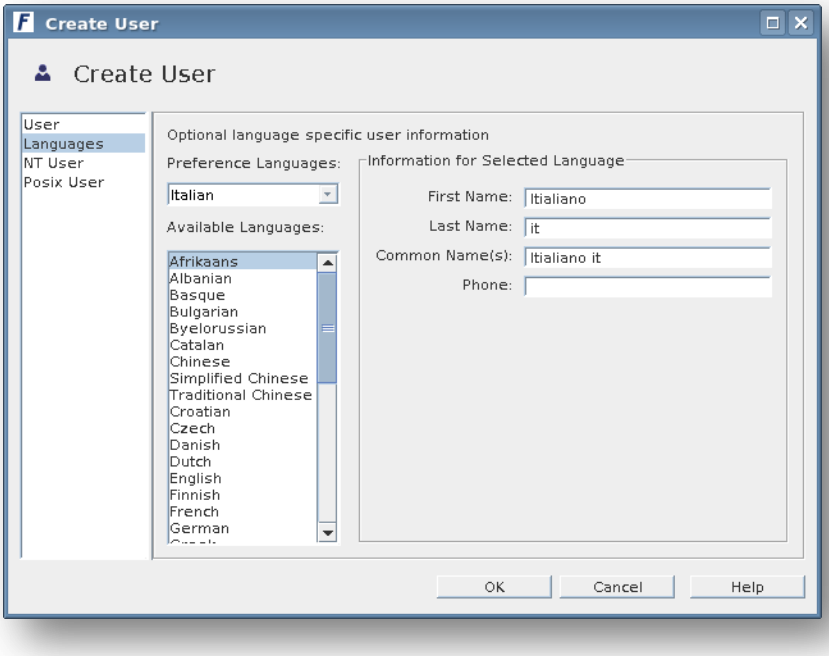


Descriviamo di seguito il significato di ogni campo della finestra.

- *First Name*: Il nome dell'utente;
- *Last Name*: Il cognome dell'utente;
- *Common Name(s)*: Questo è il nome completo. È generato automaticamente sulla base del Frist Name e Last Name inserito sopra. È possibile modificare questo nome, come necessario;
- *User ID*: Quando si immette un nome e cognome, l'ID utente viene generato automaticamente. E' possibile sostituire questo ID utente con uno a scelta. L'ID utente deve essere unico rispetto a tutti gli altri ID utente nella directory;
- *Password*: (Facoltativo) Password dell'utente. Caratteri alfanumerici, spazi e segni di interpunzione sono tutti accettabili.
- *Confirm Password*: Se si è inserito la password dell'utente, la si deve immettere nuovamente per confermare.
- *E-mail*: (Facoltativo) Indirizzo e-mail. Se l'utente ha più indirizzi e-mail, si separano con una virgola;
- *Phone*: (Opzionale) Inserire il numero di telefono dell'utente. Se l'utente ha più numeri di telefono, separata con una virgola;
- *Fax*: (Facoltativo) Numero di fax. Se l'utente ha più numeri di fax, inserirli separati con una virgola.

Se si vuole specificare la lingua e le relative informazioni, fare clic sulla scheda "*Languages*". Dal l'elenco a discesa "*Preference Languages*", selezionare la lingua preferita dell'utente, e quindi immettere le informazioni relative lingua:

- *First Name*: Inserisci il nome utente nella lingua selezionata;
- *Last Name*: Inserisci la cognome nella lingua selezionata;
- *Common Name*: Questo è il nome completo nella lingua selezionata. È generato automaticamente sulla base del Nome e Cognome inserito sopra. È possibile modificare questo nome, come necessario;
- *Phone*: Inserire il numero di telefono dell'utente. Se l'utente ha più numeri di telefono, inserirli separati da una virgola;
- *Pronunciation*: Se la lingua selezionata viene comunemente rappresentata foneticamente, sono visualizzati altri campi. Si inserisce la rappresentazione fonetica per il First Name, Last Name e Common Name.



5.2.2 Creazione e modifica dei gruppi

Un gruppo è costituito da utenti che condividono una comune attributo o fanno parte di una lista. Fedora Directory Server supporta tre tipi di gruppi: statici, dinamici, e gruppi certificati. Ogni gruppo è diverso nel modo in cui gli utenti, o i

membri (*Membres*), vengono aggiunti ad esso. Un gruppo statico consiste solo di utenti che sono stati aggiunti ad esso. Si chiama statico perché non cambia a meno che un utente non viene aggiunto o eliminato in esso.

Uno speciale *gruppo statico* è chiamato "*Configuration Administrators group*". Viene creato automaticamente e popolato quando la configurazione della directory viene installata. I membri del gruppo "*Configuration Administrators group*" hanno accesso illimitato alla directory di configurazione. Il gruppo è memorizzato nella directory di configurazione sotto il seguente DN:

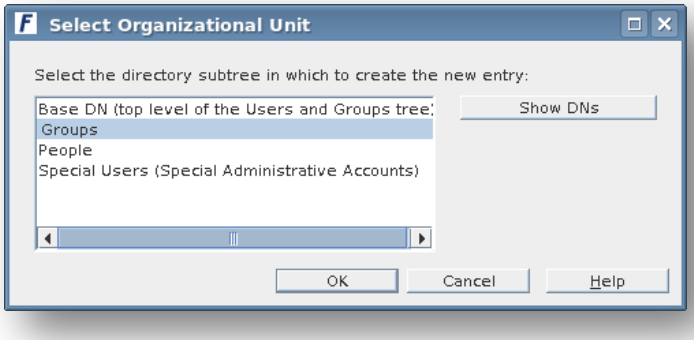
```
ou=Groups, ou=TopologyManagement, o=NetscapeRoot
```

Inizialmente, il "*Configuration Amministrator*" è l'unico membro della "*Configuration Administrators group*". Se si vuole dare ad altri utenti il privilegio dell'attività amministrativa si può farlo aggiungendoli come membri di tale gruppo. Questi utenti possono accedere alla Directory di configurazione allo stesso modo in cui accede l'amministratore di configurazione.

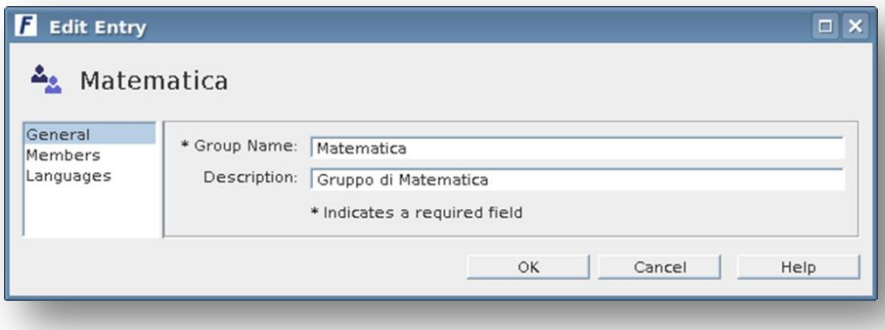
Una *gruppo dinamico* include automaticamente utenti sulla base di uno o più attributi nella loro entry. Questi attributi sono specificati come parte di un URL LDAP. Ogni volta che si cerca i membri del gruppo, i risultati contengono tutte le entries localizzate con l'URL.

Un *gruppo certificato* comprende tutti gli utenti che hanno un certificato contenente un attributo comune. Quando un singolo utente accede a un server, se tutti questi attributi sono trovati nel suo certificato, l'utente viene automaticamente riconosciuti come appartenenti al gruppo. Se l'utente certificato non contiene questi attributi, non è riconosciuto come un membro del gruppo, e non riceve lo stesso tipo di accesso, gli stessi privilegi e permessi come i membri del gruppo.

Per creare nuovi gruppi si cliccando su "*Create >*"→"*Group...*" compare la seguente schermata in cui selezionare l'unità organizzativa.



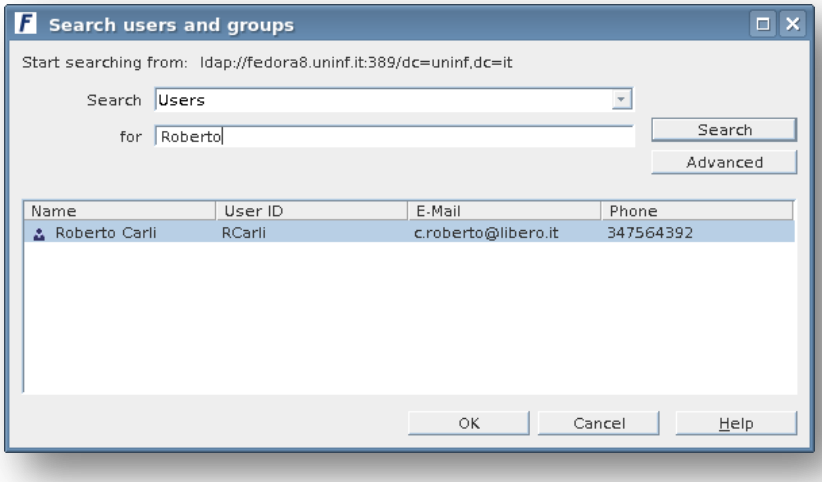
A questo punto, cliccando su "*Ok*", viene mostrata la seguente schermata in cui definire le impostazioni relative al nuovo gruppo.



Se si desidera creare solo il gruppo e aggiungere i membri del gruppo, si clicca su "*Ok*" e si salta il resto di questa procedura.

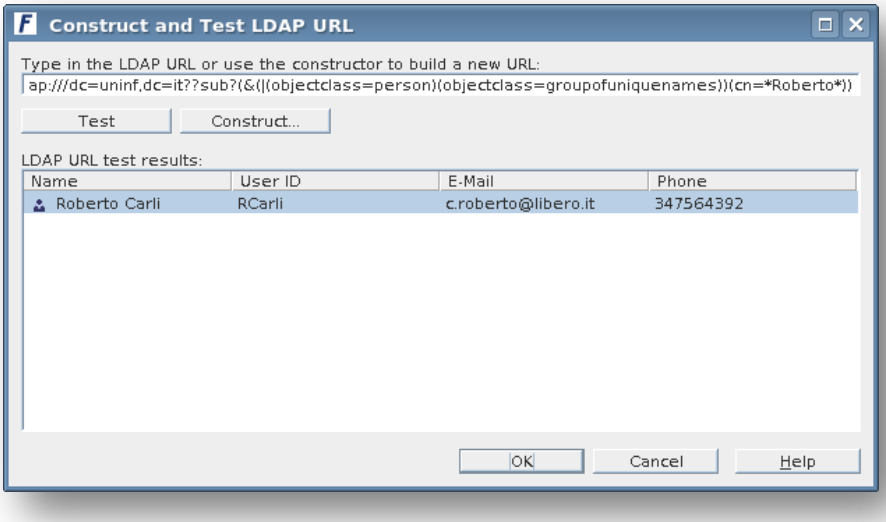
Se si desidera invece aggiungere immediatamente i membri del gruppo, si clicca su "*Membres*" e si passa alla fase successiva.

Nel pannello "*Membres*", si clicca sul tipo di gruppo "*Static Group*", poi su "*Add…*" e si utilizza la seguente finestra di dialogo di ricerca, per individuare un utente che si desidera aggiungere alla lista "*Members User ID*".



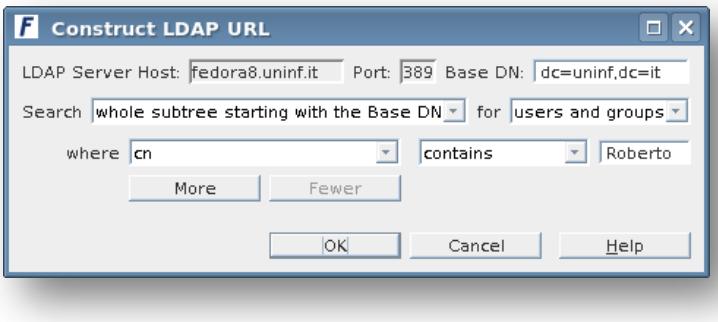
Una volta individuato si clicca su "*Ok*" per aggiungerlo. Si ripetere questo procedimento fino a quando tutti gli utenti che si desidera aggiungere al gruppo sono presenti nella lista.

Per aggiungere i membri, in un gruppo dinamico, nel pannello "*Membres*", si clicca sul tipo di gruppo "*Dynamic Group*", poi su "*Add…*" e si utilizza la seguente finestra di dialogo "*Construct and Test LDAP URL*", per specificare i criteri per includere gli utenti al gruppo dinamico.



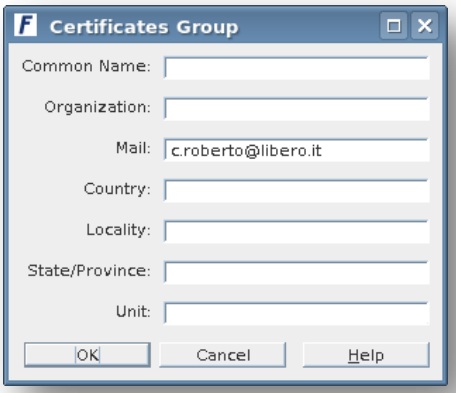
Nell'immagine precedente si vede il risultato visualizzato cliccando su "*Test*", relativo all'URL LDAP specificata. Per poter comporre in modo più

agevole l'URL LDAP è possiblie cliccare su "*Construct…*" viene aperta la seguente finestra di dialogo, in cui specificare tutti i paramentri.



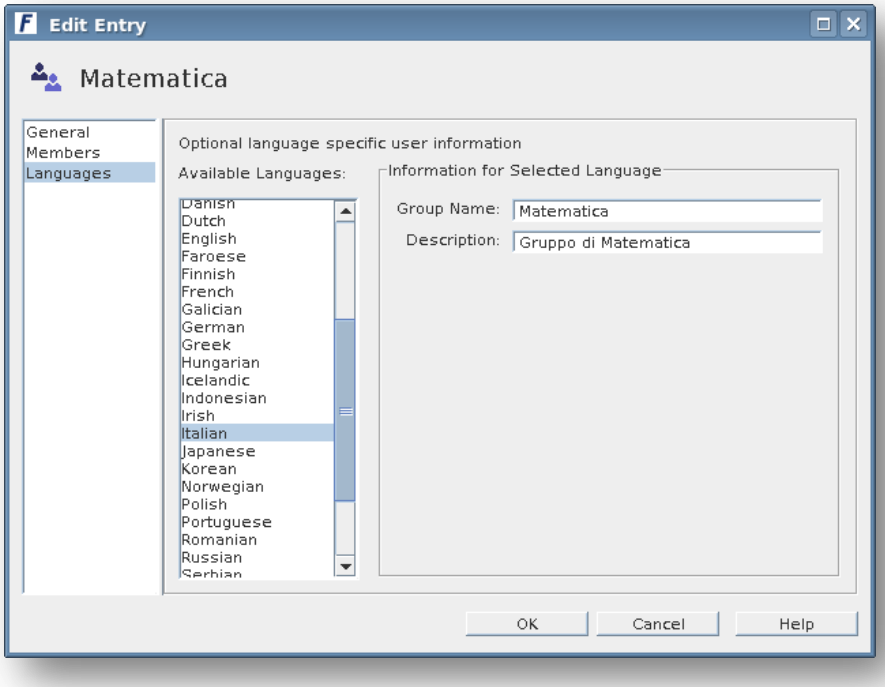
Come risulta evidente dall'immagine, sono stati specificati i paremtri per ricercare eventuali utenti, memorizzati nella directory, che si chiamano "*Roberto*". Tale ricerca fornisce il risultato visibile nella penultima immagine. A questo punto occorre cliccare su "*Ok*" per poter aggiungere il membro trovato, al gruppo dinamico.

L'ultima possibilità è quella di poter aggiungere membri a un gruppo certificato, su "*Members*" si clicca su "*Certificate Group*", poi su "*Add…*", viene mostrata la seguente finestra di dialogo.



Nella finestra di dialogo precedente è possibile specificare diversi valori di attributi, in base al quale è possibile selezionare i membri per il gruppo certificato.

L'ultima scheda disponibile, per la creazione del gruppo è "*Languages*" in cui è possibile specificare la lingua per il gruppo, il nome del gruppo e una descrizione [26].



5.3 Interrogazione delle Directories tramite clients LDAP

Il client utilizzato per effettuare interrogazioni LDAP, che supporta sia Active Directory e Fedora Directory Server, è Softerra LDAP Administrator. E' un client LDAP progettato per Windows. Softerra LDAP Administrator consente di visualizzare e analizzare le directory LDAP facilmente e in modo efficace.

LDAP Administrator presenta una comoda interfaccia intuitiva, un unico wizard per la creazione delle entries, pieno sostegno di tutti i più popolari server LDAPv3 e molte altre caratteristiche potenti. Nel processo di sviluppo Softerra LDAP Administrator è stato prestato particolare attenzione a rendere l'applicazione velocemente e funzionale con grandi quantità di dati, che è di fondamentale importanza quando si cerca di creare con una valida soluzione di e-business.

Esso è indispensabile se si è coinvolto nella creazione e nella manutenzione di sistemi complessi, composti da vari componenti basati su LDAP. Esista anche una versione più leggera e gratuita che è Softerra LDAP Browser con funzionalità

limitate per tutti i tipi di utilizzo. Diversamente da Softerra LDAP Administrator, il Browser non permette ai suoi utenti di modificare le directory LDAP.

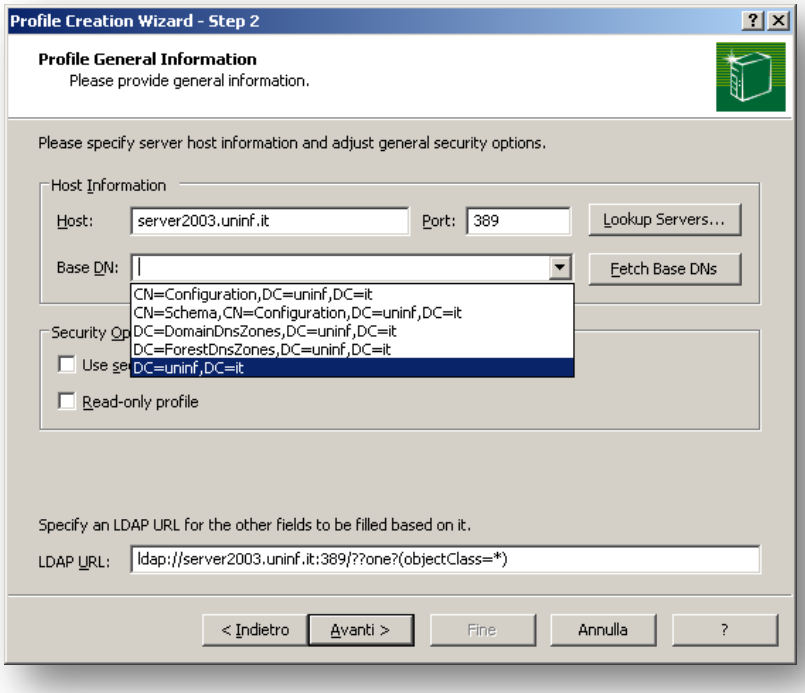
LDAP Administrator fornisce una vasta gamma di funzioni essenziali per chi è coinvolto nell'amministrazione o sviluppo con LDAP. A differenza della maggior parte dei software LDAP attualmente sul mercato, l'obiettivo principale di LDAP Administrator, è di fornire un sistema integrato, potente e facile da usare grazie alla comoda interfaccia, in grado di lavorare con qualsiasi server LDAP attualmente disponibili.

Per poter installare e provare il funzionamento di LDAP Administrator, si scarica il file dal sito del produttore: http://www.ldapadministrator.com/. Successivamente verranno riportati degli esempi di utilizzo di tale software.

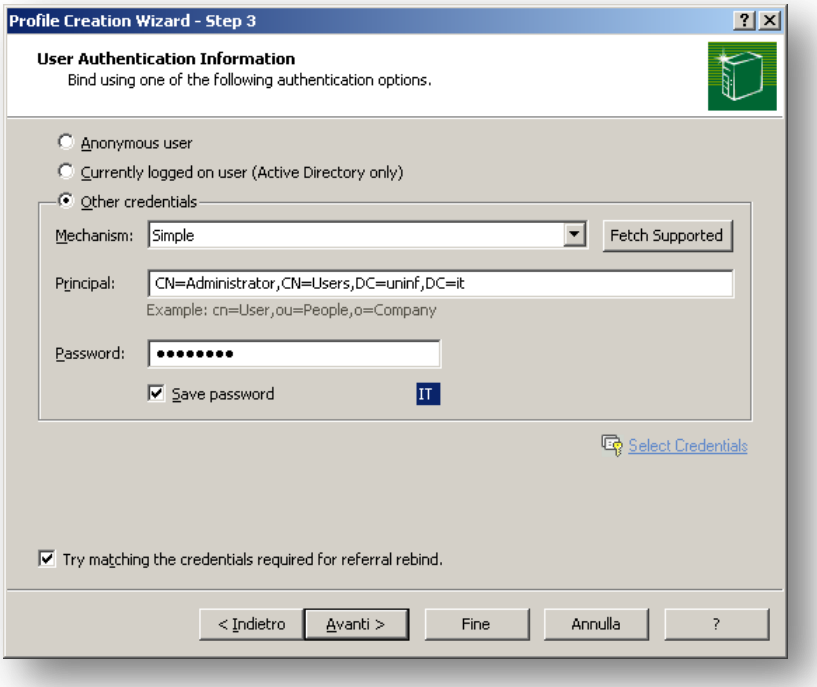
5.3.1 *Interrogazione di Active Directory tramite LDAP*

Per poter interrogare Active Directory si procede creando il profilo, nel seguente modo. Clicchiamo su "*New Profile*" ci compare la finestra di dialogo in cui impostare il nome del profilo, come visibile nella seguente immagine.

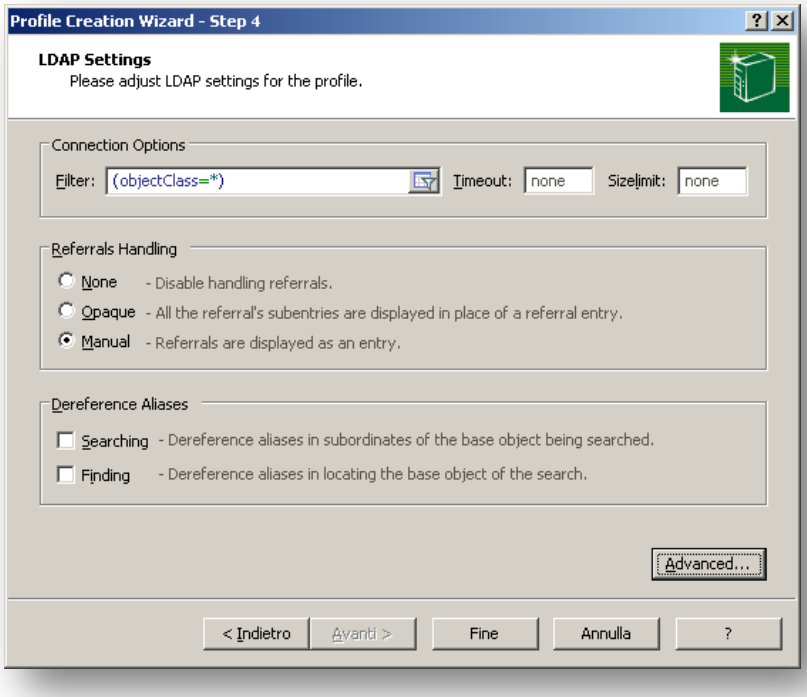
Una volta immesso il nome del profilo clicchiamo su "*Avanti* >" per visualizzare la successiva finestra di dialogo, in cui è possibile impostare i valori relativi al server LDAP da contattare.



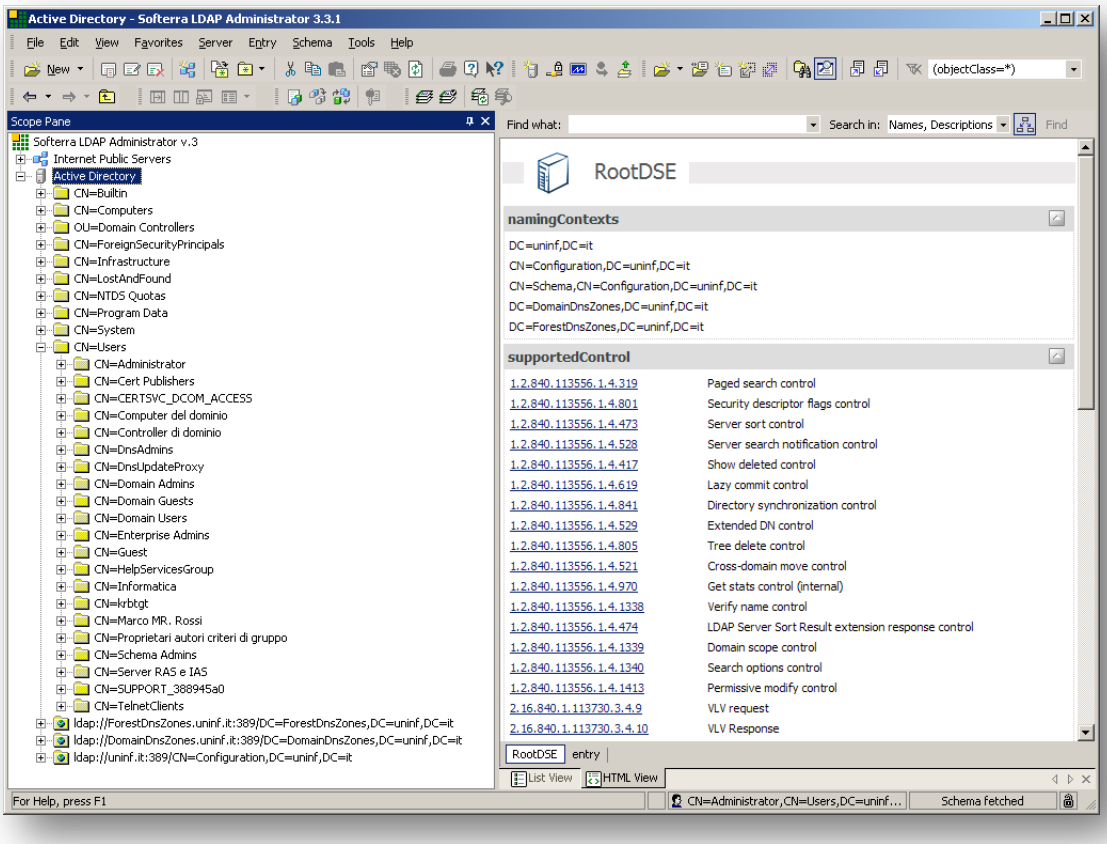
Qunidi occorre inserire il nome del server in cui è in escuzione Active Directory, nel nostro caso "*server2003.uninf.it*", per il corretto funzionamento occorre anche una corretta configurazione dei parametri del DNS. Andiamo quindi a specificare la porta in cui è in esecuzione il server LDAP ossia la "*389*" e in fine il parametro più importante, che il punto del sottoalbero in cui effettuare le interrogazioni, nel nostro caso occorre scegliare dal menù a tendina il DN "*DC=uninf,DC=it*", dopodichè clicchiamo su "*Avanti* >" e ci viene mostrata la seguente finestra in cui impostare i paramentri per l'autenticazione del client.



Qunidi specifichiamo, il meccanismo di autenticazione (*Mechanism*) che deve essere "*Simple*", il DN dell'amministratore (*Principal*) che deve essere "*CN=Administrator,CN=Users,DC=uninf,DC=it*" e la password (*Password*) relativa all'amministratore. A questo punto clicchiamo su "*Avanti >*", ci compare l'ultima finestra di dialogo in cui impostare gli ultimi parametri per il profilo.



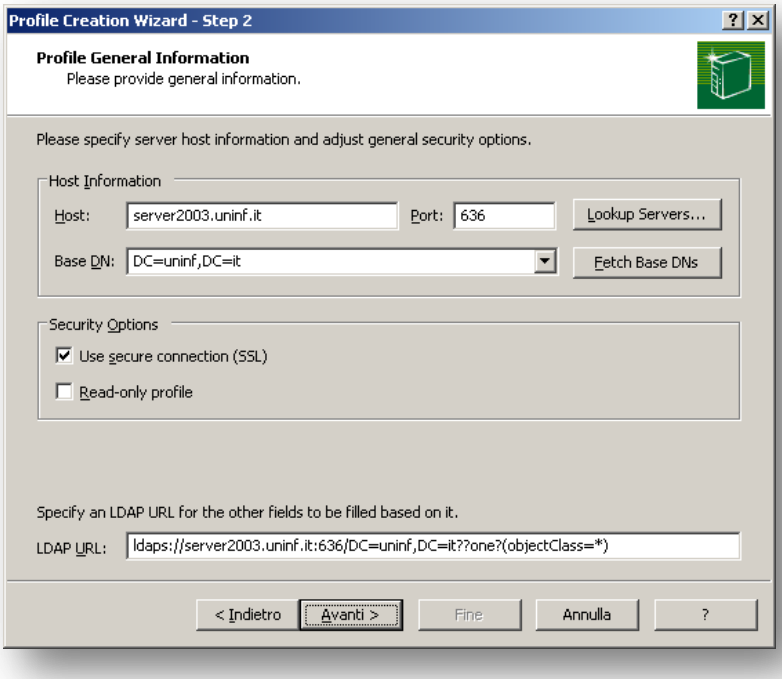
Arrivati a questo punto la procedura di creazione del profilo è completa, qunidi clicchiamo su "*Fine*" per terminare.



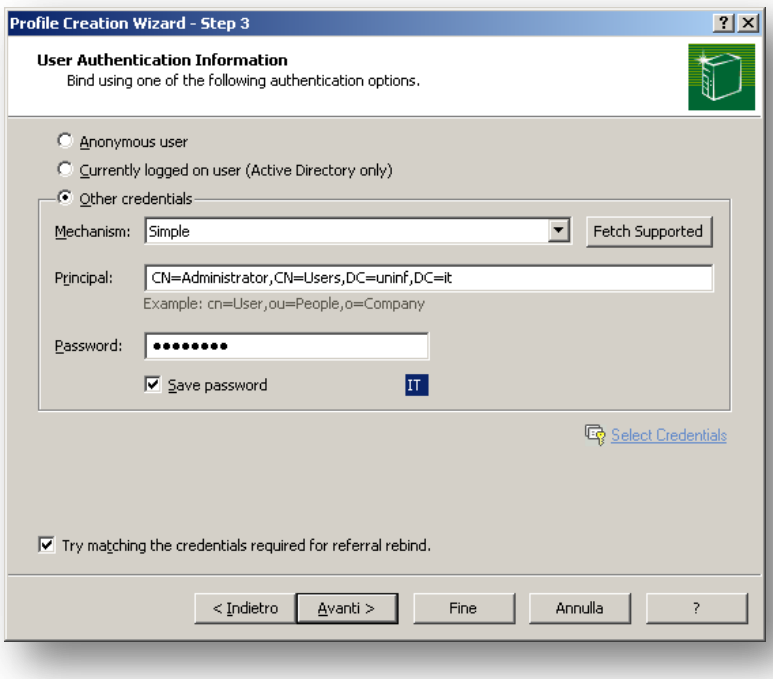
5.3.2 *Interrogazione di Active Directory tramite LDAPS*

Per poter interrogare Active Directory utilizzando la crittografia, si procede creando il profilo, nel seguente modo. Clicchiamo su "*New Profile*" ci compare la finestra di dialogo in cui impostare il nome del profilo.

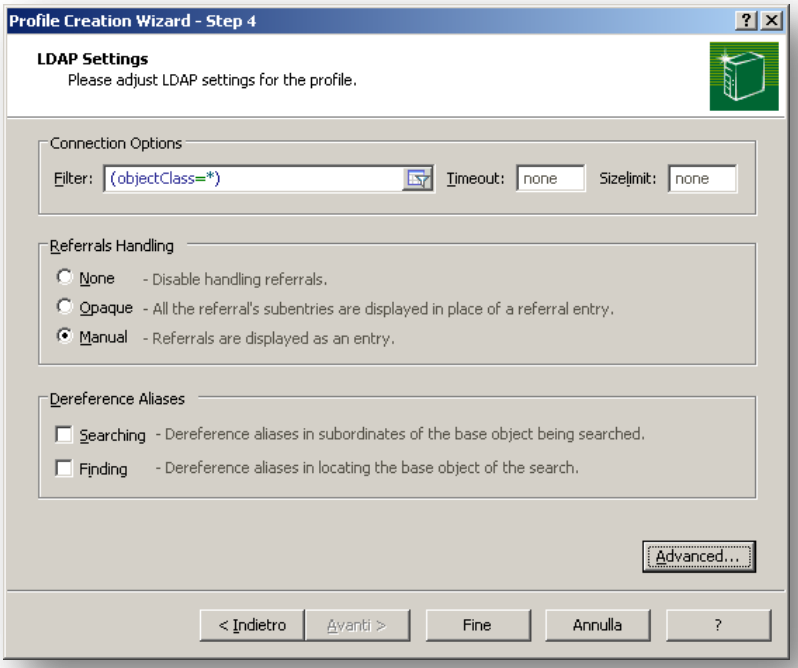
Una volta immesso il nome del profilo clicchiamo su "*Avanti* >" per visualizzare la successiva finestra di dialogo, in cui è possibile impostare i valori relativi al server LDAP da contattare.



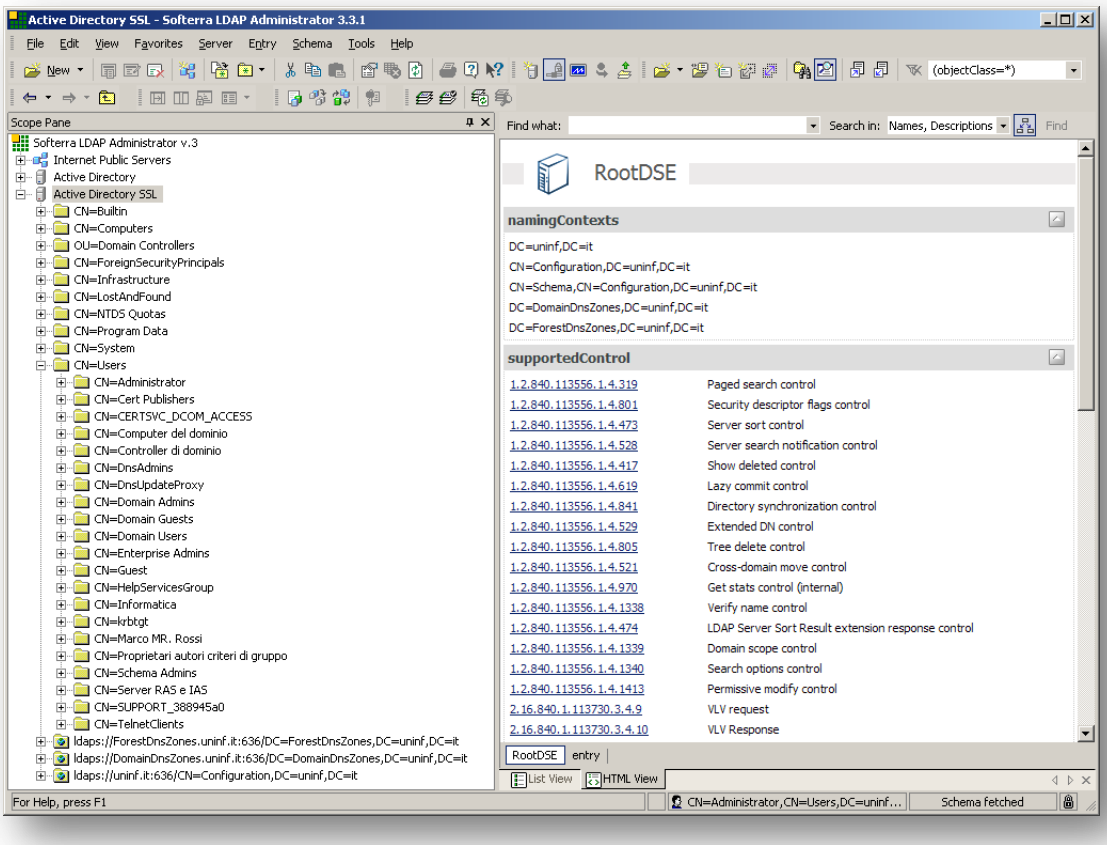
Qunidi occorre inserire il nome del server in cui è in escuzione Active Directory, nel nostro caso "*server2003.uninf.it*". Andiamo quindi a specificare la porta in cui è in esecuzione il server LDAPS ossia la "*636*" andanto a mettere un segno di spunta su "*Use secure connectio (SSL)*" e in fine,a ndiamo ad impostare, il parametro più importante, che è il punto del sottoalbero in cui effettuare le interrogazioni, nel nostro caso occorre scegliare dal menù a tendina il DN "*DC=uninf,DC=it*", dopodichè cliccando su "*Avanti >*" ci viene mostrata la seguente finestra in cui impostare i paramentri per l'autenticazione del client.



Qunidi specifichiamo, il meccanismo di autenticazione (*Mechanism*) che deve essere "*Simple*", il DN dell'amministratore (*Principal*) che deve essere "*CN=Administrator,CN=Users,DC=uninf,DC=it*" e la password (*Password*) relativa all'amministratore. A questo punto clicchiamo su "*Avanti >*", ci compare l'ultima finestra di dialogo in cui impostare gli ultimi parametri per il profilo.



Arrivati a questo punto la procedura di creazione del profilo è completa, qunidi clicchiamo su "*Fine*" per terminare.

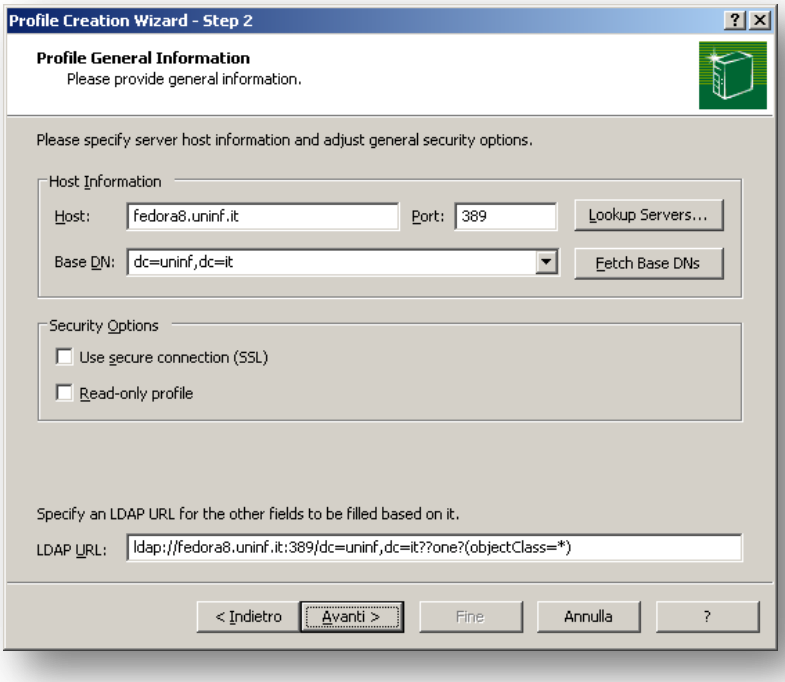


Vediamo nell'immagine precedente la stessa struttura dell'albero visibile anche nel profilo non provvisto di crittografia della directory, e anche il sottoalbero "*Users*" contenente tutti gli utenti registrati in Active Directoy.

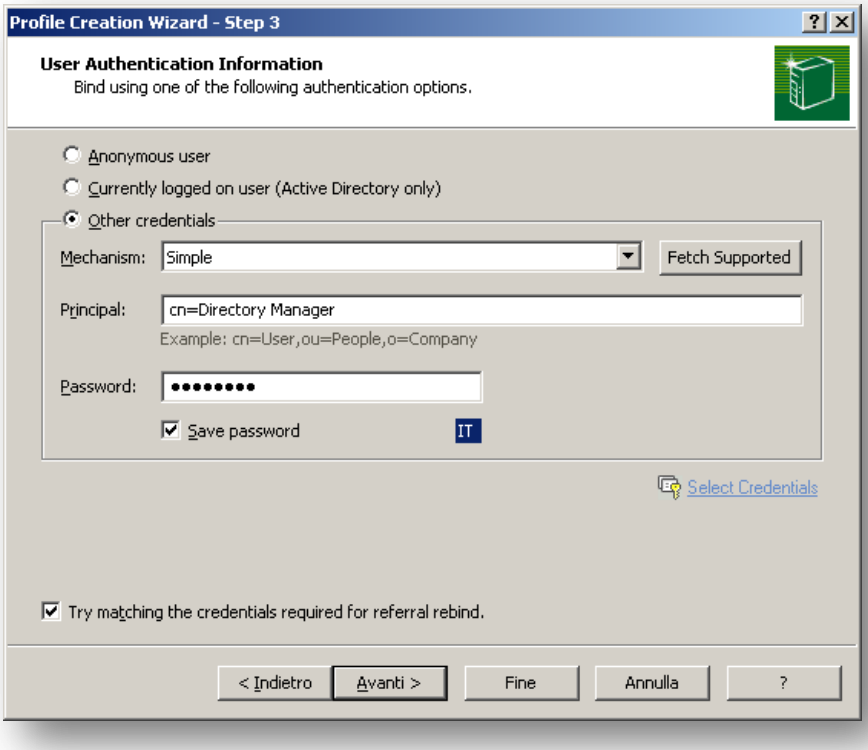
5.3.3 Interrogazione di Fedora Directory Server tramite LDAP

Vediamo ora come creare un profilo, adatto per poter interrogare e quindi verificare il funzionamento del Fedora Directory Server. Iniziamo con il cliccare su "*New Profile*" ci compare la finestra di dialogo in cui impostare il nome del profilo.

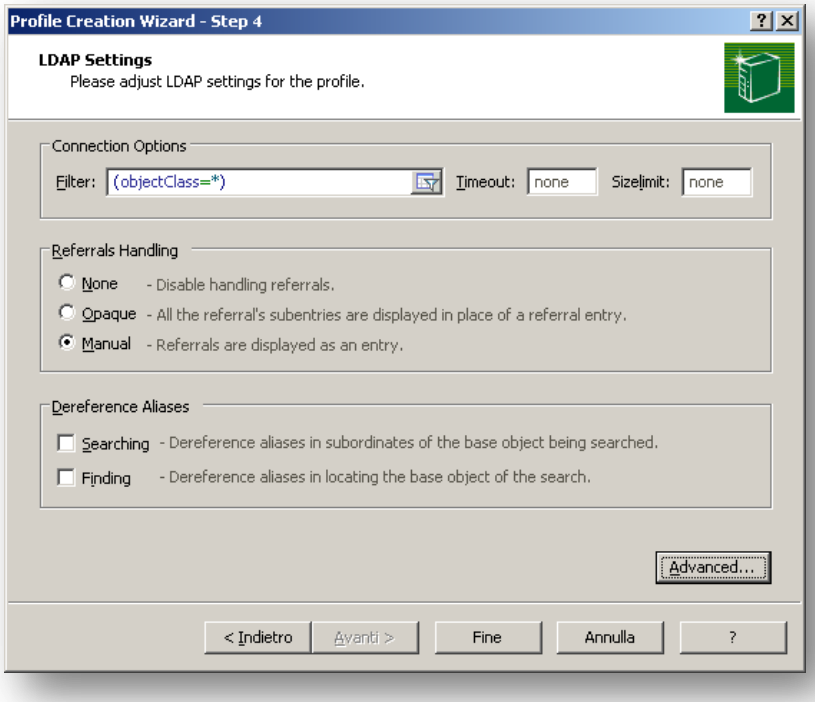
Una volta immesso il nome del profilo clicchiamo su "*Avanti* >" per visualizzare la successiva finestra di dialogo.



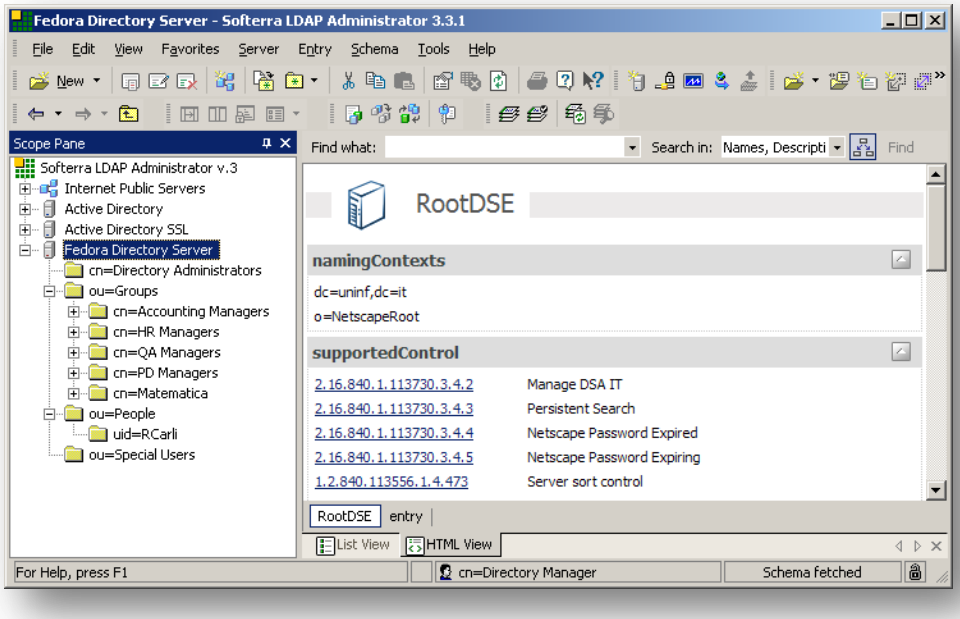
Qunidi occorre inserire il nome del server in cui è in escuzione Fedora Directory Server, nel nostro caso "*fedora8.uninf.it*", come risulta ovvio, per il corretto funzionamento occorre anche una corretta configurazione dei parametri del DNS. Andiamo quindi a specificare la porta in cui è in esecuzione il server LDAP ossia la "*389*" e in fine il parametro più importante, che è il punto del sottoalbero in cui effettuare le interrogazioni. Nel nostro caso occorre scegliare dal menù a tendina il DN "*dc=uninf,dc=it*", dopodichè clicchiamo su "*Avanti >*" e ci viene mostrata la seguente finestra in cui impostare i paramentri per l'autenticazione del client.



Qunidi specifichiamo, il meccanismo di autenticazione (*Mechanism*) che deve essere "*Simple*", il DN dell'amministratore (*Principal*) che deve essere "*cn=Directory Manager*" e la password (*Password*) relativa all'amministratore. A questo punto clicchiamo su "*Avanti* >", ci compare l'ultima finestra di dialogo in cui impostare gli ultimi parametri per il profilo.



Arrivati a questo punto la procedura di creazione del profilo è completa, qunidi clicchiamo su "*Fine*" per terminare.



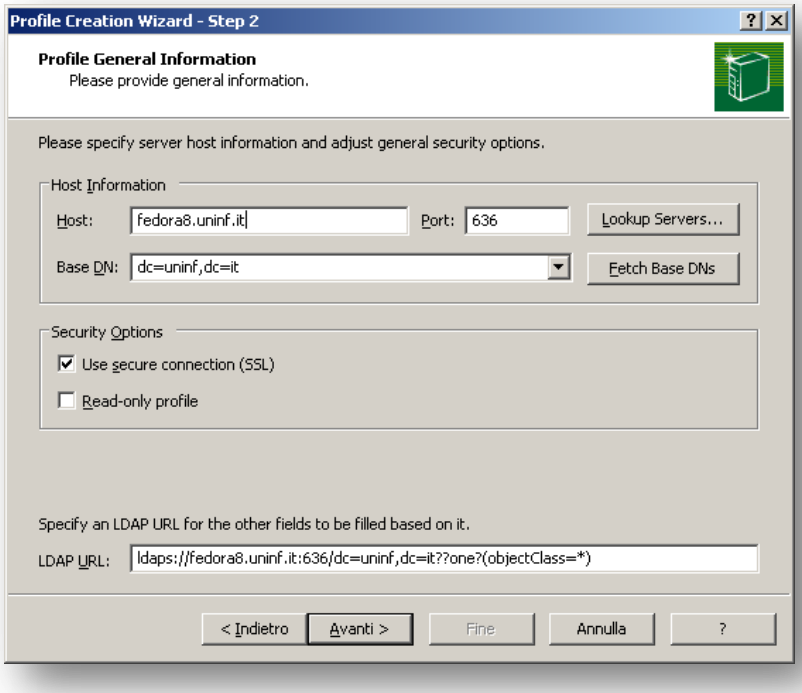
Come risulta evidente dall'immagine è presente l'albero della directory memorizzata nel Fedora Directory Server, contenente anche i sottoalberi "*Groups*"

e "*People*" conteneti rispettivamente i gruppi e gli utenti memorizzati nella directory.

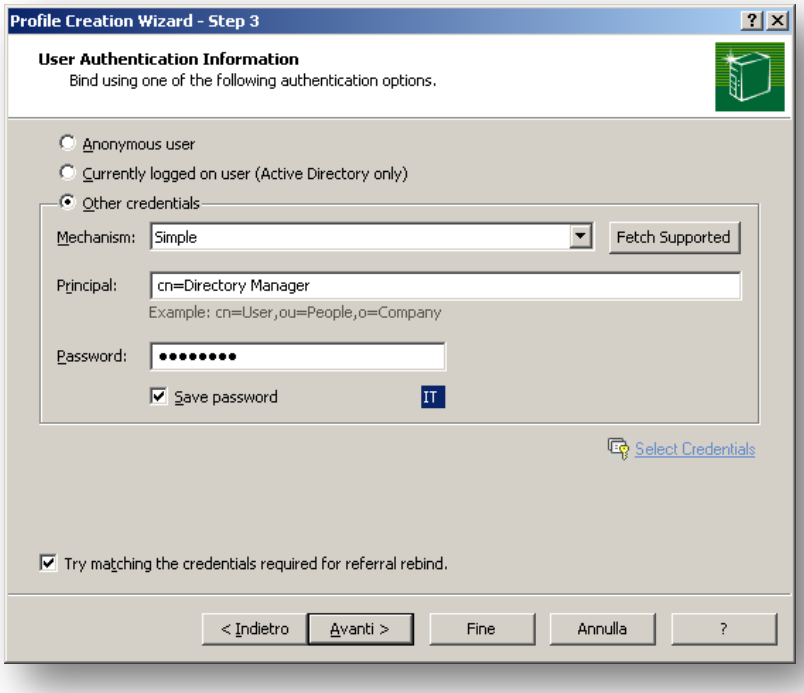
5.3.4 Interrogazione di Fedora Directory Server tramite LDAPS

Vediamo ora come creare un profilo, adatto per poter interrogare e quindi verificare il funzionamento del Fedora Directory Server utilizzando il protocollo LDAPS. Iniziamo con il cliccare su "*New Profile*" ci compare la finestra di dialogo in cui impostare il nome del profilo.

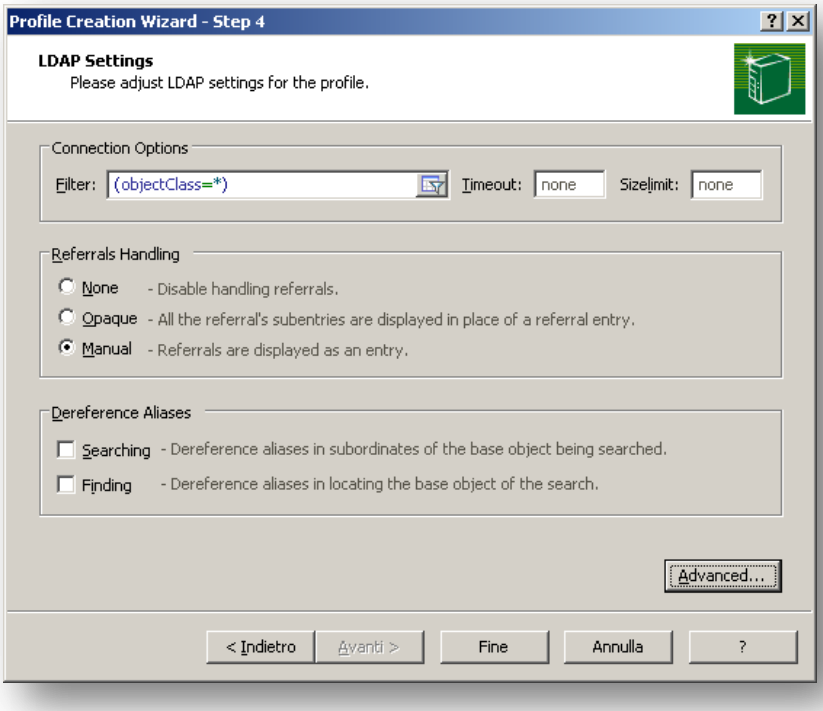
Una volta immesso il nome del profilo clicchiamo su "*Avanti* >" per visualizzare la successiva finestra di dialogo.



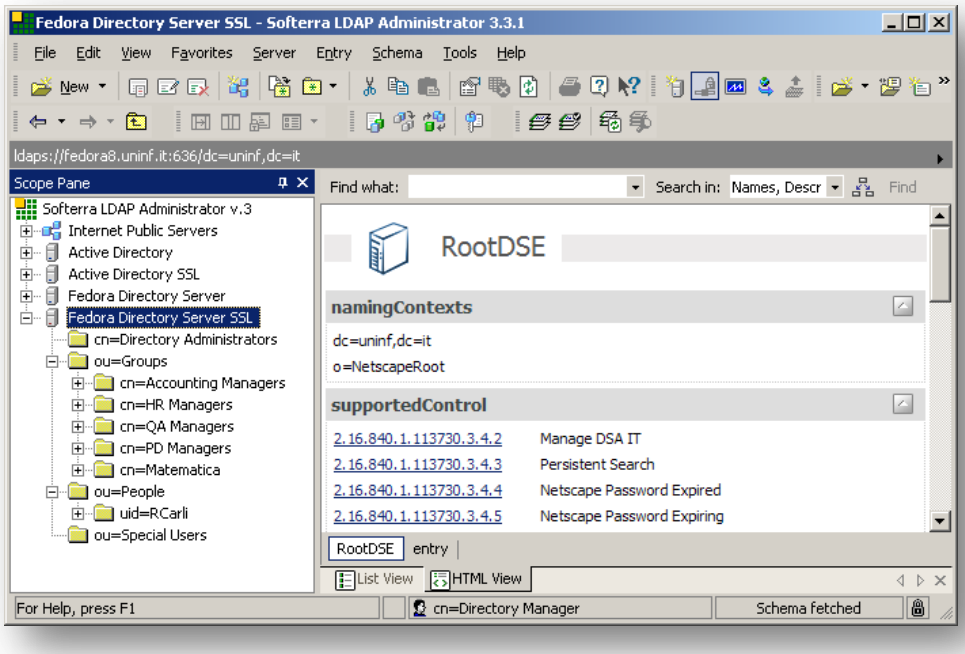
Qunidi occorre inserire il nome del server in cui è in escuzione Fedora Directory Server, nel nostro caso "*fedora8.uninf.it*", come risulta ovvio, per il corretto funzionamento occorre anche una corretta configurazione dei parametri del DNS. Andiamo quindi a specificare la porta in cui è in esecuzione il server LDAPS ossia la "*636*" spuntando la casella "*Use secure connection (SSL)*". In fine impostiamo il parametro più importante, che è il punto del sottoalbero in cui effettuare le interrogazioni. Nel nostro caso scegliamo dal menù a tendina il DN "*dc=uninf,dc=it*", dopodichè clicchiamo su "*Avanti* >" e ci viene mostrata la seguente finestra in cui impostare i paramentri per l'autenticazione del client.



Qunidi specifichiamo, il meccanismo di autenticazione (*Mechanism*) che deve essere "*Simple*", il DN dell'amministratore (*Principal*) che deve essere "*cn=Directory Manager*" e la password (*Password*) relativa all'amministratore. A questo punto clicchiamo su "*Avanti* >", ci compare l'ultima finestra di dialogo in cui impostare gli ultimi parametri per il profilo.



Arrivati a questo punto la procedura di creazione del profilo è completa, qunidi clicchiamo su "*Fine*" per terminare.

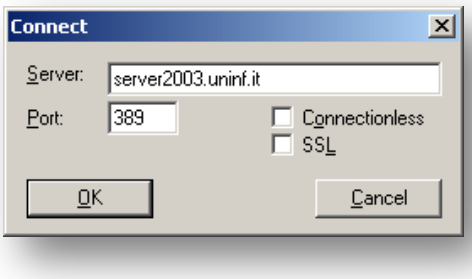


Come risulta evidente dall'immagine è presente l'albero della directory memorizzata nel Fedora Directory Server, contenente anche i sottoalberi "*Groups*"

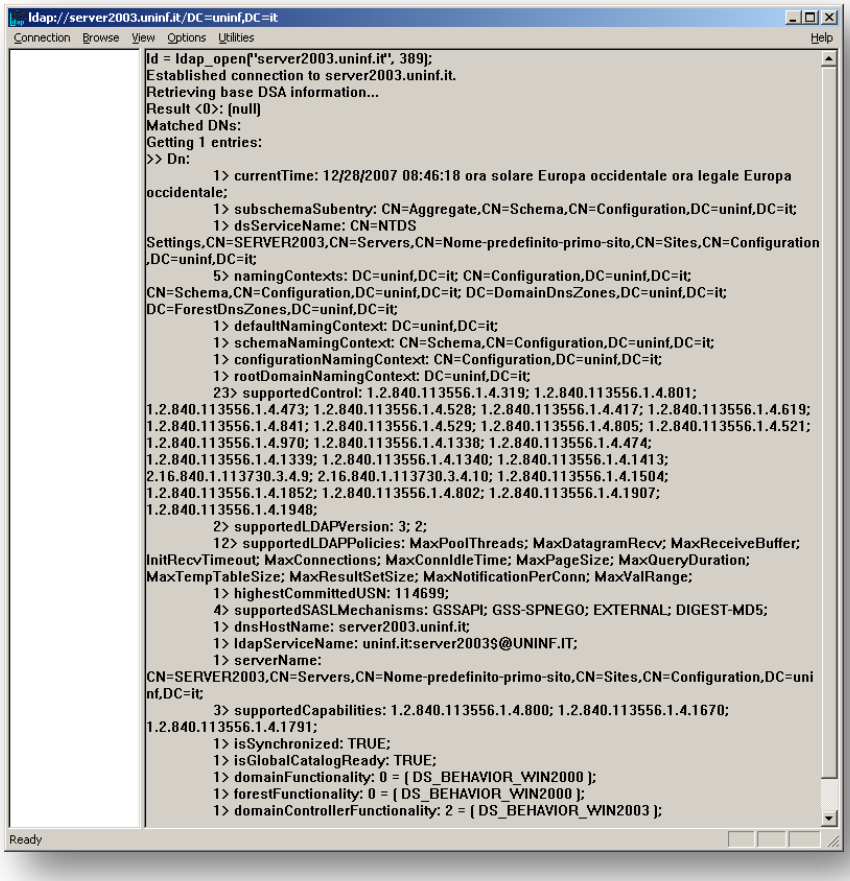
e "*People*" conteneti rispettivamente i gruppi e gli utenti memorizzati nella directory [28].

5.3.5 *Interrogazione di Active Directory mediante LDP*

Le ricerche all'interno di Active Directory, possono essere eseguite anche con LDP, incluso nelle utilità di supporto di Microsoft Windows Server 2003. È necessario innanzitutto aprire LDP e connettersi a un controller di dominio valido, nel nostro caso "*server2003.uninf.it*". Clicchiamo su "*Connection*" e ci viene mostrata la seguente schermata.

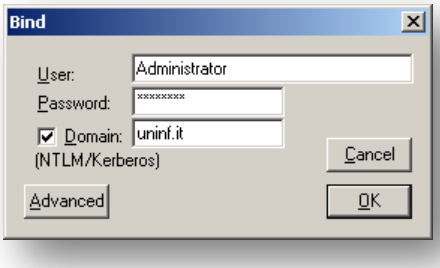


Quindi andiamo ad inserire il server "*server2003.uninf.it*" e la porta di connessione standard per le interrogazioni LDAP "*389*".



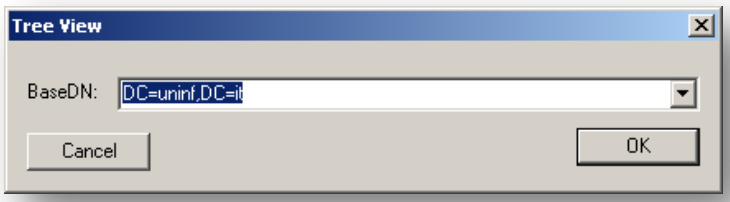
La schermata precedente ci viene mostrata, se Active Directory è configurato correttamente e se abbiamo inserito i giusti vaolori nella finestra di dialogo "*Connect*" e abbiamo cliccato su "*Ok*" per confermare le impostazioni.

A questo punto per poter effettuare delle interrogazioni e delle modifiche relative alle entries, all'interno della directory, occorre autenticarsi con l'utente amministratore. Per effettuare questo clicchiamo su "*Connection*"→ "*Bind…*" e ci viene mostrata la seguente finestra di dialogo.

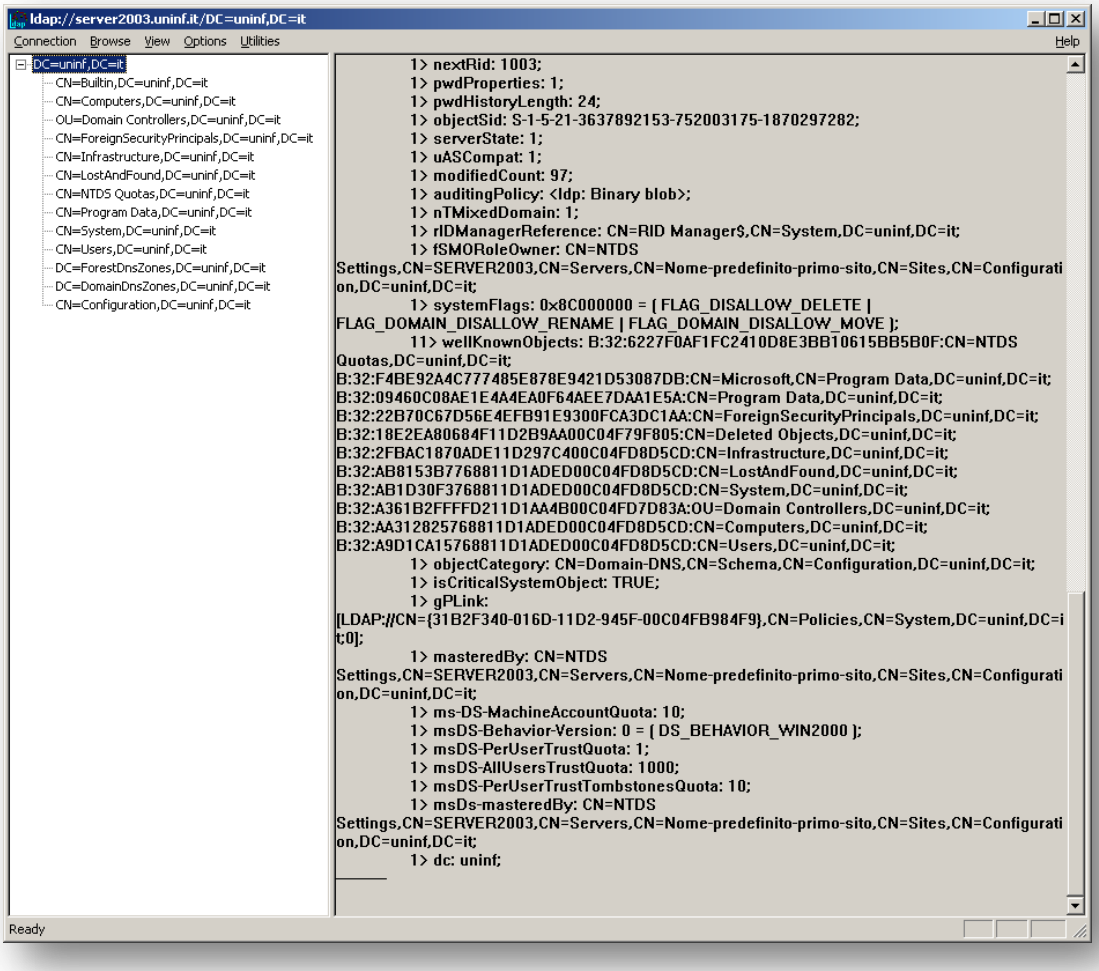


Nella finestra di dialogo precedente si va inserire il valore "*User*" che è "*Administrator*" la password relativa "*Password*" e il dominio di appartenenza di Active Directory, "*Domain*" che è "*uninf.it*". A questo punto si clicca su "*Ok*" per confermare, e si procede con le ricerche all'interno della directory.

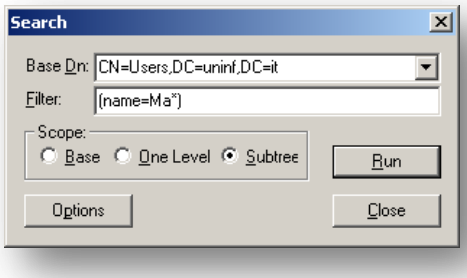
Successivamente per rendere visibile la struttura dell'albero della directory, cliccando su "*View*"→"*Tree*", ci viene mostrata la seguente finestra in cui impostare il DN di base.



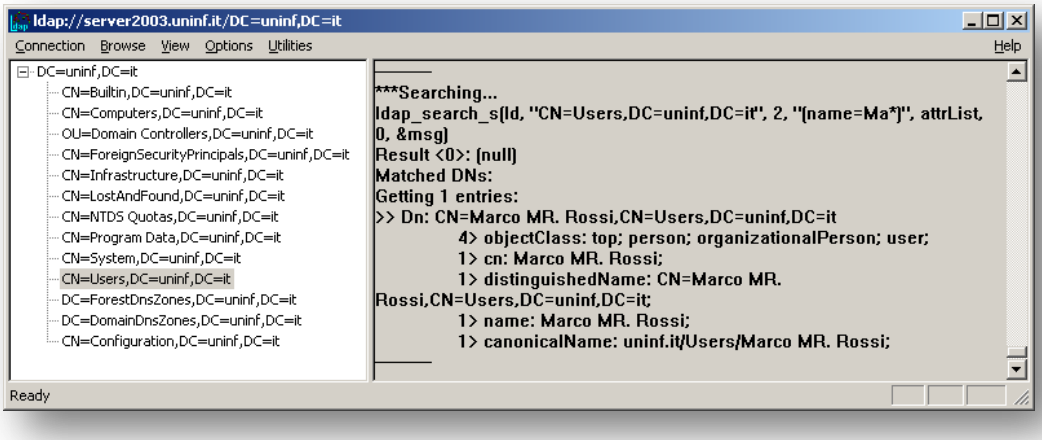
Quindi cliccando su "*Ok*" ci viene mostrato anche la struttura dell'albero, come segue.



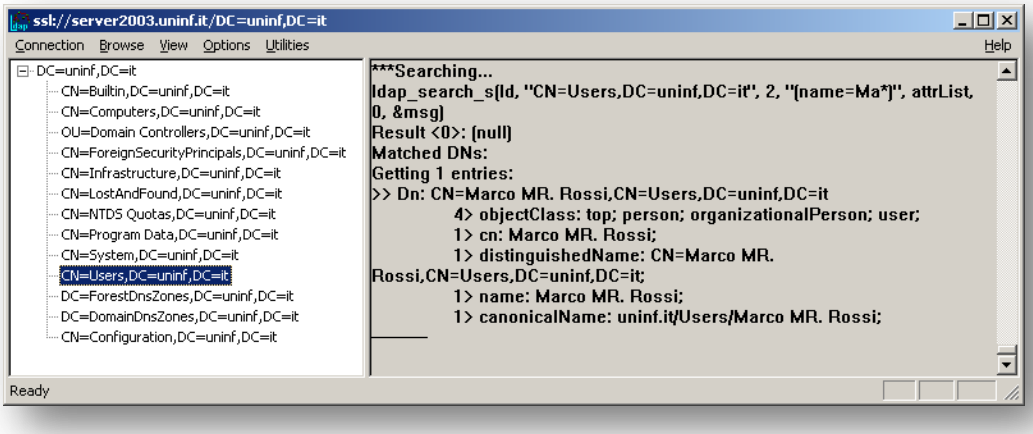
Arrivati a questo punto per poter ricercare delle entry all'interno della directory, possiamo cliccare su "*Browse*"→"*Search*" per ricercare all'interno di tutta la directory oppure in alternativa cliccare con il tasto destro, ad esempio, su "*CN=Users,DC=uninf,DC=it*". Ci vene mostrata la seguente finestra, in cui inserire i paramentri di ricerca.



Nella finestra sovrastante, vengono specificati i parametri DN di base per la ricerca, lo scope e il filter. Come risulta evidente al campo filter è stato aseegnato il valore "*name=Ma**" che ci permette di ricercare tutti gli utenti all'interno del sottoalbero "*CN=Users,DC=uninf,DC=it*", che hanno il nome che inizia per *Ma*. Di seguito viene riportata l'immagine relativa alla risposta fornita da tali criteri diricerca, confermati cliccando su "*Ok*".



Tale tool ci permette comunque, non solo di ricercare entries all'interno della directory, ma anche di crearne di nuove, di modificarle, e molto altro ancora. E' possibile anche utilizzarlo per verificare il corretto funzionamento di Active Directory configurato per l'utilizzo della crittografia e quindi utilizzarlo per interrogare la directory tramite la porta crittografata "*636*". Vediamo un esempio della stessa interrogazione predente, utilizzando il protocollo LDAPS [29] [30].

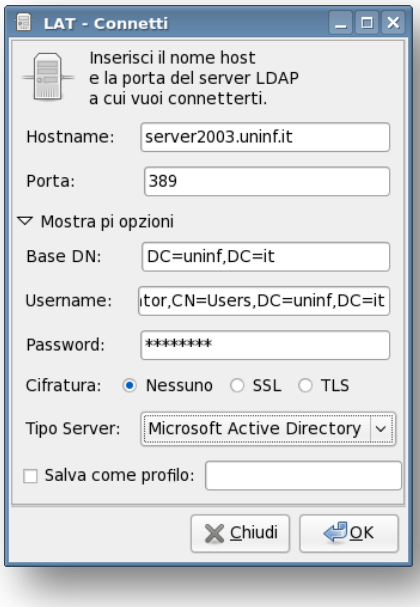


5.3.6 *Interrogazione di Active Directory mediante LAT*

Vediamo ora un client LDAP in ambiente Linux, che ha la possibilità di poter interrogare Active Directory che è LDAP Administrator Tool. L'installazione del pacchetto software, è possibile utilizzando la comoda interfaccia "*Amministrazione pacchetti*" messa a disposizione da Fedora 8.

Tale software, consente di sfogliare le directory basate su LDAP e aggiungere, modificare o eliminare le voci contenute all'interno. È possibile anche memorizzare i profili per un rapido accesso a diversi server. Dispone anche punti di vista differenti, quali utenti, gruppi e Host, che permette di gestire facilmente gli oggetti.

All'avvio del software, ci viene mostrata la seguente finestra in cui impostare i parametri di connessione ad un server LDAP.

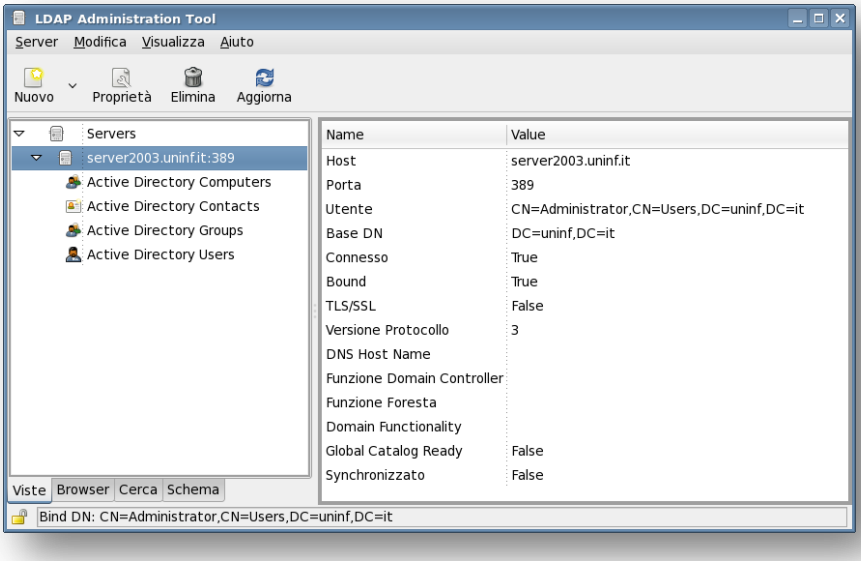


Nella finestra sovrastante, vengono specificati tutti parametri per poter connettersi correttamente ad active directory utilizzando il protocollo LDAP. Le impostazioni corrette sono:

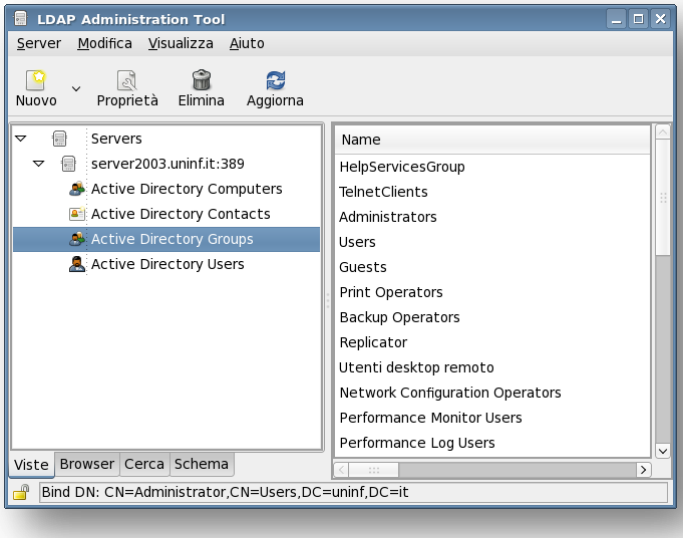
- Hostname: *server2003.uninf.it*;
- Porta: *389*;

- Base DN: *DC=uninf,DC=it*;
- Username: *CN=Administrator,CN=User,DC=uninf,DC=it*;
- Password: la password dell'utente amministratore;
- Cifratura: *Nessuna*;
- Tipo Server: *Microsoft Active Directory*.

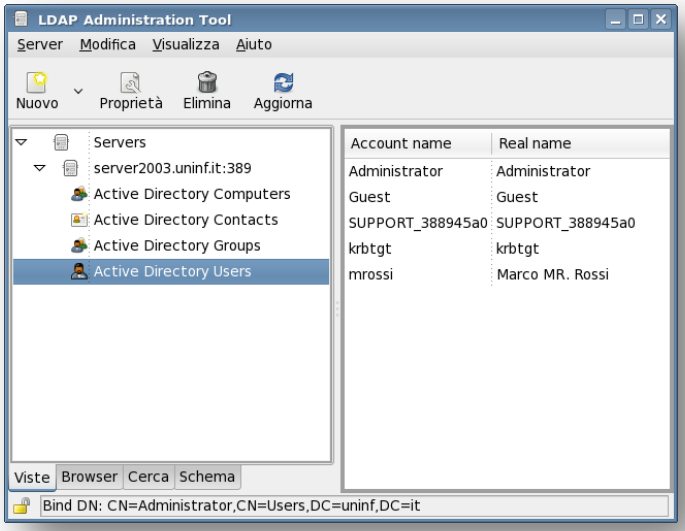
confermiamo tali parametri cliccando su "*Ok*". A questo punto ci viene mostrata la seguente schermata.



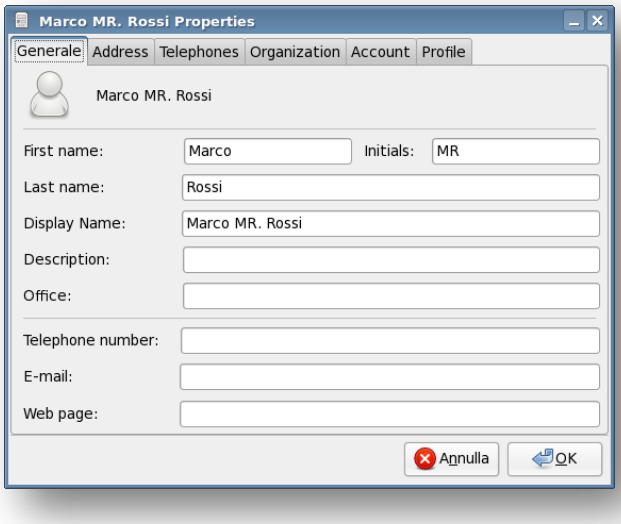
Nell'immagine precedente ci viene riportato il riassunto delle impostazioni di configurazione. Nell'immagine successiva vediamo i gruppi memorizzati in AD.



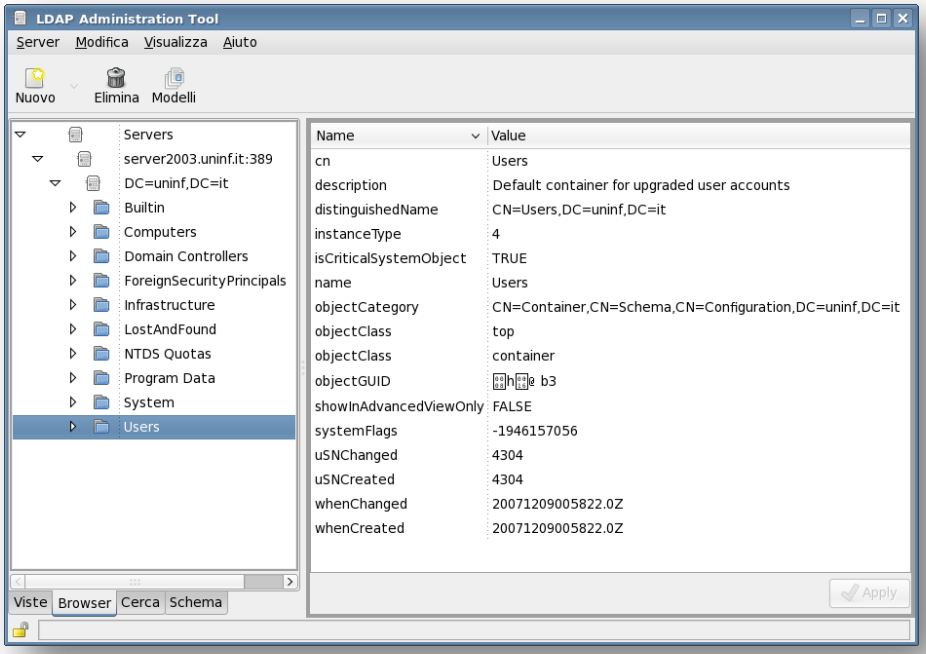
Mentre in quella successiva vediamo gli utenti memorizzati in Active Directory.



Tramite questo tool è possibile anche modificare le entry, vediamo di seguito le informazioni relative all'utente "*Marco Rossi*" che è possibile modificare.



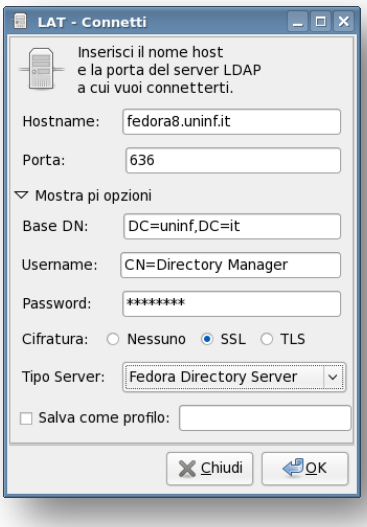
E' possible anche navigare nell'albero della directory memorizzato in Active Directory. Per poterlo sfogliare, clicchiamo su "*Browser*". Nella seguente immagine vediamo un esempio.



Tale software permette di effettuare anche altre funzioni, come il cercare informazioni all'interno della directory e gestire lo schema.

5.3.7 *Interrogazione di Fedora Directory Server mediante LAT*

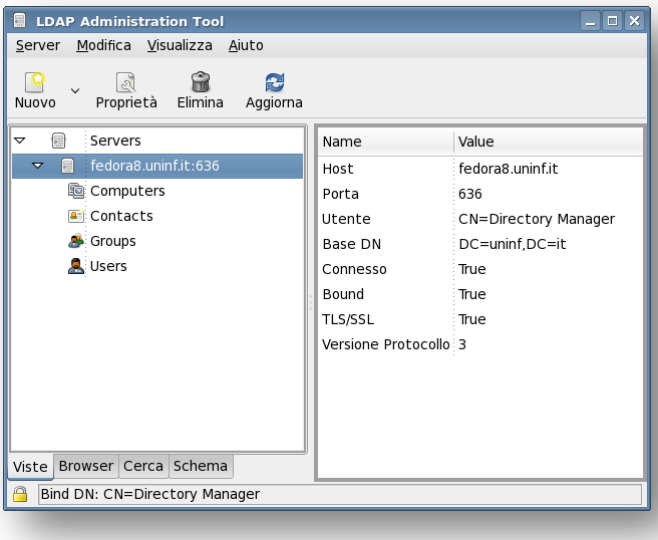
Vediamo ora come utilizzare tale software per interrogare Fedora Directory Server, utilizzando la porta "636" quindi la crittografia. Vediamo di seguito i parametri da impostare.



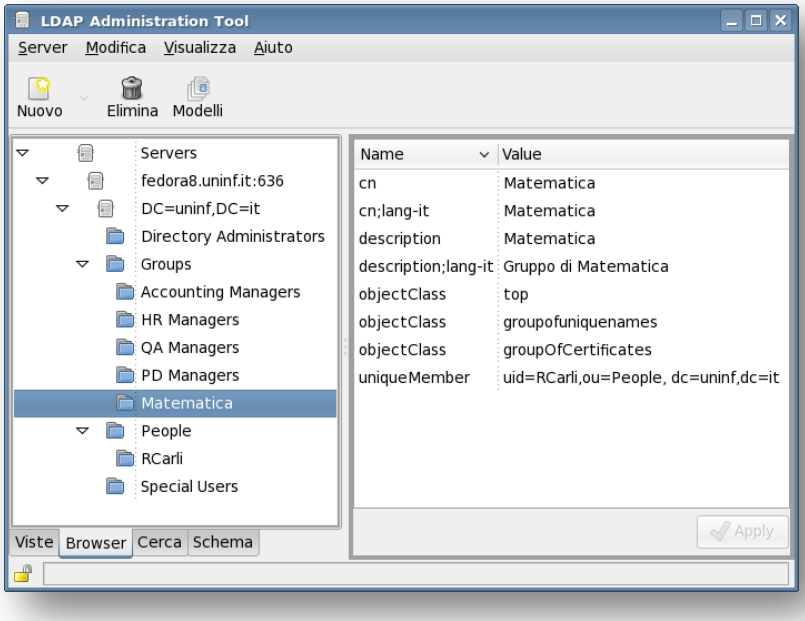
Nella finestra sovrastante, vengono specificati tutti parametri per poter connettersi correttamente a Fedora Directory Server utilizzando il protocollo LDAPS. Le impostazioni corrette sono:

- Hostname: *fedora8.uninf.it*;
- Porta: *636*;
- Base DN: *DC=uninf,DC=it*;
- Username: *CN=Directory Manager*;
- Password: la password dell'utente amministratore;
- Cifratura: *SSL*;
- Tipo Server: *Fedora Directory Server*.

confermiamo tali parametri cliccando su "*Ok*". A questo punto ci viene mostrata la seguente schermata.



E' possible anche navigare nell'albero della directory memorizzato in Fedora Directory Server. Per poterlo sfogliare, clicchiamo su "*Browser*". Nella immagine successiva vediamo un esempio. E' possibile anche vedere tutti gli attributi realtivi al gruppo "*Matematica*" creato in precedenza, con il relativo membro, che è l'utente "*Roberto Carli*" [31].


LDAP Administration Tool
Server Modifica Visualizza Aiuto
Nuovo
Elimina
Modelli
Servers
fedora8.uninf.it:636
DC=uninf,DC=it
Directory Administrators
Groups
Accounting Managers
HR Managers
QA Managers
PD Managers
Matematica
People
RCarli
Special Users
Viste
Browser
Cerca
Schema
Name
Value
cn
Matematica
cn;lang-it
Matematica
description
Matematica
description;lang-it
Gruppo di Matematica
objectClass
top
objectClass
groupofuniquenames
objectClass
groupOfCertificates
uniqueMember
uid=RCarli,ou=People, dc=uninf,dc=it
Apply

CAPITOLO 6

SINCRONIZZAZIONE TRA ACTIVE DIRECTORY E FEDORA DIRECTORY SERVER

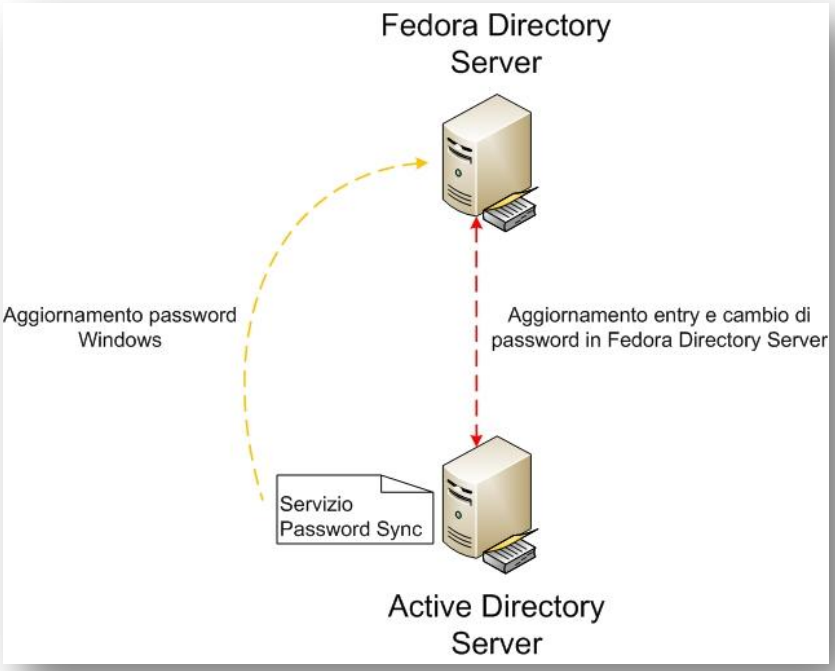
6.1 Metodologia di Sincrozizzazione

La funzionalità di sincronizzazione permette di aggiungere, cancellare e modificare i gruppi, entries degli utenti e la loro password tra Fedora Directory Server e Microsoft Active Directory. Fornisce un efficiente ed efficace modo per mantenere coerente le informazioni all'interno di diverse directory.

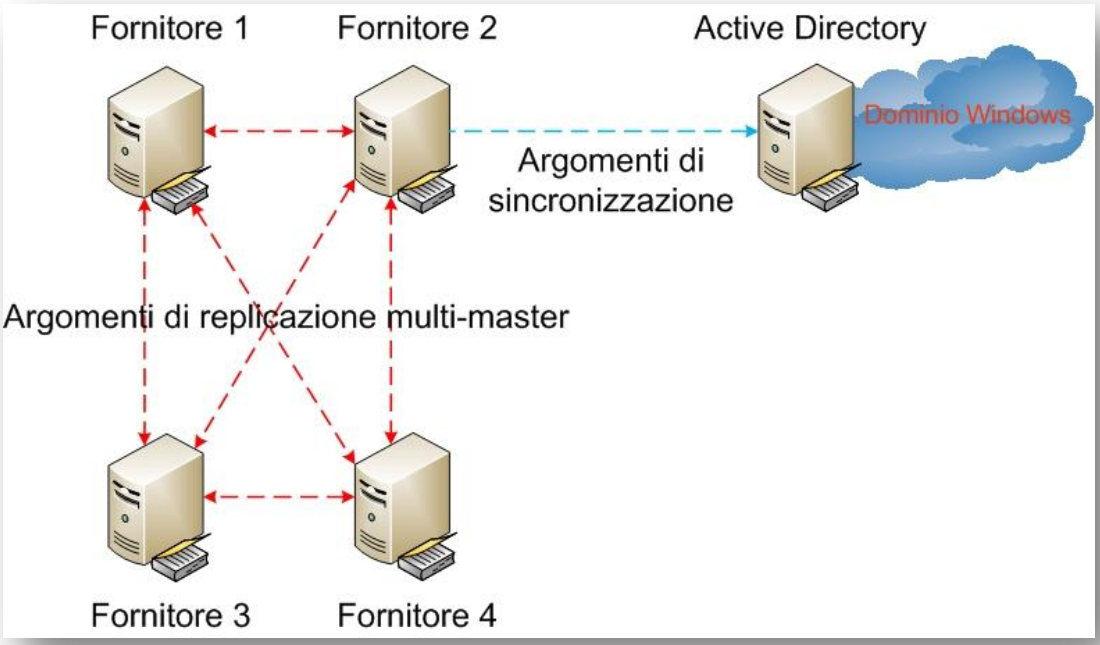
La funzione di sincronizzazione completa è implementata in due parti:

- **Il codice Windows Sync di Fedora Directory Server**: Il server contiene il codice che si svolge una parte considerevole della funzionalità di sincronizzazione. Questo codice è strettamente integrato con il server e con il plug-in multi-master di replicazione. Il changelog stesso, che viene utilizzato per la replica multi-master, viene utilizzato anche per riprodurre in uscita le modifiche che riguardano le voci sincronizzate. Le corrispondenti modifiche vengono apportate in Active Directory, tramite il protocollo LDAP. Il server LDAP esegue anche operazioni di ricerca in senso contrario con Active Directory, per la sincronizzazione in ingresso delle modifiche apportate alle entries reative agli utenti Windows.
- **Il servizio Password Sync**: Questa è una applicazione che deve essere installato sul computer in cui è in esecuzione Active Directory. Il suo scopo è quello di catturare le modifiche delle password per gli utenti di Windows e trasmettere tali modifiche ad Active Directory, tramite il protocollo LDAP con SSL, per grarantire la sicurezza di trasmissione.

La figura successiva riporta la relazione che esiste rispettivamente, tra Fedora Directory Server e Active Directory.



La figura successiva invece riporta come avviene la sincronizzazione tra più Fedora Directory Server e Active Directory.



6.2 Come lavora Windows Sync

La sincronizzazione è configurata e controllata per mezzo di uno o più *accordi di sincronizzazione*. Questi sono simili agli accordi di replica e contengono un'insieme simile di informazioni, incluso il nome host e il numero di porta per Windows Server.

Il Fedora Directory Server si connette al server Windows tramite il protocollo LDAP e SSL per inviare e ricevere aggiornamenti.

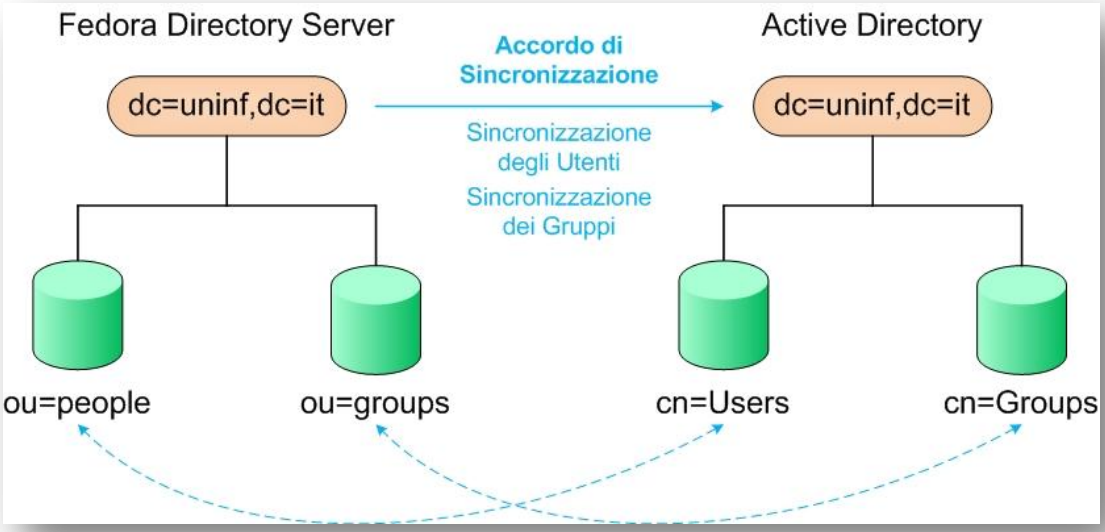
L'unità di sincronizzazione è un sottoalbero. Un unico sottoalbero di Windows può essere sincronizzato con un unico sottoalbero di Fedora Directory e viceversa. Il sottoalbero DNs di Fedora Directory Server e di Active Directory sono specificati neell'accordo di sincronizzazione. Tutte le entries all'interno dei rispettivi sottoalberi sono candidati per la sincronizzazione, comprese le entries che non sono immediatamente figli del sottoalbero root. È importante notare, tuttavia, che ogni discendente contiene entries che dovranno essere create separatamente dall'amministratore. Windows Sync non crea entries contenitore.

Windows Sync fornisce il controllo su alcune entries, che sono sincronizzate. Questo consente agli amministratori di stabilire che solo un sottoinsieme di tutte le entries devono essere oggetto di sincronizzazione e dare una sufficiente flessibilità per supportare vari scenari di distribuzione. Pertanto, certe regole sono applicate prima di determinare se una particolare entry dovrebbe essere sincronizzata e se una nuova entry dove essere creata nel server.

In particolare, solo le entries con classi oggetto users o group, sono sincronizzati da Active Directory a Fedora Directory Server. Inoltre, due flag con l'accordo di scope consentono la creazione di nuove entries per le nuove entries trovate in Active Directory per essere attivate o disattivate. Una flag controlla la creazione di un nuove entries per gli utenti, mentre l'altra flag controlla la creazione di nuove entries per i gruppi. Allo stesso modo, solo le entries con le

necessari, classi oggetto e valori di attributi, saranno sincronizzate in Fedora Directory Server.

Il Fedora Directory Server mantiene un *changelog di replica*, che è costituito da un database che registra le modifiche che sono avvenute. Il changelog è utilizzato da Windows Sync per generare in uscita, le modifiche apportate aa Active Directory. Pertanto, il changelog e i rispettivi oggetti di replica devono essere configurati nel Fedora Directory Server, prima di eseguire Windows Sync.



Durante il normale funzionamento, tutti gli aggiornamenti effettuati a entries in Fedora Directory Server, che devono essere inviate ad Active Directory, sono generate tramite il changelog.

Tuttavia, quando il server è configurato per la prima volta o dopo importanti modifiche al suo contenuto, è necessario avviare un nuovo *processo di sincronizzazione*. Con la risincronizzazione, l'intero contenuto del sottoalbero di sincronizzazione nel Directory Server, viene esaminato e, se necessario, spedito ad Active Directory. Questo viene fatto senza utilizzare il changelog.

Le modifiche dirette verso l'interno, che modificano le entries in Active Directory, si trovano utilizzando la funzione di ricerca "*Dirsync*" di Active Directory. Siccome non vi è alcun changelog da utilizzare, è necessaria una ricerca periodica con Dirsync.

L'intervallo predefinito è di cinque minuti. L'amministratore può anche attivare immediatamente una ricerca Dirsync, cliccando con il tasto destro su un'accordo di sincronizzazione, e selezionando "*Send and Recive Upadates Now*". L'utilizzo della ricerca con Dirsync, assicura che solo le entries, che sono cambiate dopo la precedente ricerca, sono recuperate. Tuttavia, nel caso in cui in un server ci sono stati importanti cambiamenti al suo contenuto, una ricerca con Dirsync può essere eseguita, per restituire tutte le entries (e non solo le entries recentemente cambiate). La ricerca completa con Dirsync viene fatta ogni volta che l'amministratore avvia il processo di "ri-sincronizzazione" accennato precedentemente. In alcune situazioni, non si potrebbe attendere fino a cinque minuti per la prossima ricerca con Dirsync. Infatti durante questo tempo, le recenti modifiche apportate su Active Directory non saranno apportate nel Fedora Directory Server. In questo caso, l'amministratore può avviare manualmente un'immediata ricerca con Dirsync.

In aggiunta ai meccanismi di sincronizzazione discussi precedentemente, il Servizio "*Password Sync*" è necessario per recuperare le passwords modifiche, all'interno di Active Directory. Senza il servizio "*Password Sync*", sarebbe impossibile ottenere le passwords di sincronizzazione, perché per le passwords che devono essere memorizzate in Active Directory, viene calcolato l'hash e memorizzato quest'ultimo al posto delle passwords. La funzione di hashing è incompatibile con quella utilizzata da Fedora Directory Server. Inoltre, non è possibile recuperare i valori della password da un server Windows esterno. Le password provenienti dall'esterno, vengono sincronizzate con altri attributi di ingresso, utilizzando una particolare funzione, del Fedora Directory Server, per conservare i valori delle password in chiaro, nel changelog.

6.3 Installare i Servizi di Sincronizzazione

C'è un servizo che deve essere installato sul computer, in cui è in esecuzione Active Directory, per la sincronizzazione di più aspetti del Fedora Directory Server con Windows Server.

Password Sync deve essere installato sul sistema Windows in cui è in esecuzione Active Directory. Esso sincronizza le modifiche apportate alle password in Active Directory, con le voci corrispondenti passwords nel Fedora Directory Server.

6.3.1 Installazione del Servizio Password Sync

Arrivati a questo punto installiamo e configuriamo, sul server Windows in cui è in esecuzione Active Directory, il servizio *PassSync*, che è comodamente scaricabile dal seguente link: http://directory.fedoraproject.org/download/PassSync-20060330.msi. Mostriamo di seguito i passi necessari per l'istallazione:

1. Copiamo il file *PassSync-200060330.msi* nel server Windows;
2. Doppio click sul file *PassSync-200060330.msi* per avviare l'installazione; appare la finestra di setup di Password Sync, cliccare su "*Next*" per inizialre l'installazione;
3. Inserire i paramentri come il nome host del Fedora Directory Server, il numero di porta con SSL, il nome utente (come `cn=sync manager,cn=config`), il certificato (password), e la base di ricerca (come `ou=People,dc=uninf,dc=it`);
4. Installati i parametri e completata la procedura di installazione occorre riavviare la macchina Windows per avviare Password Sync.

Password Sync viene installato nella cartella:; `C:\Programmi\Red Hat Directory Password Synchronization\` e `passsync.exe` è l'unico file nella directory di installazione. Nel sistema Windows vengono installate le seguenti `.dlls`, nella cartella: `C:\winnt\system32\`, utilizzate da Password Sync:

```
    passhook.dll                nsldap32v50.dll
    nsldapssl32v50.dll          libplc4.dll
    nsldappr32v50.dll           nss3.dll
    libnspr4.dll                ssl3.dll
```

Il servizio Password Sync viene eseguito come servizio di Windows, il che significa che esso può essere avviato, arrestato, ed è controllato dal comando `net start|stop`, l'applet del pannello di controllo del servizio Servizi, e di altri meccanismi di gestione dei servizi di Windows.

I cambiamenti di password vengono catturati, anche se il servizio di sincronizzazione Password non è in esecuzione. Se il servizio di sincronizzazione delle password (*Password Sync*) viene riavviato, i cambiamenti delle passwords sono immediatamente inviati al Fedora Directory Server.

6.4 Abilitare la crittografia SSL per PassSync

A questo punto provvediamo all'abilitazione della crittografia per PassSync.

Per prima cosa andiamo a creare due nuovi database, per i certificati (`cert8.db`) e per le chiavi (`key.db`), tramite console di Windows, nella macchina in cui è installato Password Sync, come segue.

```
cd "C:\Programmi\Red Hat Directory Password Synchronization\"
certutil.exe –d . -N
```

Ci viene chiesto di fornire una password che verrà usata per criptare le chiavi, come segue.

```
Enter new password:********
Re-enter password:********
```

A questo punto ci spostiamo sulla macchia Linux e da shell digitiamo i seguenti comandi, per poter esportare il certificato del server, usando l'utility

pk12util.

```
cd "/opt/fedora-ds/alias/"
pk12util –d . –P slapd-fedora8- -o servercert.p12 –n Server-Cert
```

Ci viene chiesto di inserire la password o il pin per il database dei certificati NSS, come segue.

```
Enter Password or Pin for "NSS Certificate DB":
```

Per fare in modo che venga esportato il certificato, invece di inserire la password, andiamo ad inserire il pin, contenuto nel file `slapd.fedora8.pin.txt`, che si trova nella directory: `/opt/fedora8-ds/alias/`, vediamo un esempio di tale file.

```
Internal (Software) Token:cc175ab117edd9fb57117e163ee3177c7e5d8d23
```

Ora ci viene chiesto di fornire la password per il file PKCS12, come segue.

```
Enter password for PKCS12 file:********
Re-enter password:********
```

A questo punto, se tutto è avvenuto correttamente, ci viene indicato che l'esportazione del certificato è avvenuta con successo. Il file contenete il certificato è `servercert.p12`, e si trova nella directory `/opt/fedora8-ds/alias/`. Copiamo il file, contenete il certificato, nella cartella `C:\Programmi\Red Hat Directory Password Synchronization\` della macchina Windows, e importiamo il certificato del Fedora Directory Server, all'interno del database dei certificati, presente nella macchina Windows, con l'utility `pk12util.exe`, come segue.

```
pk12util.exe –d "C:\Programmi\Red Hat Directory Password
Synchronization" –i servercert.p12
```

Ci viene chiesto di inserire la password o il pin per il database dei certificati NSS, come segue.

```
Enter Password or Pin for "NSS Certificate DB":********
```

Non inseriamo il pin, ma la password precedentemete impostata, in seguito ci viene chiesto di inserire la password per il file PKCS12, come segue.

```
Enter password for PKCS12 file:********
```

Se tutto è avvenuto correttamente, ci viene indicato che l'importazione del certificato è avvenuta con successo.

Occorre impostare lo stato di "reciproca fiducia" con il server, andando ad esguire il seguente comando.

```
certutil.exe –d "C:\Programmi\Red Hat Directory Password
Synchronization" –M –n Server-Cert –t "P,P,P"
```

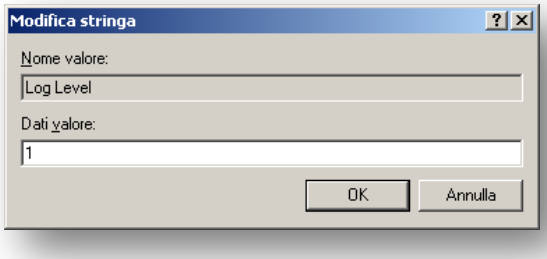
A questo punto andiamo a vedere le proprieta associate al certificato, digitando il seguente comando.

```
certutil.exe –d "C:\Programmi\Red Hat Directory Password
Synchronization" -L
```

Ci viengono mostrati i seguenti valori.

```
CA certificate                                    c,c,c
Server-Cert                                       Pu,Pu,Pu
```

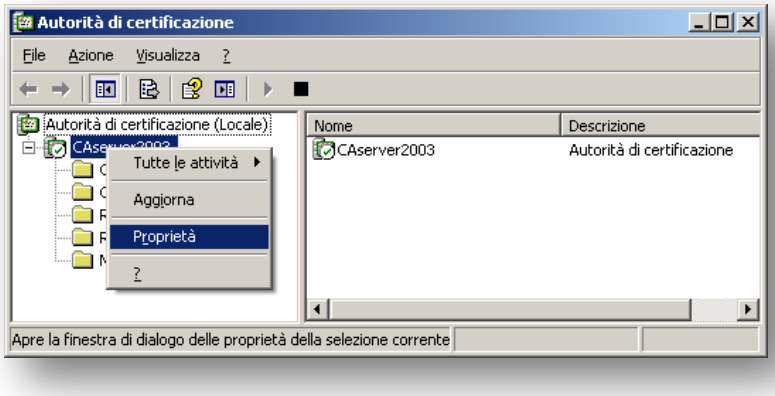
Il passo succesivo è quello di abilitare il logging a PassSync, nel seguente modo. Andare su "*Start*"→"*Esegui…*", inserire nella finestra di dialogo "*Regedit*" e cliccare su "*Ok*" per avviare l'applicazione. Una volta aperta l'applicazione andare su "`HKEY_LCAL_MACHINE`"→"`SOFTWARE`"→"`PasswordSync`" e impostare il valore `1` nel "`Log Level`", come è visibile nell'immagine successiva.



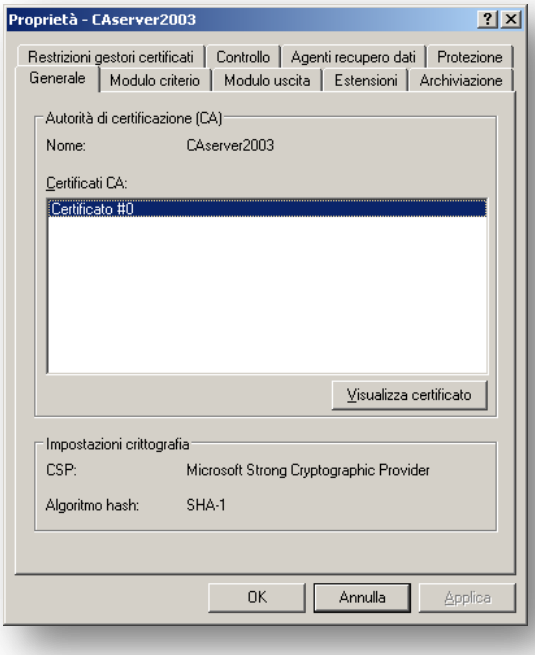
Quindi confermare la modifica cliccando su "*Ok*", a questo punto il logging per Password Sync è abilitato e il file si trova nella cartella `C:\Programmi\Red Hat Directory Password Synchronization\`.

6.5 Abilitare la crittografia SSL per FDS

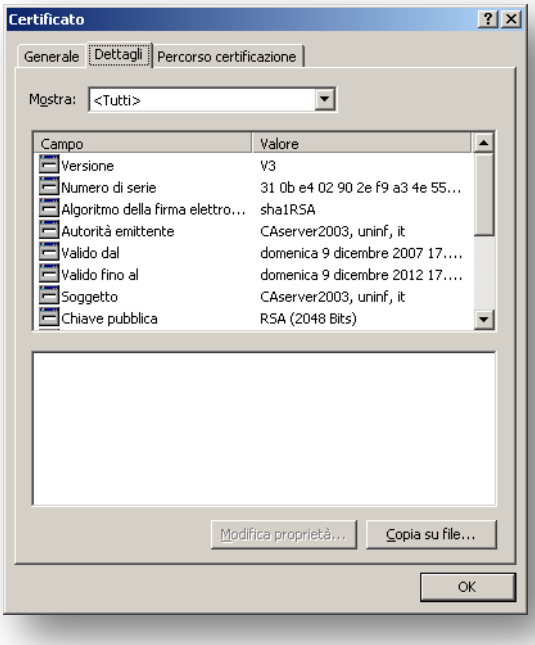
Per poter abiltare la crittografia SSL, occorre innanzitutto esportare il certificato della macchina Windows e importarlo in Fedora Directory Server. Quindi andiamo su "*Start*"→"*Strumenti di amministrazione*"→"*Autirità di certificazione*" e qundi clicchiamo con il tasto destro sul nome della CA, e quindi su "*Proprietà*", come evidente nell'immagine seguente.



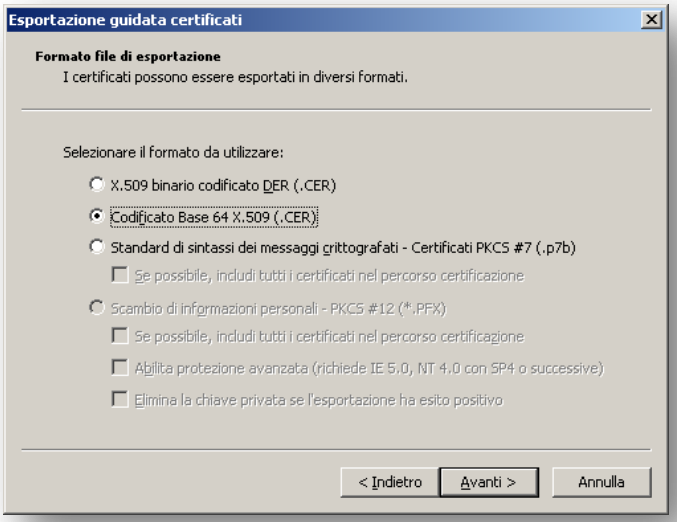
Quindi cliccando su "*Proprietà*" compare la seguente finestra.



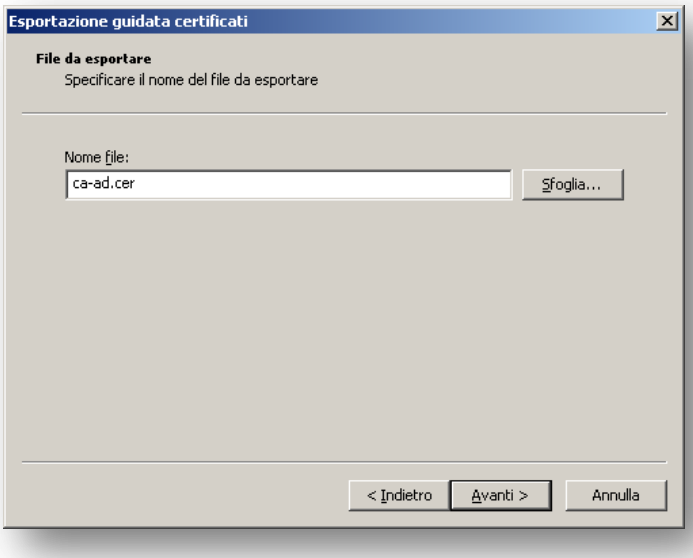
A questo punto clicchiamo su "*Visualizza Certificato*" e dalla finestra "*Details*" del certificato appena aperto, selezioniamo "*Copia su file…*".



Cliccando su "*Copia su file…*" viene aperto il seguente wizard per esportare il certificato.



Nella finestra selezioniamo "*Codificato Base 64 X.509 (.CER)*" come visibile nell'immagine, e cliccare su "*Avanti* >" a questo punto ci viene aperta la segente finestra, in cui inserire il nome del file contenente il certificato da esportare.

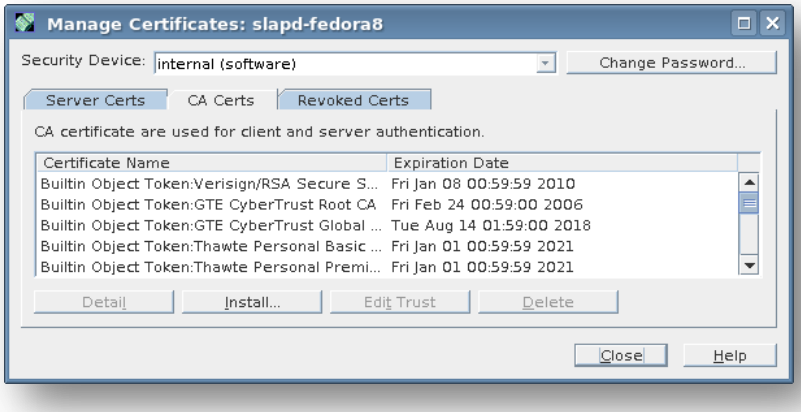


Inseriamo il nome del file, ad esempio *ca-ad.cer* e clicchiamo su "*Avanti* >", poi nella finestra successiva su "*Fine*", per completare l'esportazione del certificato. Quindi prendiamo il file *ca-ad.cer* e lo copiamo all'interno della macchina Linux.

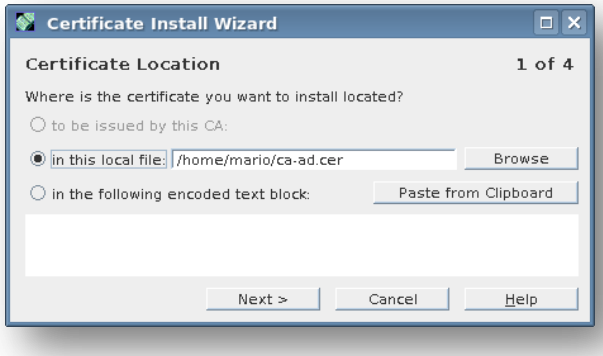
Una volta copiato il file, mandiamo in esecuzione la Console di Fedora Directory Server, e importiamo il certificato nel seguente modo.

Clicchiamo due volte su "*Directory Server (fedora8)*" e ci viene fornita la seguente schermata.

Clicchiamo su "*Manage Certificates*" e ci viene aperta la seguente finestra di dialogo.

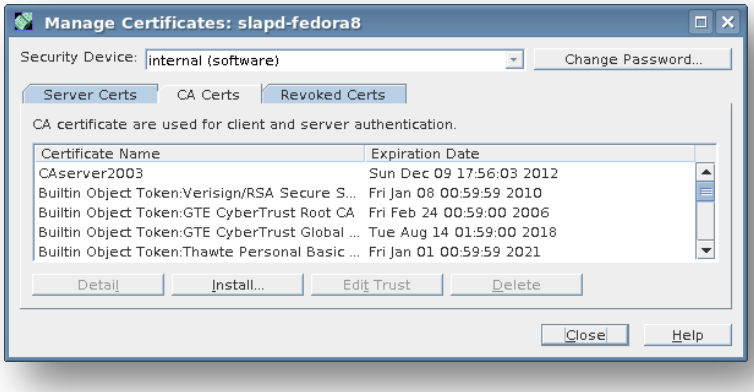


A questo punto clicchiamo su "*Install…*" ci viene mostrata la seguenter finestra in cui inserire il percorso del file contenete il certificato da importare.

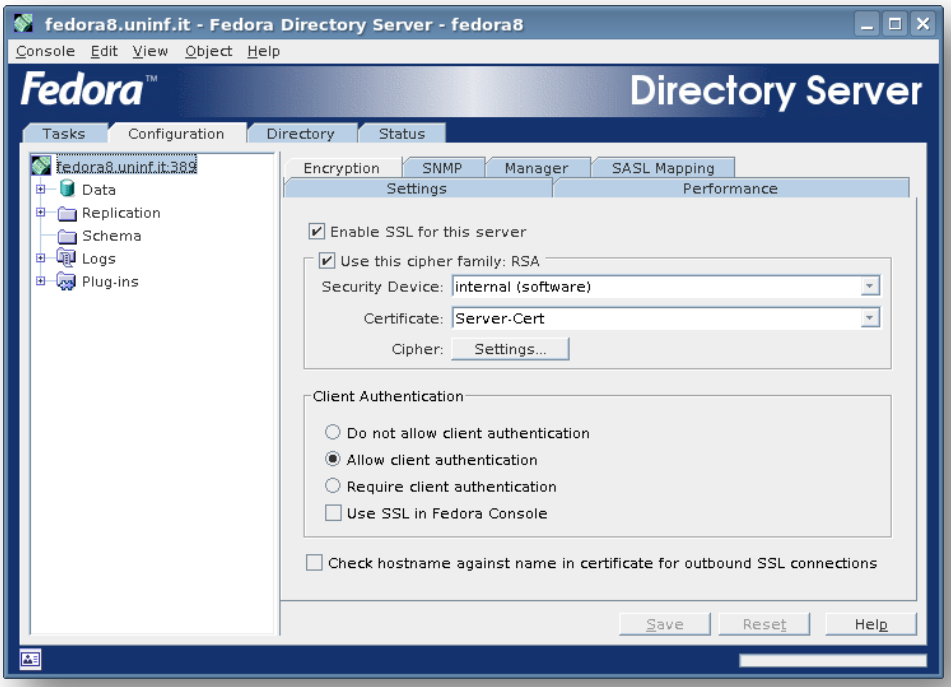


Clicchiamo su "*Next >*" nelle tre finestre di dialogo successive e arriviamo all'ultima finestra, visibile nell'immagine successiva.

Nella precedente finestra, lasciamo le impostazione come riportato e clicchiamo su "*Done*". A questo se tutto è andato per il verso giusto, il certificato è installato nella CA del Fedora Directory Server, come segue.



Completata tale procedura, è possibile abilitiare l'SSL di Fedora Directory Server, andado su "*Configuration*"→"*Encryption*" e abilitando l'SSL per il server, come è evidente nell'immagine successiva.



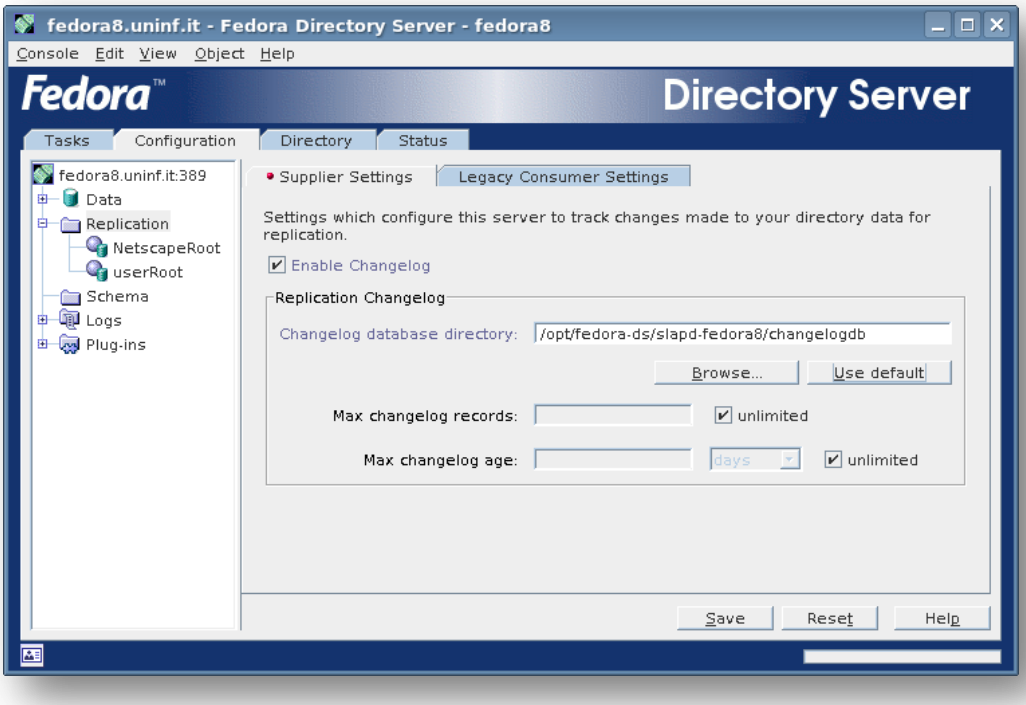
A questo punto occorre riavviare Fedora Directory Server, per poter rendere effettive le modifiche. Quindi eseguiamo i seguenti comandi da shell.

```
[root@uninf fedora-ds]# /etc/init.d/fedora-ds restart
Stopping slapd trying: fedora8                             [  OK  ]
Starting slapd trying: fedora8                             [  OK  ]
[root@uninf fedora-ds]# /etc/init.d/fedora-ds-admin  restart
Riavvio di Fedora-DS Admin:                                [  OK  ]
```

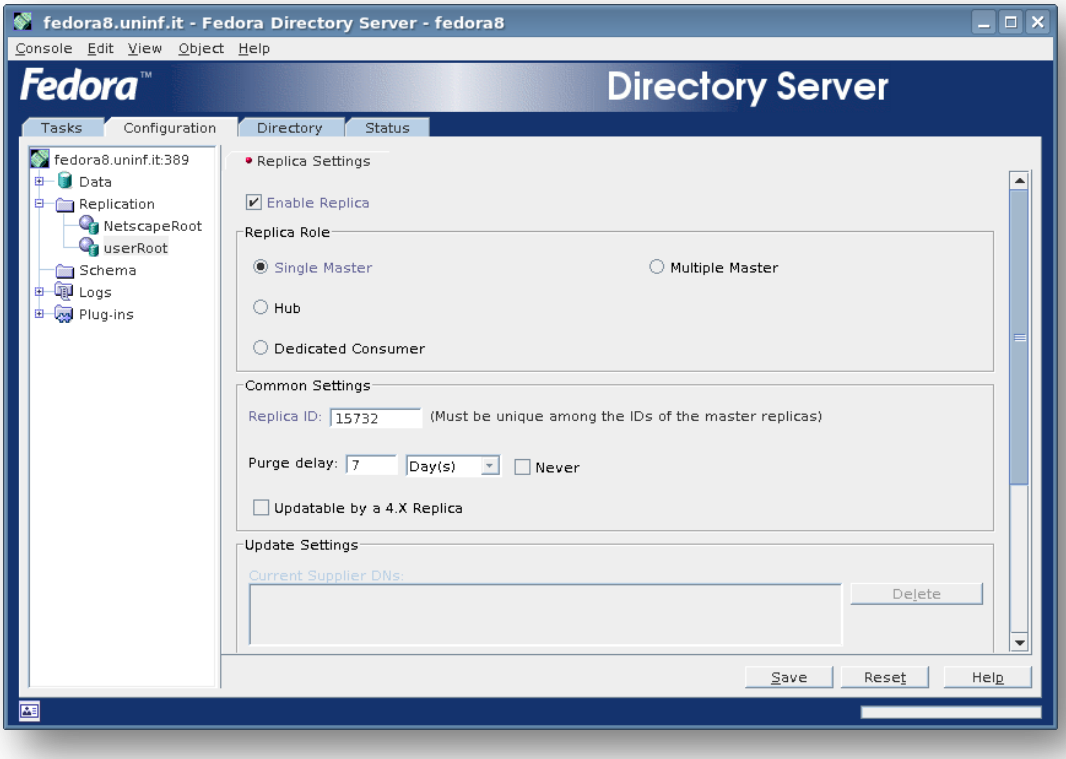
6.6 Configurare i Parametri di FDS

Per poter configurare i parametri relativi alla sincronizzazione, procediamo in questo modo, facciamo doppio click su "*Directory Server (fedora8)*" quindi clicchiamo sulla scheda "*Configuration*", poi nell'albero a sinistra, clicchiamo su "*Replication*" e nella schermata a destra abilitiamo il changelog spuntando "*Enable Changelog*" in "*Supplier Settings*". Mentre in "*Replication Changelog*" possiamo

impostare il percorso del changelog, scegliendo "*Browse*…", oppure più semplicemente cliccare su "*Use default*" e ci viene inserito automaticamente il percorso di default per il changelog, come evidente nell'immagine successiva.

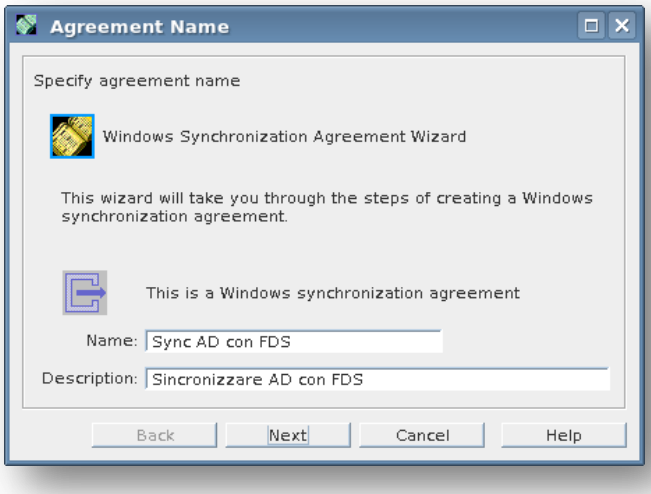


Per confermare le impostazioni clicchiamo su "*Save*". Poi andiamo su "*userRoot*" e abilitiamo la replica, spuntando "*Enable Replica*" in "*Replica Settings*" e spuntiamo "*Single Master*" in "*Replica Role*", mentre in "*Common Settings*" specifichiamo il parametro "*Replica ID*", come evidente nell'immagine.

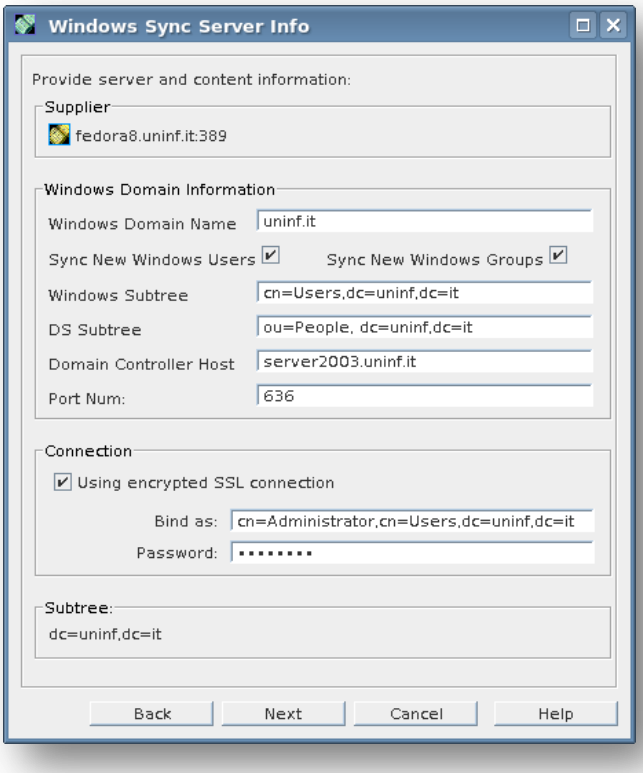


Quindi clicchiamo su "*Save*" per memorizzare le impostazioni effettuate.

A questo punto clicchiamo con il tasto destro su "*userRoot*", ci viene aperto un menù in cui andiamo a cliccare su "*New Windows Sync Agreement*", ci viene apero il seguente wizard in cui impostare tutti gli attributi.



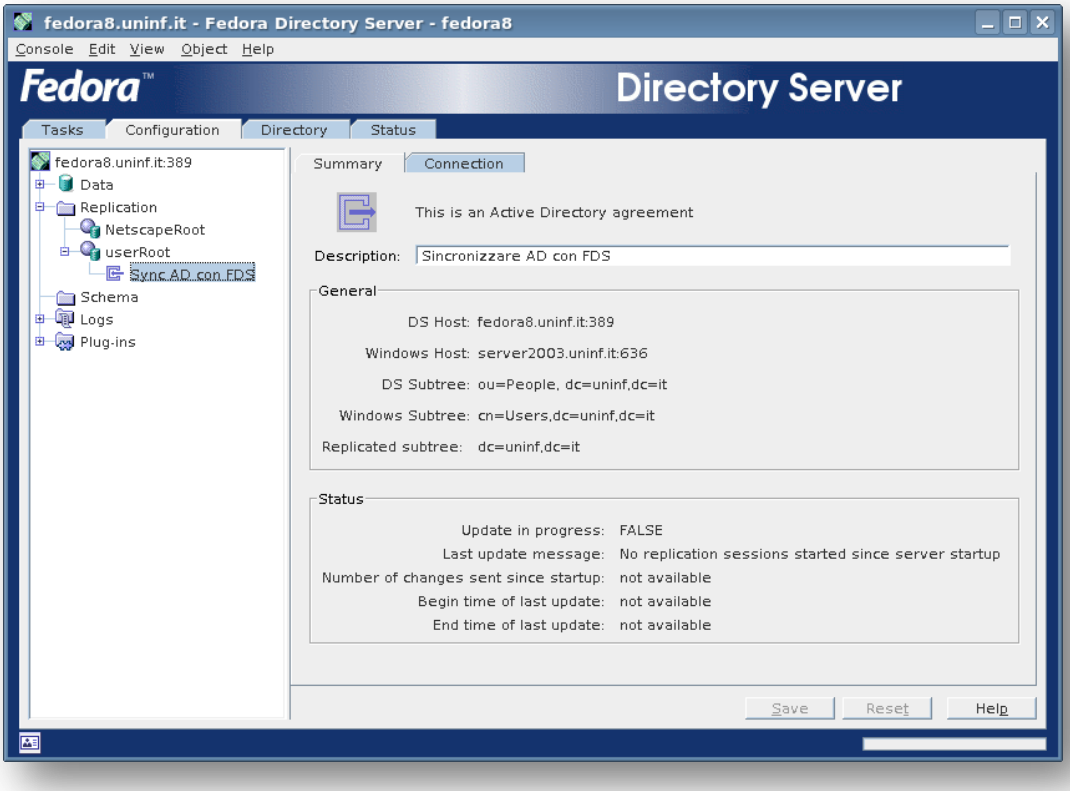
Nell'immagine precedente abbiamo inserito il nome "*Sync AD con FDS*" e la descrizione "*Sincronizzare AD con FDS*", poi clicchiamo su "*Next*" e ci viene mostrata la segente schermata, in cui inserire diversi parametri.



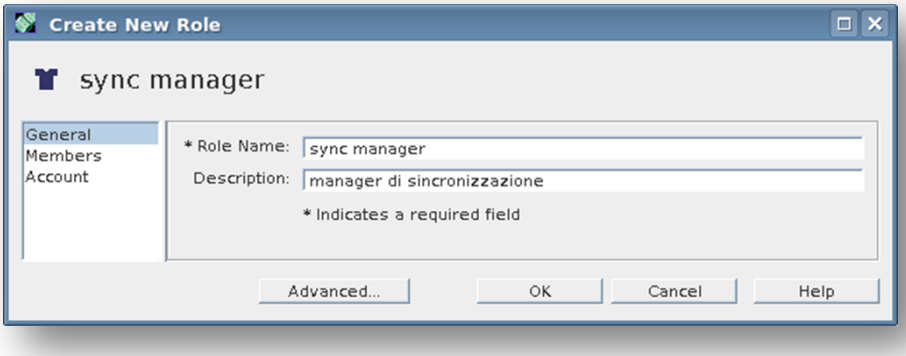
I parametri specificati nell'immagine precedente nel "*Windows Domain Information* " sono, il nome del dominio di Windows "*uninf.it*", spuntare entrembe le opzioni "*Sync New Windows Users*" e "*Sync New Windows Groups*", per abilitare la sincronizzazione sia degli utenti che dei gruppi. Poi è stato specificato il sottoalbero di Active Directory, contenete gli utenti "*cn=Users,dc=uninf,dc=it*" e il sottoalbero di Fedora Directory Server, contenete gli utenti "*ou=People,dc=uninf,dc=it*". Poi è stato pecificato l'host che contiene in cui è in esecuzione il *Domain Controller*, ossia la macchina in cui è in esecuzione Active Directory "*server2003.uninf.it*" e la porta crittografata "*636*".

In "*Connection*" invece è stata spuntata l'opzione "*Use encrypted SSL connection*" e specificato il DN dell'amministratore della macchina Windows "*cn=Administrator,cn=Users,dc=uninf,dc=it*" con la relativa password. Una volta

competta l'immissione di tali informazioni clicchiamo su "*Next*" per proseguire. A questo punto ci viene mostrato il sommario delle impostazioni, e clicchiamo su "*Done*" per confermare. Andiamo quindi a osservare, nell'immagine seguente, il risultato reativo alle impostazioni appena effettuate.



Arrivati a questo punto, per far funzionare la sincronizzazione, dobbiamo creare una nuova ruolo chiamato "*sync manager*" in "*config*". Per fare questo, clicchiamo sulla scheda "*Directory*" poi clicchiamo con il tasto destro su "*config*", ci viene aperto un menù in cui selezionare "*New*", ci viene aperto un altro sottomenù, in cui selezionare "*Role…*" e ci viene mostrata la seguente finestra.



Nella finestra sovrastante andiamo ad inserire il nome del ruolo "*sync manager*" e la relativa descrizione "*manager di sincronizzazione*", a questo punto clicchiamo su "*Ok*" per confermare e quindi creare il nuovo ruolo.

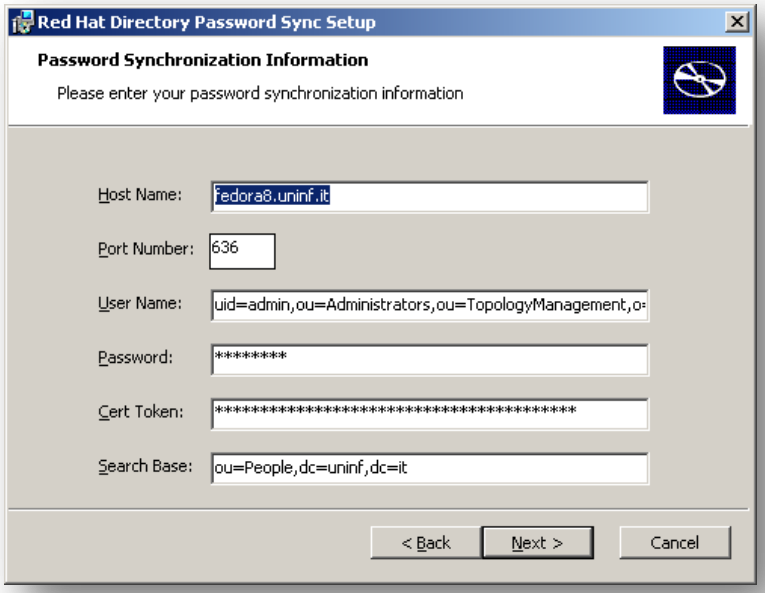
6.7 Configurare i Parametri di PassSync

Per poter impostare i giusti parametri di sincronizzazione in Password Sync, avviamo nuovamente l'installazione del file *PassSync-200060330.msi* e clicchiamo su "*Modify*" per poter modificare le impostazioni di configurazione;

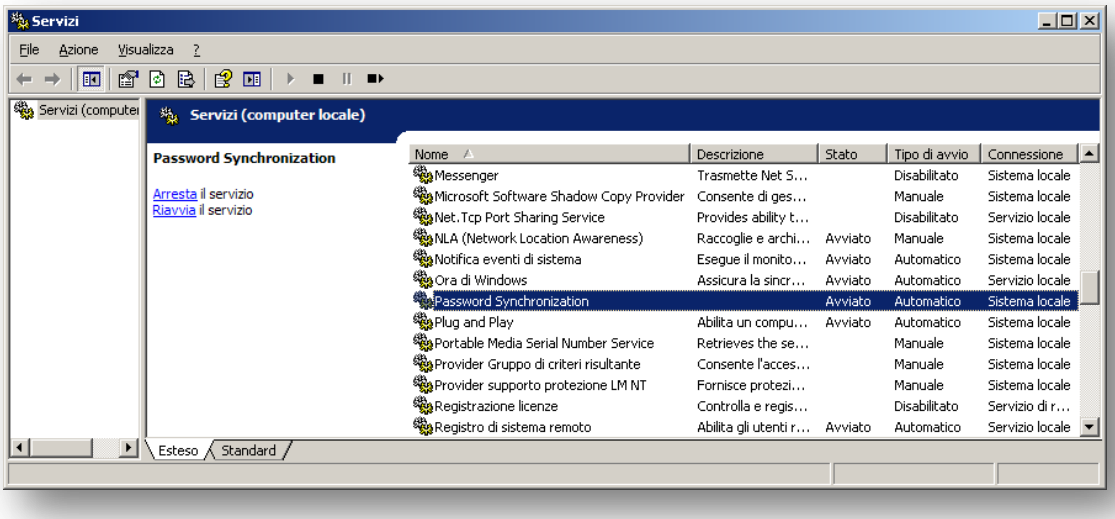
I parametri che occorre specificare sono, il nome host della macchina Linux in cui è in esecuzione Fedora Directory Server "*fedora8.uninf.it*", la porta crittografata "*636*", il nome utente dell'amministratore di Fedeora Directory Server "*uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot*", e la relativa password. Poi si deve inserire il token del certificato che è presente nel file *slapd-fedora8-pin.txt.* Nel nostro caso tale valore è quello precedentemente visto ossia:

```
Internal (Software) Token:cc175ab117edd9fb57117e163ee3177c7e5d8d23
```

E per ultimo occorre inserire il DN di base per la ricerca, in cui sono contenuti gli utenti all'interno di FDS "*ou=People,dc=uninf,dc=it*", vediamo un esempiio nell'immagine successiva.



Per completare la configurazione clicchiamo su "*Next* >" e poi su "*Install*" quindi su "*Finish*". A questo punto per far funzionare PassSync con le nuove impostazioni riavviamo il servizio nel seguete modo. Clicchiamo su "*Start*"→ "*Strumenti di amministrazione*"→"*Servizi*", ci viene mostrata la finestra contenete tutti i servizi di Windows Server 2003, troviamo il servizio "*Password Synchronization*" e clicchiamo su "*Riavvia*".



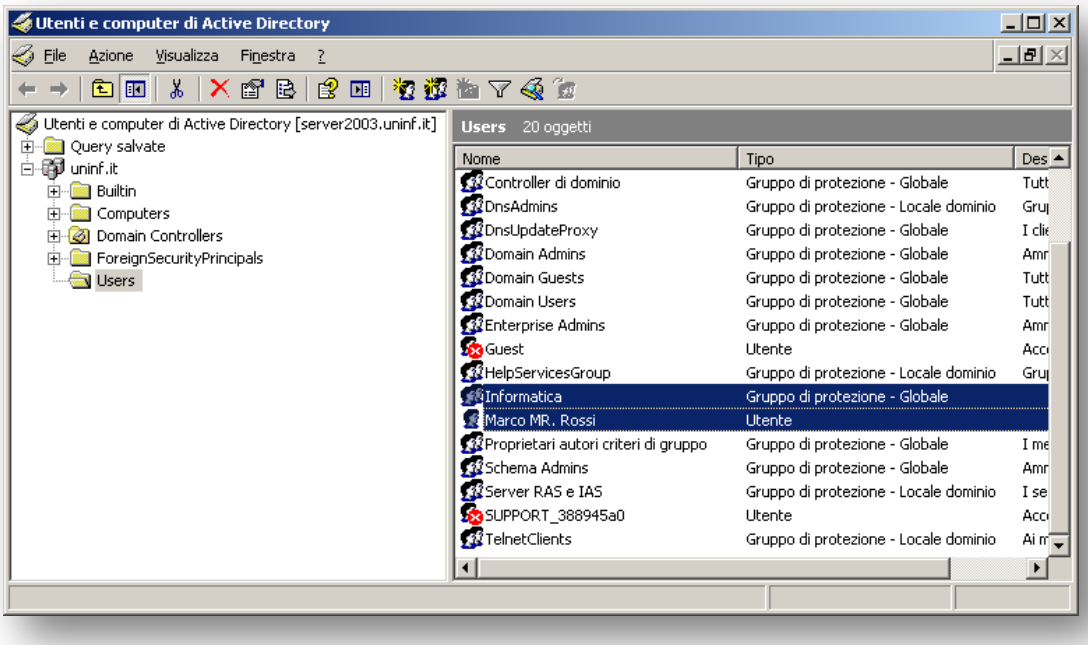
Per controllare se il servizio è partito correttamente, possiamo aprire il file `passsync.log` presente nella cartella `C:\Programmi\Red Hat Directory Password`

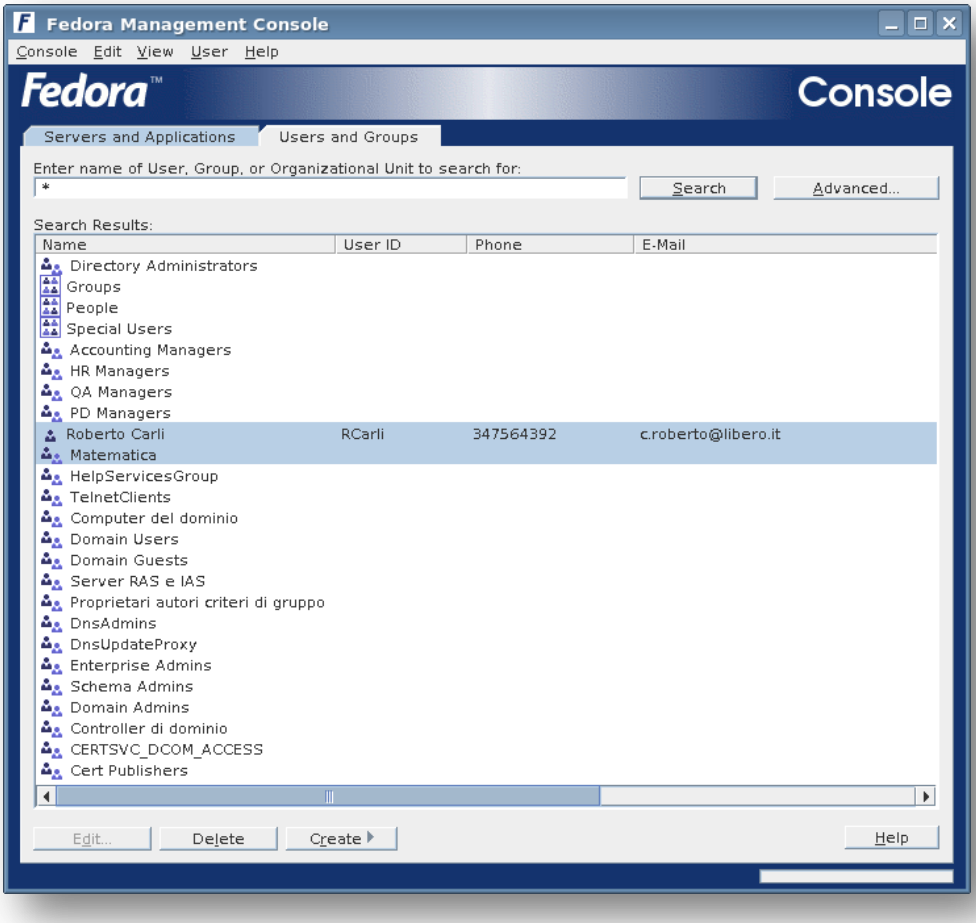
`Synchronization\` e vedre le informazioni che il servizio ci fornisce. Le informazioni possono essere di errore, per segnalare il problema che si è verificato nel momento in cui si è avviato il servizio, oppure che il servizio è partito correttamente, come nel caso visibile di seguito.

```
01/01/08 19:20:53: PassSync service started
```

6.8 Verifica del Funzionamento della Sincronizzazione

In Active Dirctory prima della sincronizzazione, è memorizzato l'utente "*Marco Rossi*" e il gruppo "*Informatica*" come visibile dall'immagine seguente.

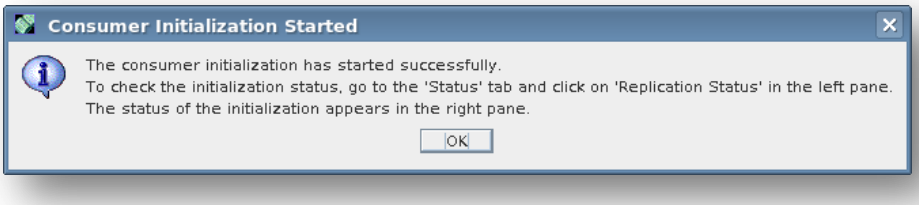




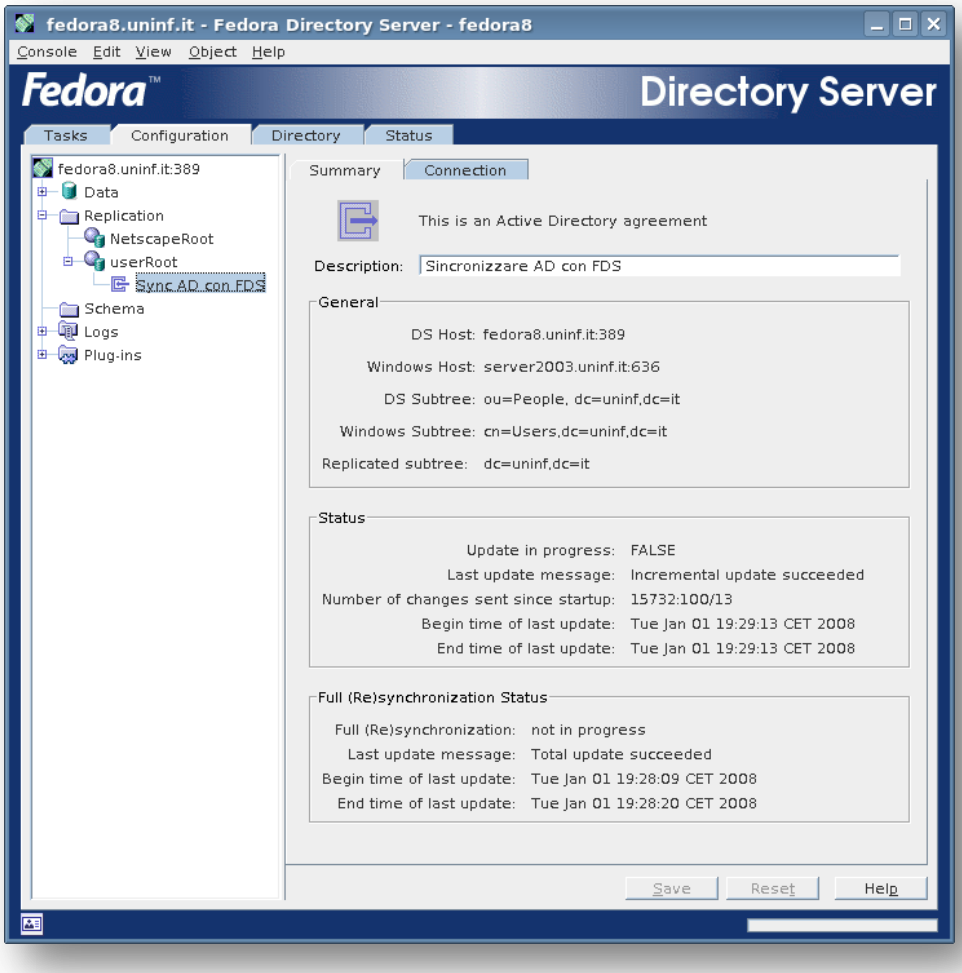
Mentre in Fedora Directory Server, prima della sincronizzazione, è memorizzato l'utente "*Roberto Carli*" e il gruppo "*Matematica*" come visibile dall'immagine precedente.

A questo punto per sincronizzare gli utenti e i gruppi presenti in Active Directory e in Fedora Directory Server, effettuiamo tale operazione. Andiamo nella Console di Fedora Directory Server, clicchiamo su "*Configuration*" e espandiamo il sottoalbero di sinistra a partire da "*Replication*". Ci viene mostrato "*NetscapeRoot*" e "*userRoot*" espandiamo anche "*userRoot*" e troviamo "*Sync AD con FDS*" precedentemente creato. Clicchiamo con il tasto destro su "*Sync AD con FDS*" e selezioniamo, se è la prima volta che si effettua la sincronizzazione, "*Initiate Full Re-syncronization*" per sincronizzare tutto il sottoalbero, oppure nelle successive volte utilizziamo "*Send and Recive Updates Now*". Nella successiva finestra di avvertimento cliccare su "*Yes*" e il processo di sincronizzazione si avvia.

Al termine del processo di sincronizzazione, viene mostrata la seguente finestra, in cui ci viene riportato l'esito della sincronizzazione.



Mentre l'immagine successiva riporta lo stato dopo la sincronizzazione.



In "*Status*" vengono riportati tutti i dettagli della sincronizzazione.

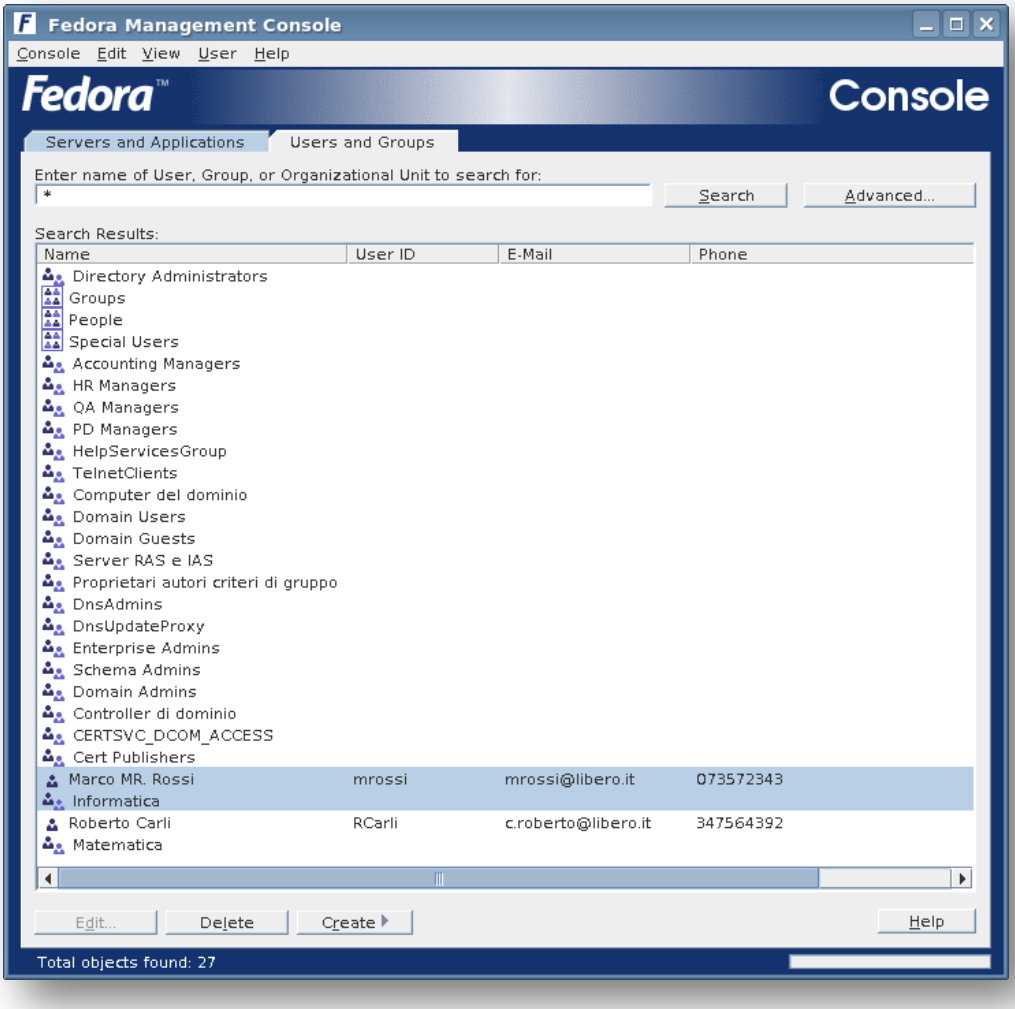
- **Update in Progress**: Ci indica se stà avvenendo una sincronizzazione;

- **Last Update Message**: Ci indica se la sincronizzazione è avvenuto correttamente;
- **Number of changes sent since startup**: Ci riporta il numero di cambiamenti apportati dall'avvio;
- **Begin time of last update**: Il tempo in cui è iniziata l'utima sincronizzazione;
- **End time of last update**: Il tempo in cui è finita l'utima sincronizzazione.

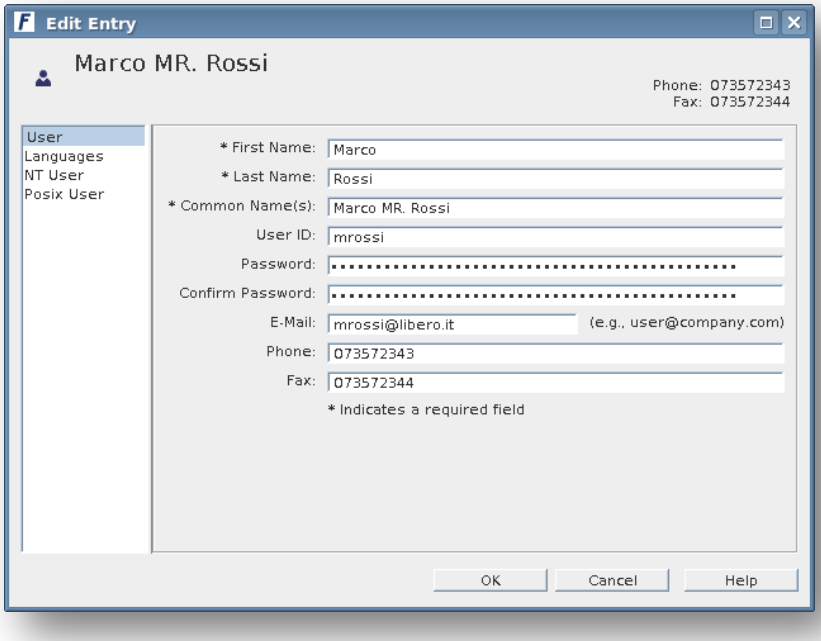
In "*Full (Re)synchronization Status*" vengono riportati tutti i dettagli della re-sincronizzazione.

- **Full (Re)synchronization**: Ci indica se stà avvenendo una re-sincronizzazione;
- **Last Update Message**: Ci indica se la re-sincronizzazione è avvenuto correttamente;
- **Begin time of last update**: Il tempo in cui è iniziata l'utima re-sincronizzazione;
- **End time of last update**: Il tempo in cui è finita l'utima re-sincronizzazione.

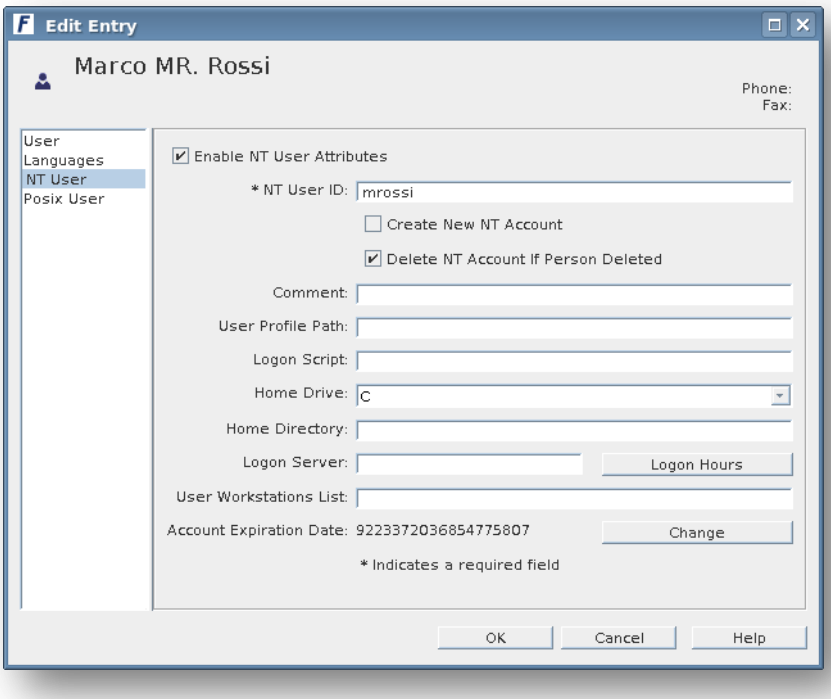
Quindi andiamo a vedere come sono cambiati i dati all'interno delle Directory di Active Directory e di Fedora Directory Server. In Active Directory non è stato aggiunto nessun nuovo utente ne gruppo. Mentre in Fedora Directory Server, è stato aggiunto l'utente e il gruppo, con i rispettivi valori, contenuti in Active Directory. Come risulta evidente in fondo all'immagine seguente.



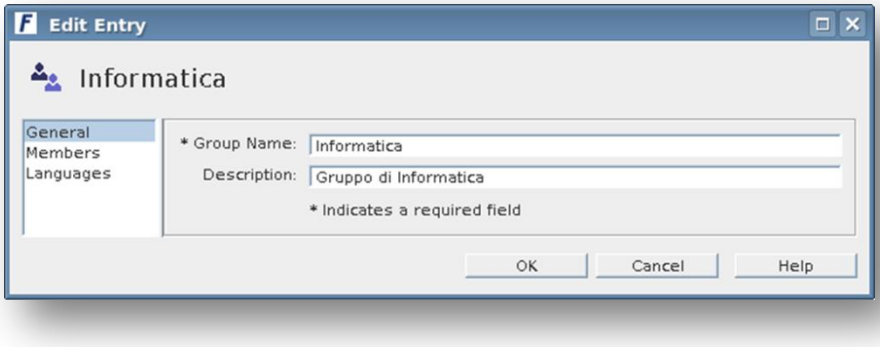
Vediamo, cliccando sull'utente "*Marco Rossi*", aggiunto dal processo di sincronizzazione, le informazioni ad esso associate.



Vediamo nell'immagine, che sono riportare tutte le informazioni dell'utente impostate quando era stato creato l'utente in Active Directoy. E' presente anche la password, che è stata spedita dal servizio, precedentemente descritto, *Password Sync*. Sono stati impostati automaticamente anche gli attributi per un utente NT, come evidente dall'immagine seguente.

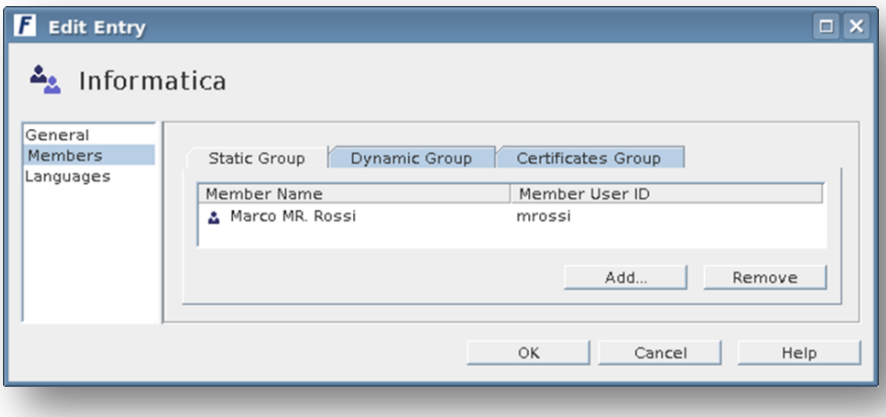


Vediamo invece nell'immagine successiva i dettagli del gruppo aggiunto dalla sincronizzazione.

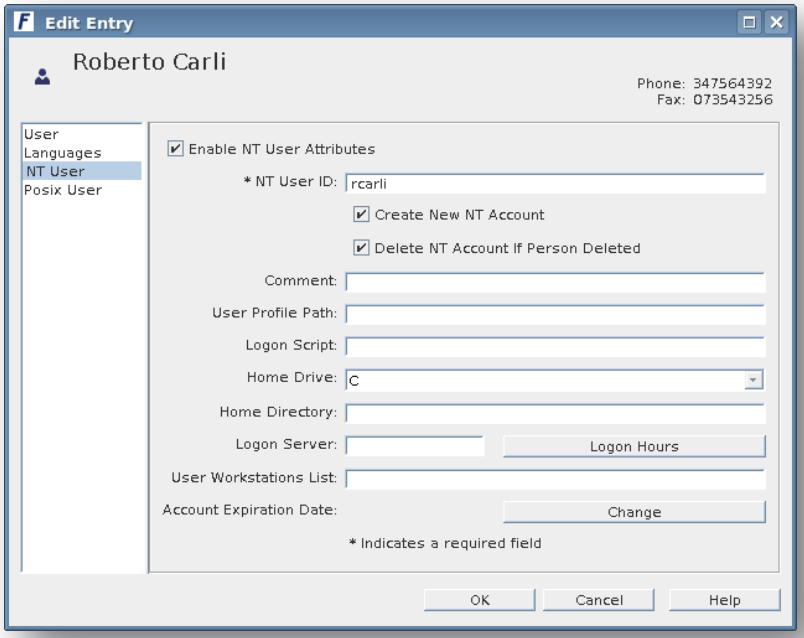


Come è evidente dall'immagine viene aggiunto il gruppo, ma non la sua descrizione, in quanto non è un campo impostabile in Active Directoy. Comunque è sempre possibile aggiungerlo successivamente in Fedora Directory Server.

Vediamo anche, nell'immagine seguente i dettagli del gruppo aggiunto con la sincronizzazione, ossia i membri che fanno parte di tale gruppo.

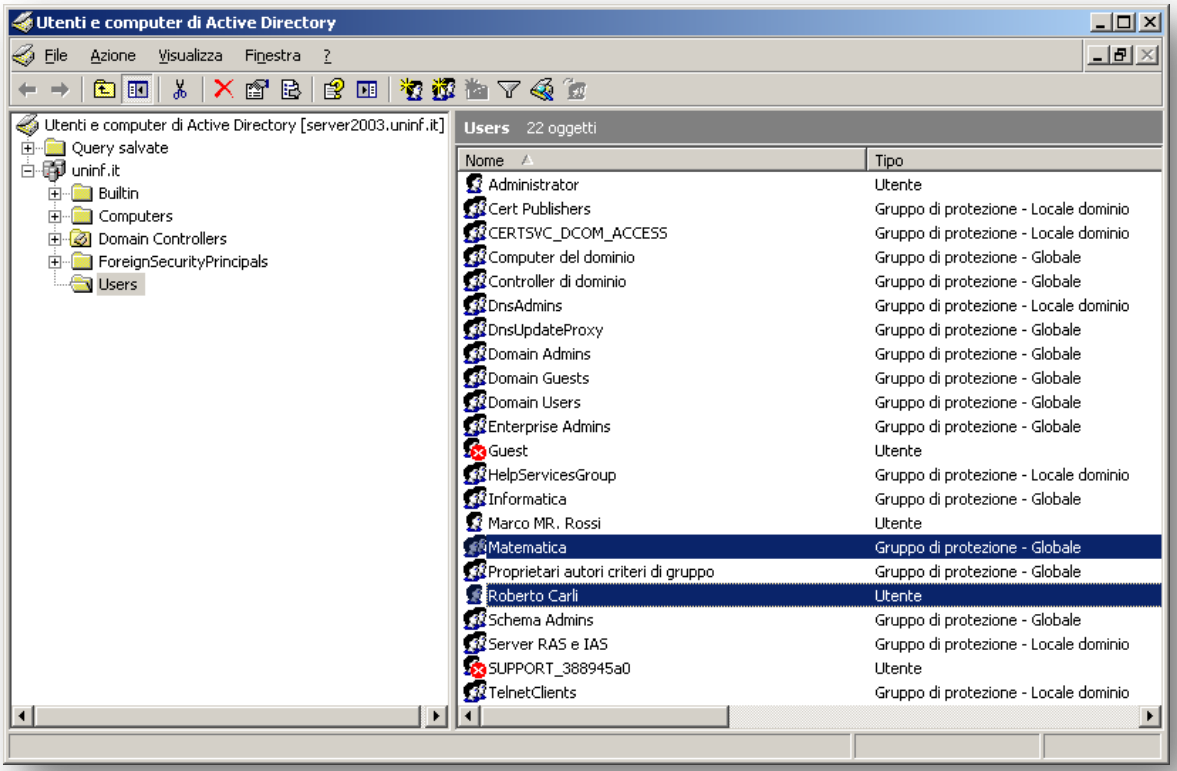


Per fare in modo che anche l'utente "*Robeto Carli*", e il gruppo "*Matematica*" siano trasferito, e quindi memorizzati, in Active Directory occorre andare ad abilitare "*Enable NT User Attributes*" per l'utente "*Robeto Carli*", come segue.



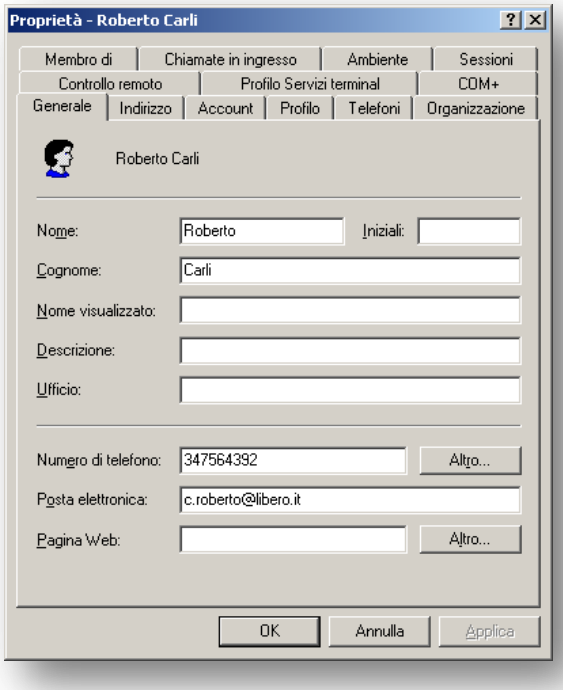
Una volta inserito "** NT User ID*" e spuntato le due opzioni "*Create New NT Account*" e "*Delete NT Account if Person Deleted*" è possibile cliccare su "*Ok*" per confermare le modifiche.

A questo punto per avviare la sincronizzazione andiamo sulla console di Fedora Directory Server, clicchiamo su "*Configuration*" e espandiamo il sottoalbero di sinistra a partire da "*Replication*". Ci viene mostrato "*NetscapeRoot*" e "*userRoot*" espandiamo anche "*userRoot*" e troviamo "*Sync AD con FDS*". Clicchiamo con il tasto destro su "*Sync AD con FDS*" e selezioniamo "*Send and Recive Updates Now*". Qunidi andiamo ad osservare se l'utente e il gruppo sono stati aggiunti in Active Directory, tramite "*Utenti e computer di Active Directory*" come evidente nell'immagine successiva.

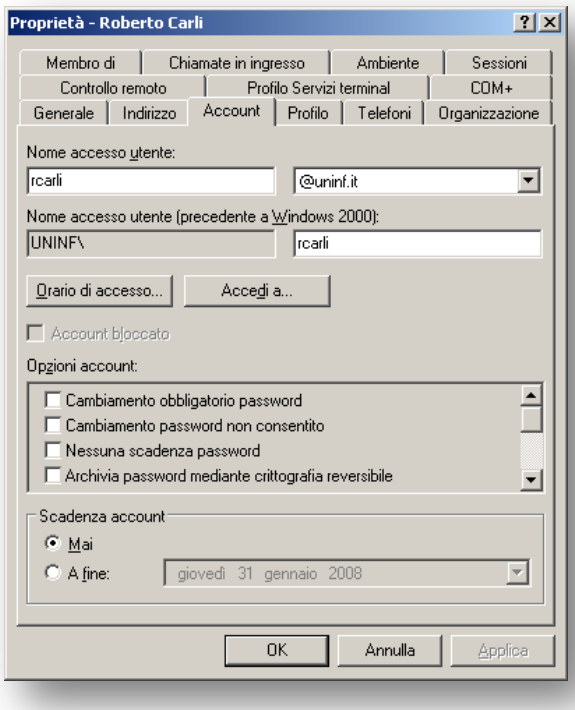


Come risulta evidente dall'immagine sovrastante, l'utene "*Roberto Carli*" e il gruppo "*Matematica*" sono stati aggiunti in Active Directory.

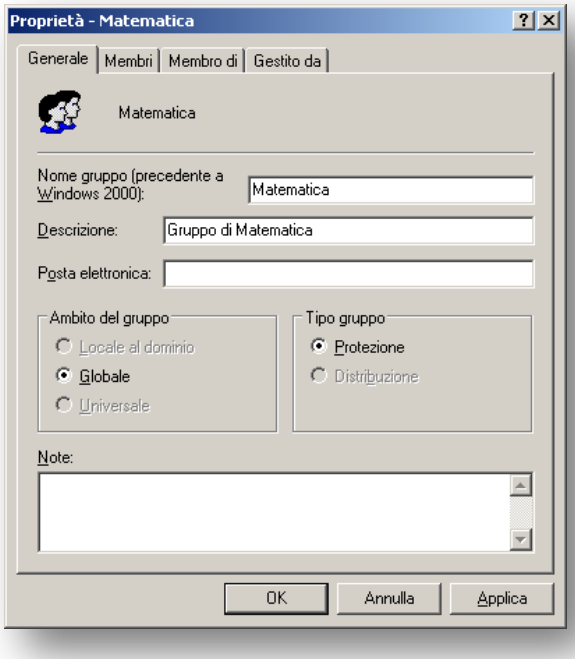
Quindi mostriamo le informazioni generali associate all'utente, cliccado su di esso. Tali informazioni sono state impostate precedentemente durante la creazione dell'utente, in Fedora Directory Server.



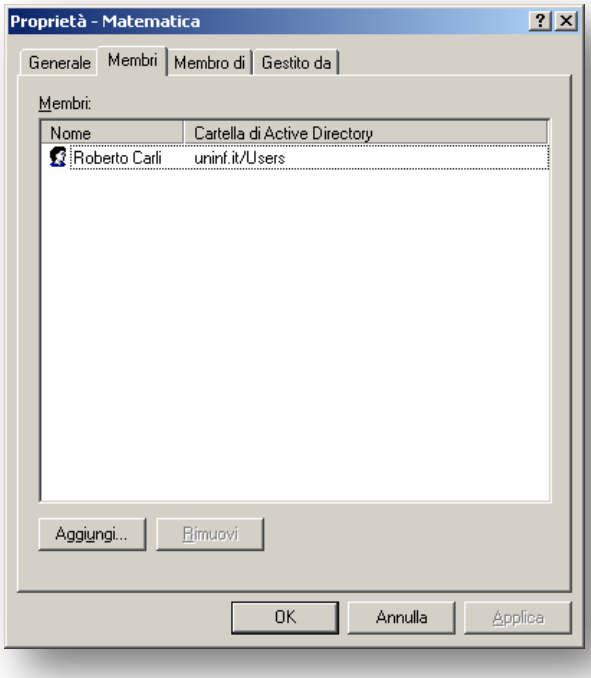
Vediamo invece mell'immagine seguente le informazioni relative all'account dell'utetnte aggiornato.



Vediamo ora i dettagli relativi al gruppo "*Matematica*" aggiunto, cliccando su di esso.



E vediamo anche i membri associato a tale gruppo. Le informazioni visibili sono state impostate precedentemente, durante la creazione del gruppo in Fedora Directory Server.



Se invece andiamo ad elimiare un utente o un gruppo all'interno ai Active Directory, e poi andiamo ad effettuare una nuova sincronizzazione, con "*Initiate Full Re-syncronization*" o con "*Send and Recive Updates Now*" l'utente o il gruppo viene cancellato anche in Fedora Directory Server. Anche nel caso in cui un'utente o un gruppo viene eliminato in Fedora Directory Server, allora con una nuova operazione di sincronizzazione, l'utente o il gruppo viene eliminato anche in Active Directory.

L'utente può decidere di effettuare quindi manualmente una completa sincronizzazione del sottoalbero, utilizzando l'opzione "*Initiate Full Re-syncronization*", oppure inviare aggiornamenti parziali, utilizzando l'opzione "*Send and Recive Updates Now*". Comunque c'è anche la possibile effettuare sincronizzazioni in automatico, senza intervento dell'utente, e questa avviene ogni cinque minuti. Così ogni nuovo utente o gruppo aggiunto, verrà replicato, al massimo dopo cinque minuti, automaticamentenell'altro Directory Server.

6.9 Sincronizzazione delle Entries

Uno speciale schema è applicato alle entries nel Fedora Directory Server, che sono oggetto di sincronizzazione. Tale schema è molto simile, ma non identica, a quello usata dal vecchio Netscape Directory Server 4.x NT per la funzione di sincronizzazione.

In primo luogo, vi è una clausula per individuare la corrispondente entry, per una data entry di Windows. Questo viene fatto grazie all'attributo *ntUniqueId*, che contiene il valore del attributo *objectGUID* per la corrispondente entry. Questo attributo è totalmente sotto il controllo del codice di sincronizzazione e non devono essere modificati manualmente. Mentre, l'attributo *ntDomainUser* contiene il valore del attributo *samAccountName* dalla corrispondente entry di Windows.

Infine, gli attributi *ntUserCreateNewAccount* e *ntUserDeleteAccount* controllano il ciclo di vita della corrispondente entry di Windows. Solo se *ntUserCreateNewAccount* ha un valore true, viene creata una nuova entry nel server Windows. Allo stesso modo, solo se *ntUserDeleteAccount* ha un valore true, la corrispondente entry è cancellata, quando l'entry nel Fedora Directory Server è cancellata. Questi attributi consentono all'amministratore di esercitare un preciso controllo sul ciclo di vita delle entries sincronizzate.

La tabella sottostante mostra gli attributi che vengono mappati tra il Fedora Directory Server e Active Directory.

Fedora Directory Server	**Active Directory**
cn	**name**
ntUserDomainId	**sAMAccountName**
ntUserHomeDir	homeDirectory
ntUserScriptPath	scriptPath
ntUserLastLogon	lastLogon
ntUserLastLogoff	lastLogoff
ntUserAcctExpires	accountExpires
ntUserCodePage	codePage
ntUserLogonHours	ogonHours
ntUserMaxStorage	maxStorage
ntUserProfile	profilePath
ntUserParms	userParameters
ntUserWorkstations	userWorkstations

Mentre la seguente tabella mostra gli attributi, che sono gli stessi tra Fedora Directory Server e Active Directory.

description	postOfficeBox
destinationIndicator	postalAddress
facsimileTelephoneNumber	postalCode
givenName	registeredAddress
homePhone	sn
homePostalAddress	st
initials	street
l	telephoneNumber
mail	teletexTerminalIdentifier

mobile	telexNumber
o	title
ou	userCertificate
pager	x121Address
physicalDeliveryOfficeName	

6.10 Gruppi

Simile alle entries per gli utenti, le entry del gruppo sono sincronizzate se hanno la classi oggetto *ntGroup* e *mailgroup*. Ci sono anche due attributi per il controllo, della creazione e l'eliminazione, delle entries di gruppo in Active Directory: *ntGroupCreateNewAccount* e *ntGroupDeleteAccount*.

Lo scope della entries del Gruppo sono all'interno dell'accordo di sincronizzazione e verrà sincronizzato in modo simile alle entries degli utenti. Inoltre,i membri del gruppo sono sincronizzati in relazione con i soli membri che sono anche all'interno dello scope, degli accordi che sono propagati. Il risultato è che un gruppo può contenere i membri che sono contemporaneamente all'interno e all'esterno dello scope dell'accordo, ma solo il sottoinsieme dei membri che sono allo stesso tempo un accordo di scope sono sincronizzati. I restanti membri sono lasciati invariati su entrambi i lati.

La tabella seguente, mostra gli attributi, che vengono mappati tra Fedora Directory Server e Active Directory.

Fedora Directory Server	**Active Directory**
cn	**name**
ntGroupAttributes	groupAttributes
ntGroupId	cn name samAccountName
ntGroupType	groupType
uniqueMember	member

Mentre la seguente tabella mostra gli attributi, che sono gli stessi tra Fedora Directory Server e Active Directory.

seeAlso	l
description	ou

6.11 Compatibilità dello Schema di Active Directory

Sebbene Active Directory supporta la stessa base di classi oggetto X.500 di Fedora Directory Server, ci sono un paio di sottili incompatibilità di cui gli amministratori devono essere consapevoli:

- Sia Active Directory che Fedora Directory Server possono rafforzare la politica sulle password per far rispettare alcuni requisiti sulle password: lunghezza minima, età massima, e così via. Windows Sync non sincronizzare le politiche, né garantire che le politiche siano coerenti. Quindi gli amministratori di entrambi i sistemi devono garantire la corenza delle politiche. Se la politica della password non è coerente, allora le modifiche apportate alla password, in un sistema, potrebbe non funzionare quando riprodotto su altro sistema.

- Gruppi nidificati (dove un gruppo contiene un altro gruppo in qualità di membro) sono supportati e saranno sincronizzati. Tuttavia, Active Directory impone determinati vincoli per la composizione dei gruppi annidati. Ad esempio, un gruppo locale di dominio non può essere un membro di un gruppo globale. Fedora Directory Server non ha alcuna nozione di gruppi locali e globali, e quindi, è possibile creare entries su Fedora Directory Server, che violano i vincoli di Active Directory quando sono sincronizzate. Anche in questo caso, è responsabilità degli amministratori, garantire che questo non accada.

- Active Directory utilizza l'attributo *streetAddress* per un utente o un gruppo fisico o un'indirizzo postale. Fedora Directory Server utilizza l'attributo RFC2798 *inetOrgPerson street* per questo scopo. Tuttavia, come definito nel RFC2256, *streetAddress* è un alias per *street*. Per peggiorare la confusione, Active Directory ha anche l'attributo *street*, ma non è un alias per *streetAddress* ma un attributo che può contenere un valore. Windows Sync mappe *streetAddress* in Active Directory su *street* in Fedora Directory Server, e, pertanto, esclude l'uso dell'attributo *street* in Active Directory [32] [33] [34].

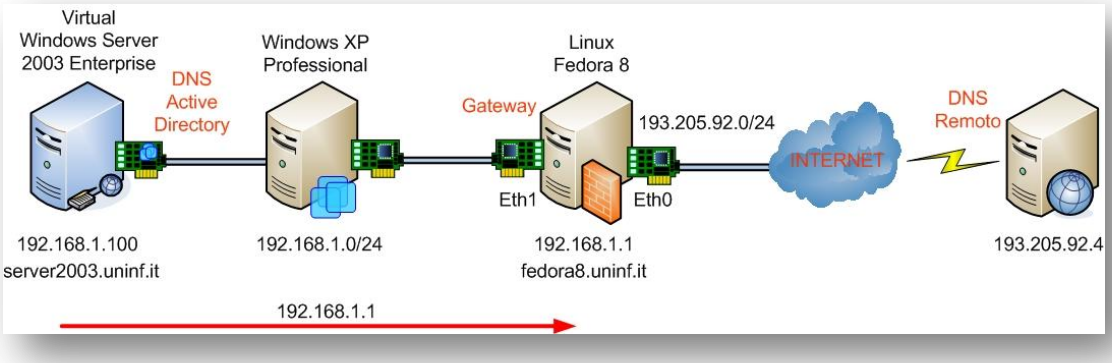
CAPITOLO 7

DNS E ACTIVE DIRECTORY

7.1 DNS Microsft e Active Directory

Nell'installazione e configurazione descritta precedentemente, relativa ad Active Directory, è stato installato e configurato il DNS Microsft. Questo perché per poter funzionare adeguatamente Active Directory necessita di un server DNS che supporta i records RSV. La Microsft raccomanda l'utilizzo del DNS disponibile in Windows Server 2003, ma in un dominio di rete in cui è disponibile già un server DNS installato e configurato su una macchina Linux, come il server DNS BIND, è possibile configurare quest'ultimo per supportare Active Directory.

Nella figura seguente viene riportato le interrogazioni al server DNS configurato su Windows Server 2003.

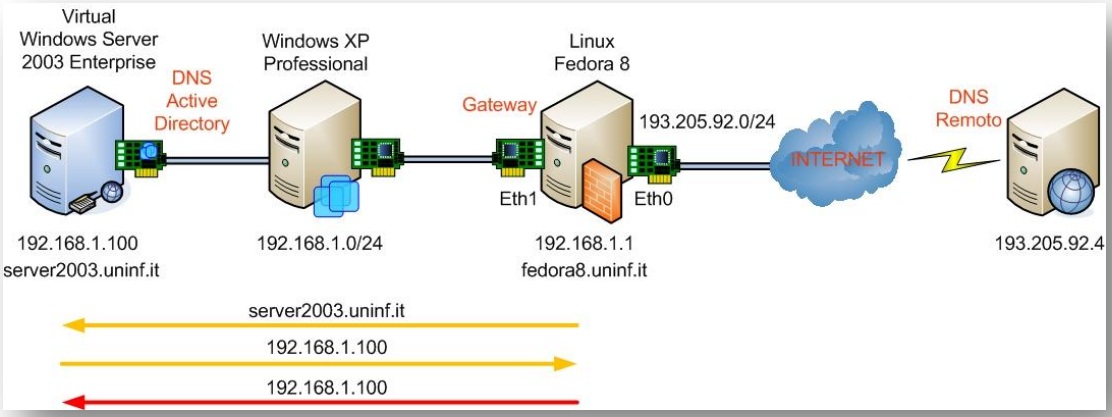


Nell'immagine precedente è evidente lo schema della rete precedentemente configurato, con il server DNS installato su Windows Server 2003. Tale immagine riporta anche un esempio di interrogazione, tramite il comando *ping* che viene effettuato a partire dal server Windows.

```
ping fedora8.uninf.it
```

Il precednte comando quindi effettua un'interrogazione al server DNS presente nella stessa macchina, per la risoluzione di *fedora8.uninf.it*. Gli viene fornito l'indirizzo IP relativo, e quindi è possibile verificare la raggiungibilità della macchina Linux.

Nel caso invece dell'immagine successiva, lo stesso comando *ping* viene eseguito dalla macchina Linux, per poter verificare la raggiungibilità del server Windows.



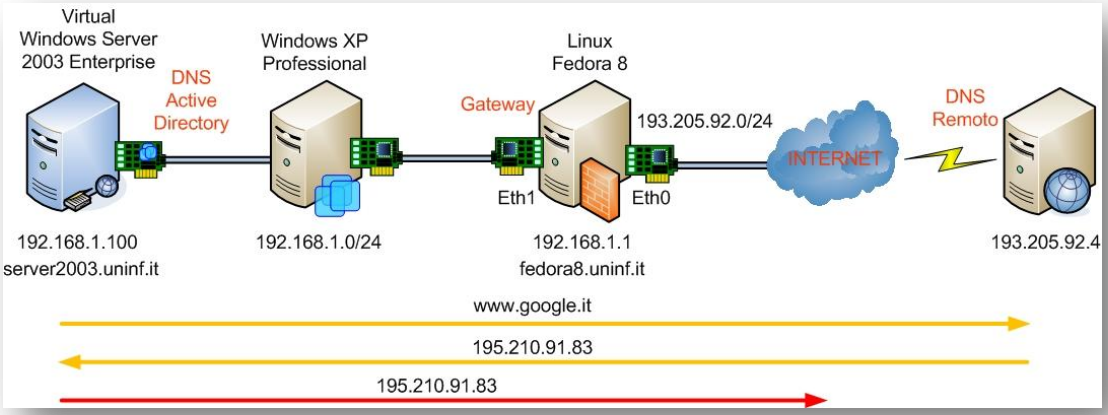
Il comando relativo è il seguente.

```
ping server2003.uninf.it
```

In questo caso il comando *ping* contatta il server Windows per la risoluzione dell'indirizzo IP del server Windows; l'indirizzo relativo viene fornito alla macchina Linux, il quale può provvedere a verificare la raggiungibilità del server Windows.

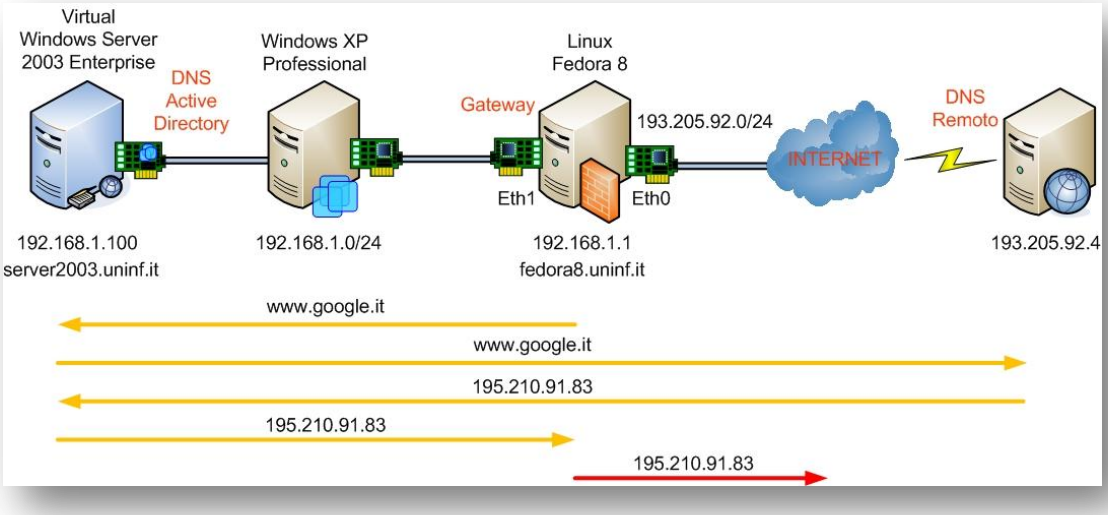
Vediamo invece nell'immagine successiva un'interrogazione relativa alla risoluzione di un indirizzo esterno alla rete LAN locale, utilizzando anche in questo caso il comando *ping*.

```
ping www.google.it
```



Come risulta evidente dall'immagine, viene contattato un server DNS esterno, se il server locale non contiene l'informazione, per la risoluzione dell'indirizzo IP relativo alla macchina esterna alla rete LAN locale. A questo punto l'indirizzo IP viene trasmesso alla macchina richiedente, che può effettuare la verifica della rraggiungibilità della macchina presente in Internet.

L'ultimo esempio riportato di seguito, mostra sempre l'utilizzo dello stesso comando *ping*, non più a partire dal server Windows, ma a partire dalla macchina Linux, per la risoluzione di un'indirizzo IP appartenete ad una macchina dislocata in Internet.

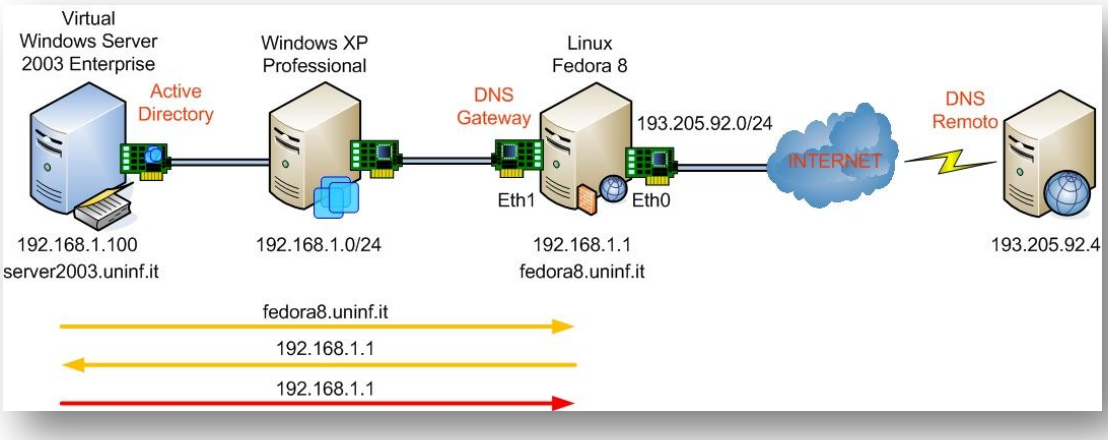


Come risulta evidente dall'immagine, inizialmente la richiesta di risoluzione dell'indirizzo IP, per la macchina presente in Internet, viene trasmessa al server

DNS presente nel server Windows; se quest'ultimo non contiene l'informazione, provvede a contattare un server DNS esterno che gli fornira sicuramente l'indirizzo IP di risoluzione. A questo punto il server Windows lo potrà fornire alla macchina Linux, la quale effettuerà la verifica di raggiungibilità della macchina dislocata in Internet. Vedimo dagli esempi mostrati precedentemente, come tutte le richieste di risoluzione sono inviate al server DNS installato sul server Windows.

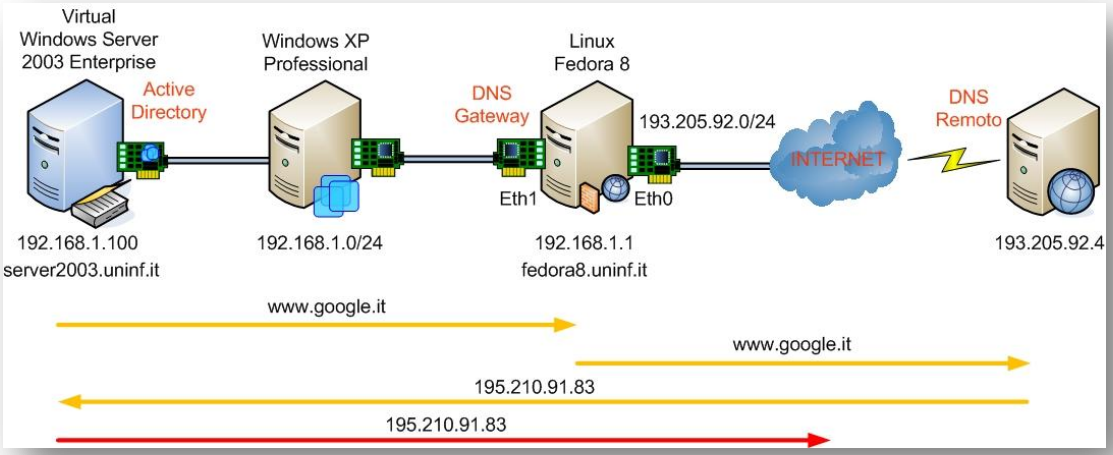
7.2 BIND DNS e Active Directory

In questo paragrafo invece descriviamo come è possibile posizionare il server DNS sulla macchina Linux, e utilizzarlo per ogni risoluzione. Inoltre verrà descritto come configurare Active Directory per poter lavorare con tale server DNS.



Vediamo nell'immagine precedente, come il comando ping eseguito sul server Windows, va a conttattare il server DNS BIND, installato e configurato sulla macchina Linux, per ottenere l'indirizzo IP della macchina Linux. Una volta ricevuto è possibile verificare la raggiungibilità della macchina Linux.

Mentre nell'immagine successiva viene mostrato come è possibile effettuare una risoluzione di una macchina dislocata in Internet.



Dall'immagine vediamo come il comando *ping*, eseguito sul server Windows, contatta il server DNS BIND per la risoluzione, e quest'ultimo non avendo a disposizione l'informazione, contatta il server DNS remoto, il quale fornisce il relativo indirizzo IP al server DNS locale, che a sua volta lo fornisce al server Windows. A questo punto è possibile verificare la raggiungibilta della macchina dislocata in Internet.

7.3 Installazione e Configurazione del Server DNS BIND

Per poter installare il server DNS BIND su un sistema Linux Fedora 8, procediamo nel seguente modo. Apriamo il terminale e da shell ci logghiamo come utente *root* con il comando *su*, poi digitamo il seguente comando.

```
[root@fedora8]# yum install bind
```

il precedente comando non fa altro che installare l'ultima versione disponibile di BIND ossia 9.5. A procedura completata andiamo ad avviare il servizio *named* relativo al server DNS andando ad eseguire il seguente comando.

```
[root@fedora8]# /sbin/service/named start
```

Arrivati a questo punto, il server DNS è correttamente installato sulla macchina Linux, quindi si procede con la configurazione per adattarlo alle nostre esigenze. Per prima cosa andiamo a modificare il seguente file.

```
[root@fedora8]# nano /etc/resolv.conf
```

Una volta aperto tale file impostiamo i seguenti valori.

```
search fedora8
nameserver 192.168.1.1
```

Una volta impostati tali valori salviamo il file e usciamo dall'editor. A questo punto possiamo verificare il funzionamento del server DNS andando a verificare se il seguente comando ha una risposta affermativa e quindi se la risoluzione dell'indirizzo IP è avvenuta correttamente.

```
[root@fedora8]# ping google.com
```

Quindi il precedente comando verifica che il server DNS riesce a risolvere gli indirizzi IP di macchine dislocate in Internet, ma non può risolvere gli indirizzi IP relativi alle macchine interne alla rete LAN. Per fare in modo che vengano risolti anche gli indirizzi IP delle macchine interne, occore andare a modificare diverisi file relativi al DNS. Il primo di essi è il seguente.

```
[root@fedora8]# nano /etc/named.conf
```

Esso è un normale file ASCII che contiene direttive e coomenti, specifica inoltre i file delle zone e la loro ubicazione nel filesystem. Apriamo tale file e impostiamo i seguenti valori.

```
options {
      listen-on port 53 { ::1; };
      directory   "/var/named";
      dump-file   "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
      recursion yes;
```

```
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
      type hint;
      file "named.ca";
};

zone "uninf.it" IN {
      type master;
      file "/var/named/uninf.it.hosts";
        allow-query {
                any;
                };
      };

zone "1.168.192.in-addr.arpa" IN {
      type master;
      file "/var/named/1.168.192.in-addr.arpa.hosts";
      allow-query {
                any;
                };
      };
```

Nel campo "*option*" possono essere incluse numerose direttive, nel file precedente sono specificate le seguenti:

- *listen-on*: Con questa opzione si può dire a named su quali indirizzi e porte ascoltare;
- *directory:* Specifica la directory di lavoro di named, di norma si indica la directory in cui si trovano i file di zona;
- *dump-file*: Specifica il percorso del file di dump del server;
- *statistics-file*: Specifica il percorso del file che raccoglie la statistica del server;

- *memstatistics-file*: Specifica il percorso del file che raccoglie la statistica dell'uso di memoria del server;

- *recursive*: Se impostato su yes, specifica che il server cercherà di elaborare una risposta ad una query del client anche se non presente nella sua cache.

Nel campo "*logging*" sono specificate le direttive relative al logging del server, quindi viene abilitato il log per i messaggi della categoria "*default_debug*", e memorizzati nel file "*data/named.run*" e si fa in modo che vengano salvati i messaggi con priorità "*dynamic*".

I tre campi successivi definiscono le *zone*. La prima zona "." specifica che il nameserver utilizza i server del dominio radice per le richieste non presenti in cache. La direttiva "*file*" specifica dove sono contenuti le informazioni relative hai *root nameserver*.

La seconda *zona*, specifica il nome del domini della rete locale "*uninf.it*", e diverse direttivie, come il fatto che la zona è di tipo "*master*", ossia che il server è primario per questa zona, il percorso del file, in cui sono contenute le informazioni relative a tale zona "*/var/named/uninf.it.hosts*" e a chi è concesso effettuare query, nel nostro caso a tutte le macchine della rete LAN locale "*any*".

La terza *zona*, specifica il nome per la risoluzione inversa della rete locale "*1.168.192.in-addr.arpa*", e diverse direttivie, come il fatto che la zona è di tipo master, ossia che il server è primario per questa zona, il percorso del file, in cui sono contenute le informazioni relative a tale zona "*/var/named/1.168.192.in-addr.arpa.hosts*", e a chi è concesso effettuare query, nel nostro caso a tutte le macchine della rete LAN locale "*any*".

Il secondo è un semplice file di testo in cui si specificano le informazioni necessarie per la risoluzione dei nomi di dominio in indirizzi numerici. Tale file è il

più importante in quanto contiene tutti i dati e i record necessari per la configurazione del dominio. Il file in questione è il seguente.

```
[root@fedora8]# nano /var/named/uninf.it.hosts
```

Apriamo tale file e impostiamo i seguenti valori.

```
$ttl 38400
uninf.it.   IN    SOA   fedoracore8. mario\.gabrielli78.gmail.com. (
                  1199559799
                  10800
                  3600
                  604800
                  38400 )
uninf.it.   IN    NS    fedoracore8.
fedoracore8.uninf.it.   IN    A     192.168.1.1
ubuntu7.uninf.it.       IN    A     192.168.1.50
server2003.uninf.it.    IN    A     192.168.1.100
```

Il campo "*$ttl*" indica il default time-to-live. Come si vede si applica globalmente a tutti i record che precedono qualunque altra direttiva di TTL, che può essere indicata anche per singolo host. Il nameserver specifica questo valore in tutte le risposte per la zona o il dato record indicando per quanto tempo gli altri nameservers possono tenerlo in cache.

La righa successiva costituisce la parte principale del file di zona e serve ad indicare lo Start of Authority per la zona "*uninf.it*". In questo caso "*fedora8.*" È il nome del server autoritativo per la zona. Se ne può specificare uno solo e non di più. A seguire abbiamo un record che indica l'indirizzo del responsabile della gestione per la zona. I nameserver non utilizzano mai questa risorsa che è ad uso esclusivo di chi vuole comunicare con il gestore del dominio. Non si specifica l'indirizzo come mario.gabrielli78@gmail.com ma si deve sostituire la @ con il punto.

Invece i campi, successivi, chiusi tra parentesi sono principalmente per gli slave server.

Il primo numero "*1199559799*" indica il numero di serie, ossia la versione relativa alla modifica del file, occorre per far sapere agli slave che sis sono effettuati dei cambiamenti.

Il secondo numero "*10800*" indica agli slave della zona ogni quando devono verificare che i file sul master sono o meno cambiati.

Il terzo numero "*3600*" indica allo slave ogni quanto tempo riprovare a connettersi al master in caso un refresh non sia andato a buon fine.

Il quarto numero "*604800*" indica allo slave dopo quando tempo deve considerare una data zona non più valida. Deve essere necessariamente superiore ai valori di refresh e di expire, altrimenti considererebbe espirati i valori di una zona prima di averla caricata.

L'ultimo valore "*38400*" costituisce il TTL che server ad indicare quando tempo una risposta negativa ad una query va tenuta dal nameserver nella cache.

La riga successiva riporta il nome del nameserver autoritativo per la zona, che nel nostro caso è "*fedora8.*", il flag "*NS*" stà per nameserver.

Le ultime due righe del file, associa i nomi della macchina con i rispettivi indirizzi IP. Il flag "*A*" sta per Address e indica che si tratta di record per la risoluzione da nome a indirizzo.

Abbiamo descritto il file di zona per il dominio *uninf.it*, orariportiamo il corrispettivo file per la risoluzione inversa. Il file è il seguente.

```
[root@fedora8]# nano /var/named/1.168.192.in-addr.arpa.hosts
```

Apriamo il file e inseriamo le seguenti informazioni.

```
$ttl 38400
1.168.192.in-addr.arpa. IN SOA fedoracore8. mario\.gabrielli78.gmail.com.
 (
```

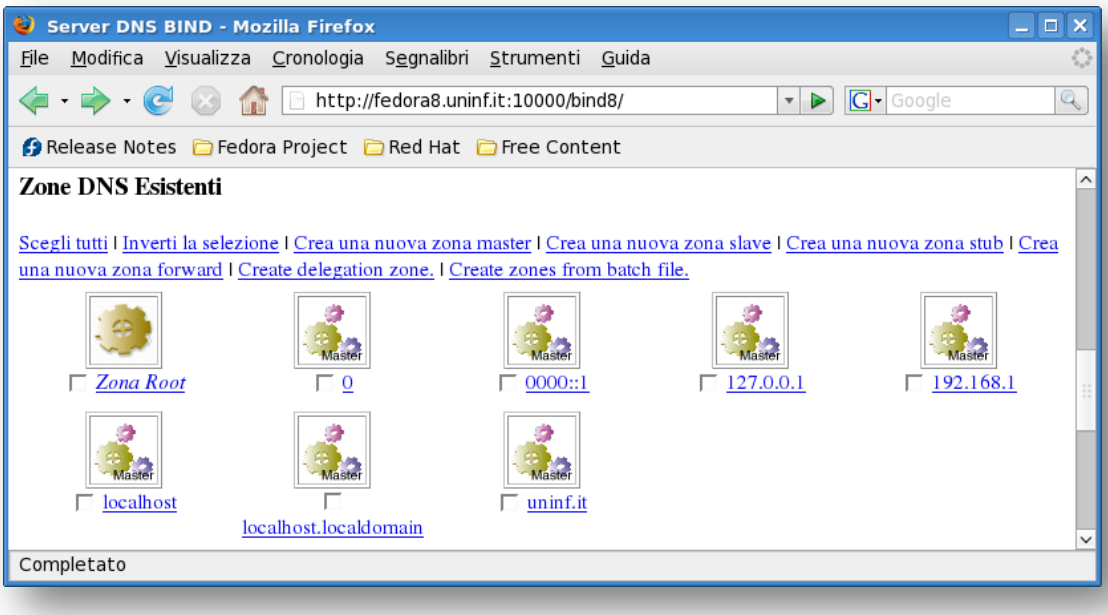
```
                  1199564085
                  10800
                  3600
                  604800
                  38400 )
1.168.192.in-addr.arpa. IN    NS    fedoracore8.
1.1.168.192.in-addr.arpa.     IN    PTR   fedoracore8.uninf.it.
50.1.168.192.in-addr.arpa.    IN    PTR   ubuntu7.uninf.it.
100.1.168.192.in-addr.arpa.   IN    PTR   server2003.uninf.it.
```

Innanzitutto occorre fare una premessa. Come si può vedere, nel file non ci sono riferimenti numerici, bensì si trova delle stringhe come "*1.168.192.in-addr.arpa.*". Se ad esmpio si volesse conoscere il corrispettivo nome DNS a partire dall'indirizzo IP, il nameserver sarebbe costretto a cercare nell'intero albero DNS dal suo dominio di competenza fino alla radice per poi ridiscendere al dominio a cui appartiene l'IP seguendo una ricerca all'interno dei file della zona singolo record per singolo record. Come è facile immaginere quando ci sono numerosi indirizzi numerici o gli amministratori creano molte subnet diverse nelle loro reti delegandole poi ad altri server DNS e visto che tali indirizzi sono sia pubblici che privati, questo lavoro sarebbe impossibile per il DNS. In più il DNS indicizza i suoi dati, inclusi quelli numerici per nome. Per questo visto che è semplice trovre le informazioni quando si fornisce il nome del dominio che mantiene i dati, gli sviluppatori hanno pensato di creare un dominio a se, che tratta gli indirizzi numerici come 'etichette', *in-addr.arpa*. In questo modo il domionio *in-addr.arpa* comprenderà 256 sotto-domini i quali includeranno altri 256 sotto-domini fino all'ultimo campo numerico di un IP che fornirà il nome di dominio completo per un dato host. La sua rappresentazione così diviene invertita, *192.168.1.1* diventa *1.1.168.192.in-addr.arpa.*, questo perché si segue la relazione con il dominio radice ".". In questo modo l'indirizzo IP sarà letto correttamente nel nome di dominio.

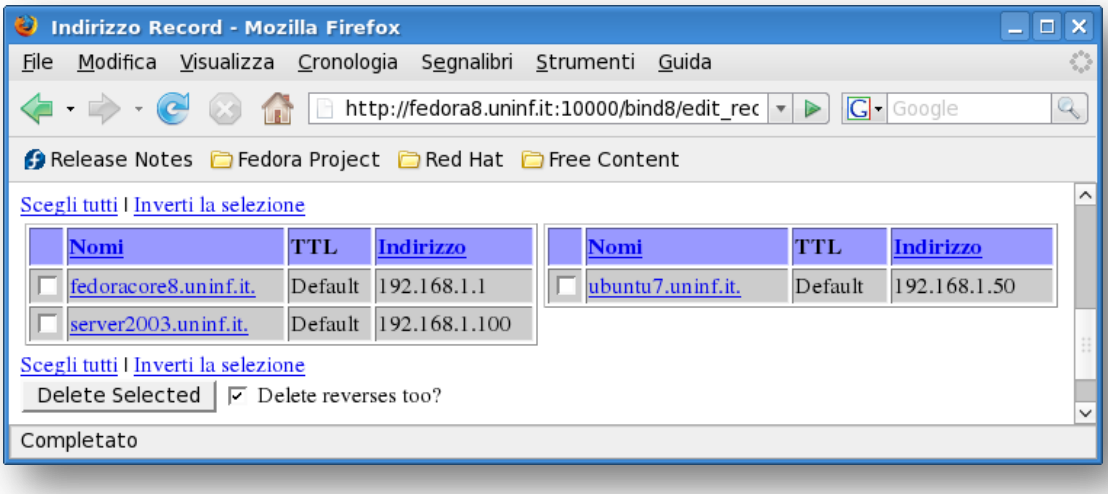
Come risulta evidente la prima parte del file "*1.168.192.in-addr.arpa.hosts*" è simile al contentuto del file "*uninf.it.hosts*" e el informazioni hanno lo stesso significato. Mentre l'ultima parte del file riporta i nomi numerici delle macchine della rete locale e i loro relativi nomi di dominio. Il flag "*PTR*" sta per *Pointer* e

indica che si tratta di record per la risoluzione da indirizzo a nome. La configurazione di tutti i file relativi al server DNS, può essere effettuata ancora più comodamente utilizzando sempre l'interfaccia browser di Webmin.

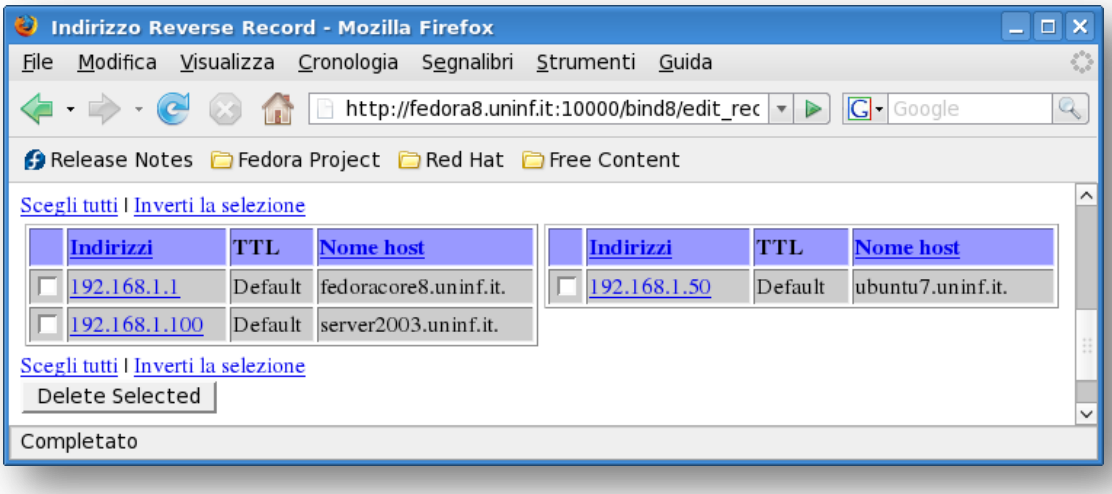
Vediamo un esempio di tutte le *zone* specificate nei file precedenti, presenti nel nostro dominio.



Nell'immagine successiva vengono riportati i dettagli realtivi alla zona "*uninf.it*" relativa al nostro dominio.



L'ultima immagine invece riporta i dettagli relativi alla zona "*1.168.192.in-addr.arpa.hosts*" sempre del nostro dominio.



Arrivati a questo punto, rimane soltanto avviare il servizio *named* e verificare se tutto funziona correttamente. Per avviare il server DNS eseguiamo il seguente script.

```
[root@fedora8]# /etc/init.d/named start
```

Oppure in alternativa

```
[root@fedora8]# /usr/sbin/named
```

Ogni volta che si va ad apportare modifiche hai file di configurazione del server DNS, esso deve essere riavviato per caricare le ultime modifiche apportate.

Per testare il funzionamento del server DNS, utilizziamo il comando *dig* nel seguente modo.

```
[root@fedora8 /]# dig server2003.uninf.it

; <<>> DiG 9.5.0a6 <<>> server2003.uninf.it
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24503
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0
```

```
;; QUESTION SECTION:
;server2003.uninf.it.           IN      A

;; ANSWER SECTION:
server2003.uninf.it.    38400   IN      A       192.168.1.100

;; AUTHORITY SECTION:
uninf.it.               38400   IN      NS      fedora8.

;; Query time: 6 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Wed Jan  9 21:46:42 2008
;; MSG SIZE  rcvd: 7
```

Con il comando precedente si testa se dalla macchina Linux il server Windows è raggiungibile e inoltre ci vengono forniti tutti i parametri relativi.

Mentre il seguente comando eseguito sul prompt dei comandi del server Windows ci garantisce che il server DNS sulla macchina Linux funziona correttamente e che il server Windows la raggiunge.

```
C:\Documents and Settings\Administrator>nslookup fedora8.uninf.it
Server:  fedora8.uninf.it
Address:  192.168.1.1

Nome:    fedora8.uninf.it
Address:  192.168.1.1
```

Tale comandi ci fornisce l'indirizzo IP relativo alla macchina Linux *fedora8.uninf.it* [35] [36] [37].

7.4 Configurare BIND per Supportare Active Directory

Il Server Domain Name System (DNS) fornito con Windows 2003 Server è uno standard IETF basato su server DNS che supporta pienamente Active Directory ed è pienamente interoperabile con altri standard basati su implementazioni di server DNS, che offre eccellenti prestazioni, facilità di installazione e

configurazione, con opzioni grafiche, e script di amministrazione. Per questi motivi, il server DNS di Windows 2003 è raccomandato per supportare le reti di Windows 2003 e Active Directory. Ma in molti ambienti, non è possibile implementare il server DNS della Microsoft in quanto la rete è già provvista di un server DNS come BIND che viene eseguito su un server Linux. Active Directory offre molte caratteristiche per ridurre il sovraccarico amministrativo, e aumentare la sicurezza, per questo motivo molti amministratori di sistema, desiderano implementare Active Directory per usufruire di queste funzionalità. Di seguito quindi viene descritto come configurare Berkeley Internet Name Domain (BIND) server per supportare Active Directory.

7.4.1 Records SRV

Microsoft, da windows 2000 in poi ha fatto dei cambiamenti relativi al metodo di risoluzione dei nomi, tornando praticamente sui suoi passi e abbandonato il metodo WINS in favore del vecchissimo metodo DNS. Come risultato, tutte le macchine da win2k in poi, per accedere alle risorse di rete utilizzano il servizio DNS.

Allo startup i clients Windows 2003 sono programmati per eseguire DDNS, registrando il loro nome e indirizzo IP, sul server DNS, dopo essergli stato assegnato. I servers win2k inoltre si registrano con il DNS, aggiungendo i record SRV che indicano quali servizi sono in esecuzione sul loro sistema. Questo permette ai clients win2k di eseguire un DNS lookup mediante i records SRV alla ricerca del Domain Controller e dei servizi di dominio (winlogin, global catalog).

Le finalità di ciascuno dei campi specialistici utilizzati in un record di risorsa SRV sono i seguenti:

- **service**: Un nome simbolico per il servizio desiderato. Per i servizi noti, è definito un nome simbolico universale riservato, come "_telnet" o "_smtp".

Se un noto nome del servizio non è definito, può essere utilizzato un nome utente locale o preferito, al suo posto. Alcuni servizi utilizzano ampiamente il protocollo TCP/IP, in particolare il POP (Post Office Protocol), non ha un nome simbolico universale unico.

- **protocol**: Indica il tipo di protocollo di trasporto. In genere, questo può essere o TCP o UDP, anche se qualsiasi protocollo di trasporto, può essere utilizzato.

- **name**: Il nome di dominio DNS è riportato da questo record di risorsa. Il record di risorse SRV è l'unico, tra gli altri tipi di record DNS, in quanto non viene utilizzato per eseguire ricerca o query.

- **priority**: Imposta la preferenza per un host specificato nel campo *target*. I clients DNS che interrogano i records di risorsa SRV, tentano di contattare il primo host raggiungibile dal numero di preferenza più basso. Sebbene gli hosts target hanno lo stesso valore di preferenza, essi possono essere processati in ordine casuale. La gamma di preferenza va da 0 a 65535.

- **weight**: Può essere utilizzato in aggiunta alla preferenza per fornire un meccanismo di bilanciamento del carico, in cui sono specificati più server *target* in un campo e tutti sono fissati allo stesso livello di preferenza. Quando si seleziona un server target tra quelli ospitanti con uguale preferenza, questo valore può essere utilizzato per impostare un ulteriore livello di preferenza che può essere utilizzati per determinare l'esatto ordine o bilanciamento, per la selezione degli hosts di destinazione utilizzati in una query SRV di risposta. Quando è utilizzato un valore diverso da zero, vengono provati i servers con uguale preferenza, in proporzione al peso di questo valore. L'intervallo dei valori va da 1 a 65535. Se il bilanciamento del carico non è necessario, occorre inserire,in questo campo, un valore pari a 0 e realizzare un record più facile da leggere.

- **port**: Questa è la porta del server host *target* che fornisce il servizio indicato nel campo *servizio*. La gamma dei numeri di porta va da 0 a 65535, anche se tale numero è spesso assegnato tra i numeri di porta di servizio noti.

- **target**: Specifica il nome di dominio DNS dell'host, che fornisce il tipo di servizio richiesto. Per ogni nome host utilizzato, un corrispondente record di risorse, che è costituito dall'indirizzo host (A), è obbligatorio nello spazio dei nomi DNS. Un unico punto (.) può essere utilizzato, in questo campo, per indicare autorevolmente che il servizio richiesto, specificato nel presente record SRV di risorsa, non è disponibile in questo server DNS.

Per fare in modo che BIND supporti Active Directory, è necessario configurare il file *named.conf* con le informazioni specifiche per Active Directory, creare quindi un file di zona per il dominio, e quindi riavviare il demone *NameD*. I parametri da aggiungere a tale file, di configurazione, sono riportati di seguito.

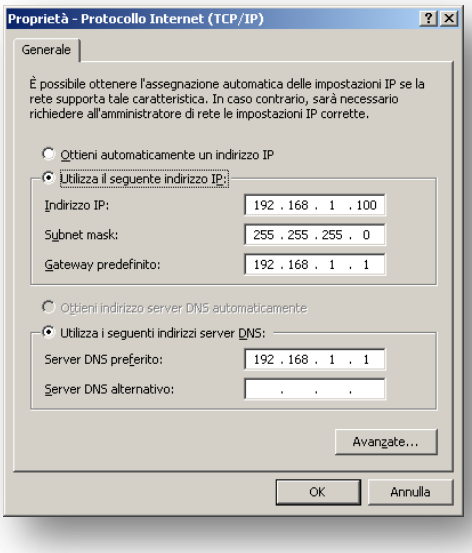
```
zone "uninf.it" IN {
      type master;
      file "/var/named/uninf.it.hosts";
      allow-update {
                192.168.1.100;
                };
      allow-query {
                any;
                };
      };

zone "1.168.192.in-addr.arpa" IN {
      type master;
      file "/var/named/1.168.192.in-addr.arpa.hosts";
      allow-update {
                192.168.1.100;
                };
      allow-query {
                any;
                };
      };
```

Le precedenti righe di configurazione, relative alle zone della nostra LAN privata, devono essere sostituite all'interno del file *named.conf*, per fare in modo

che venga attivato l'aggiornamento dinamico del server DNS. In questo modo Active Directory ha la possibilità di aggiornare automaticamente i record all'interno delle zone memorizzare nel server DNS. Lo specifico comando che assolve a questo compito è "*allow-update*" insieme all'indirizzo IP, relativo al server in cui è in esecuzione Active Directory, come visibile nella configurazione precedente. A questo punto per rendere effettive le modifiche occorre riavviare il demone *named*, come riportato dal seguente comando.

```
[root@fedora8]# /etc/init.d/named start
```

Dopo aver quindi riavviato il demone, siamo pronti a configurare Windows Server 2003, per fare in modo che vada ad interrogare, aggiornare e quindi utilizzare il server DNS BIND. Per prima cosa andiamo ad impostare l'indirizzo IP della macchina in cui è installato il server DNS BIND. Per fare questo clicchiamo con il tasto destro su "*Risorse di rete*" e poi su "*Proprietà*"; a questo punto clicchiamo con il tasto destro sulla connessione di rete attiva e nuovamente su "*Proprietà*", ci viene aperta una nuova finestra in cui andiamo a selezionare "*Protocollo internet (TCP/IP)*" e per per ultimo clicchiamo su "*Proprietà*". Viene aperta la seguente finestra di dialogo, in cui è possibile inserire l'indirizzo IP del server DNS BIND, nel campo "*Server DNS primario*".



Una volta impostato l'indirizzo IP del server DNS e cliccato su "*OK*" per confermare la modifica, si deve forzare la registrazione dei record SRV nel nuovo server DNS. Per fare questo dobbiamo riavviare il servizio "*NETLOGON*". Quindi clicchiamo su "*Start*"→"*Strumenti di amministrazione*" e poi su "*Servizi*", individiamo il servizio "*Accesso rete*" e lo riavviamo cliccando su "*Riavvia*". Il riavvio del servizio richiede di solito meno di un minuto, dopodiché verrà immediatamente aggiornato il database di zona del DNS.

A questo punto occorre eseguire il seguente comando, dal prompt dei comandi, che costringe il server Windows a registrare di nuovo tutti i record DNS con il server DNS BIND.

```
C:\> ipconfig /registerdns
```

Tale comando non registra i record immediatamente, ma può richiedere fino a quindici minuti per completare la registrazione dei record nel database della zona DNS [38] [39].

CAPITOLO 8

AUTENTICAZIONE SICURA CON CENTERIS LIKEWISE

8.1 Likewise Identity

E' sempre più raro trovare reparti IT aziendali che utilizzano un unico Sistema operativo. Le aziende più comunemente adotta un mix di sistemi Microsoft Windows, uno o più distribuzioni di Linux e alcune varianti di UNIX, in base alle applicazioni che utilizzano. Ad esempio i server e-mail possono girare su server Windows, mentre i database possono girare su server UNIX. Apparati di rete e server web possono essere eseguiti su sistemi Linux. Questo utilizzo di più sistemi operativi risultano impiegati in una rete eterogenea ed è spesso accompagnato da eterogenei Identity Management Systems (IMS).

I computer Windows e gli utenti possono essere autenticati tramite Microsoft Active Directory mentre chi ospita UNIX o Linux sono in grado di usare un'autenticazione locale, o il *Network Information System* (NIS) per l'autenticazione.

In un ambiente di rete queste variazioni di IMS non sono desiderabili. Quando gli utenti entrano o lasciare una organizzazione, ogni IMS deve essere aggiornato con le attuali informazioni relative agli utente. Questi risultati in termini di personale e di inefficienza spesso conduce a sistemi che non sono correttamente protetti. Gli amministrari di Azienda IT desideravano, per questo, di una soluzione che permettesse a tutti i sistemi di partecipare ad un comune IMS, che permetta di effettuare tutte manutenzione, su un unico sistema. Centeris Likewise Identity 3.0 offre questa funzionalità e permette a sistemi UNIX e Linux di centralizzare le loro autenticazioni e autorizzazioni usando Microsoft Active Directory.

8.1.1 Sfide per Raggiungere L'interoperabilità

Ci sono tre grandi sfide per il raggiungimento dell'interoperabilità tra UNIX e Linux con Active Directory; tuttavia l'interoperabilità deve essere definita. L'interoperabilità può assumere forme diverse in baseall'organizzazione o alle applicazioni in esecuzione. Alcune organizzazioni hanno bisogno solo di un meccanismo di autenticazione comune. Altre possono richiedere la semplice possibilità di accedere a risorse controllate da Active Directory, utilizzando le loro credenziali. Altre possono voler ottenere un archivio di dati comune per tutti i loro dati di autenticazione e autorizzazione. Altre invece desiderano disporre di tutte le seguenti funzionalità, tra cui un mezzo per applicare e gestire i criteri di gruppo in tutti i loro UNIX e Linux host. Un dominio di Active Directory è, in sostanza, un centro di distribuzione di chiave Kerberos e un database LDAP che memorizza le informazioni utente. Questa combinazione permette la memorizzazione di password e altre informazioni in un posto sicuro in moda che possa essere richiesto tramite richieste di autenticazione LDAP. Questo rende Active Directory uno spazio ideale per unire anche i sistemi UNIX e Linux. La seguente tabella illustra alcuni dei limiti dell'autenticazione e autorizzazione su sistemi UNIX e mostra dove *Linkewise Identity* unisce i sistemi UNIX con Active Directory, per fornire agli amministratori un punto unificato per memorizzare i dati di autenticazione e autorizzazione.

	Password UNIX e Linux	**Active Directory su Windows**	**Active Directory con Likewise Identity**
Tipo di Autenticazione	Più IMS (/etc/password, mappa NIS)	KRB5/LDAP	KRB5/LDAP e mappa degli esistenti UID/GID
Criteri di Gestione dei Gruppi	Componenti separati gestiti da files .conf	Amministrazione integrata delle politiche dei gruppi	Permette l'applicazione della politica sui gruppi sugli hosts UNIX, usando Active Directory
Criteri di Gestione degli Account	Componenti separati gestiti da files .conf	Amministrazione integrata delle politiche degli account	Permette l'applicazione delle politiche sugli account sugli hosts UNIX

8.1.1.1 Associare hosts UNIX/Linux in un dominio Active Directory

La prima sfida di interoperabilità è consentire agli host UNIX e Linux di partecipare in un dominio Active Directory. Questo è affrontato da Likewise Identity tramite gli strumenti di UNIX e Linux che consentono all'host di far parte di un dominio Active Directory e avere anche un account sulla macchina. Una volta che un host UNIX o Linux è unito al dominio, esso sarà in grado di autenticare gli utenti in Active Directory. Partecipare in un dominio Active Directory è il fondamento su cui poggia l'interoperabilità. Con l'adesione dei membri di dominio, sono forniti i prerequisiti necessari per applicare i criteri di gruppo in tutta l'azienda. L'atto di adesione nel dominio di Active Directory fornisce immediatamente il vantaggio di utilizzare un unico set di credenziali di Active Directory, e la capacità di applicare una politica sugli account unificata anche a tutti host UNIX e Linux. Questo, a sua volta, permette agli amministratori di sistema di utilizzare l'infrastrutture di Active Directory per l'uso e la gestione dei loro sistemi non Windows. Questo fornisce anche il beneficio di consolidare tutti gli account utente in Active Directory nonché a fornire a tutti gli utenti un unico nome utente. Likewise convalida i nomi utente e password, allo stesso modo Kerberos (KRB5). Microsoft Active Directory funzioni come un Kerberos Key Distribution Center. L'identità di agente, in esecuzione su UNIX o Linux impiega protocolli di Kerberos per comunicare con Active Directory e convalidare i nomi utente e password. L'operazione di unirsi a un dominio, crea un account per una macchina UNIX, che può essere successivamente utilizzato per effettuare un'autenticazione LDAP a un server Active Directory. Analogamente Likewise Identity include un programma UNIX (*domainjoin-gui* o *domainjoin-cli*), che consente agli utenti del computer di aderire a un dominio Active Directory. Tale strumento permette agli amministratori di includere i loro hosts UNIX e Linux, in un dominio, nel giro di pochi minuti.

8.1.1.2 Utenti di Active Directory e UID/GID di UNIX/Linux

La seconda sfida consiste nel permettere agli utenti in Active Directory di essere in grado di utilizzare le risorse su hosts UNIX o Linux. Gli host UNIX o Linux contengono i propri utenti e le proprie autorizzazioni di gruppi; ci deve essere un metodo per gli account utente di Active Directory di avere delle informazioni su ciò che possibile o meno accedere sui sistemi UNIX o Linux. L'UID o GID dei sistemi UNIX o Linux sono limitati ad un 32-bit di indirizzi e non è possibile espanderlo mentre i SID di Active Directory sono espandibili. La mappatura degli UID/GID sugli SID eseguita da Likewise Identity consente agli amministratori un modo per superare questa limitazione, pur mantenendo la compatibilità con il sistema di base e le applicazioni. Al fine di permettere agli hosts UNIX e Linux l'utilizzo di Active Directory come loro soluzione di gestione delle identità, Likewise Identity deve supportare entrambe le fasi di identificazione (nome utente e password di convalida, nonché la mappatura) e deve fornire un meccanismo per la mappatura degli utenti di Active Directory con i corrispondenti UIDs (Id utente) e GIDs (id di gruppo) degli utenti di UNIX o Linux. Nativamente, UNIX o Linux memorizzano le informazioni relative agli utenti e gruppi in maniera diversa rispetto ad Active Directory. Un meccanismo deve essere implementato per tradurre o mappare gli UID/GID nei corrispondenti oggetti di Active Directory. Likewise Identity fornisce ulteriori oggetti ad Active Directory per consentire agli account utente di Active Directory di memorizzare le informazioni relative agli UID e GID.

8.1.1.3 Associazione degli UID/GID con gli utenti di Active Directory

Ci sono varie strategie che possono essere usate per associare GID e UID con utenti di Active Directory. Un approccio è quello di assegnare dinamicamente questi ID quando gli utenti effettuano il primo accesso in uno specifico computer UNIX e memorizza questi mappaggi negli stessi computers UNIX. Likewise Identity può inoltre utilizzare questo approccio se richiesto dall'utente. Lo

svantaggio di questo approccio è che ogni macchina UNIX ha un unico mappatura tra gli utenti di Active Directory e gli UID e GID. Un approccio alternativo è quello di assegnare UID/GID basato su un numero che corrisponde all'ultimo componente del SID chiamato il RID (identificatore relativo). Questo mappatura assicura che UID/GID sono unici in tutte le macchine, in un unico dominio Active Directory. Likewise Identity mappa gli UID/GID sui RID nella modalità di installazione rapida. Lo svantaggio è che sono garantiti solo all'interno di un singolo dominio. Un altro approccio è quello di memorizzare le informazioni di mappatura in Active Directory. Sotto Molte circostanze, però, Active Directory non fornisce alcun meccanismo per associare un UID e GID con un utente. La classe dell'utente in Active Directory non può contenere le proprietà che sono pensate per questo scopo. Al fine di conservare le informazioni di mappatura degli UID/GID in Active Directory, è necessario apportare modifiche allo schema di Active Directory o memorizzare le informazioni utilizzando i tipi di oggetti già esistenti. Likewise Identity supporta entrambe queste tecniche. Se l'amministratore sceglie di apportare modifiche allo schema di Active Directory, il *Domain Preparation Wizard* nel *Likewise Identity Management Console* modifica lo schema di Active Directory ed eleva il dominio ad un livello di funzionalità uguale a Microsoft Windows Server 2003 R2. Lo "schema R2" comprende le classi oggetto *posixAccount* e *posixGroup* che includono gli attributi (*uidNumber* e *gidNumber*) che possono essere utilizzati per la mappatura degli UID/GID. In aggiunta, lo strumento di gestione del Likewise crea altre classi di oggetti in Active Directory per sostenere la sua mappatura. Se l'amministratore decide di non effettuare modifiche allo schema, lo strumento di amministrazione del Likewise Identity usa i contenitori standard di Active Directory per memorizzare le informazioni di mappatura. Con entrambe le tecniche, lo strumento di gestione dell'Likewise Identity non modifica gli oggetti utente in Active Directory. Invece, in parallelo vengono creati oggetti nella partizione relativa ai dati in Active Directory e utilizza questi oggetti per memorizzare le informazioni di mappatura. Likewise fornisce al *Microsoft Management Console* (MMC), delle estensioni per lo snap-in "*Utenti e*

computer di Active Directory", che permette all'amministratore di specificare l'UID e il GID manualmente o in alternativa, Likewise assegna automaticamente tali valori.

8.1.1.4 Applicazione dei criteri di gruppo

La sfida finale per raggiungere l'interoperabilità tra Active Directory e UNIX o Linux host è l'applicazione dei criteri di gruppo. Gli amministratori hanno necessità di applicare elementi di politica comune in tutti i sistemi collegati in rete. Likewise Identity consente l'applicazione coerente delle politiche di sicurezza e di configurazione per tutti gli hosts UNIX e Linux che hanno aderito al dominio, oltre a fornire oggetti progettati per aiutare la configurazione dei criteri nei sistemi UNIX o Linux. Active Directory dispone di molte impostazioni relative ai criteri di gruppo, ma molti di questi sono rilevanti solo per sistemi basati su Windows. Likewise Identity fornisce le impostazioni relative ai criteri di gruppo in modo che gli amministratori possono gestire la loro politica per gli hosts UNIX e Linux. Likewise Indentity rispetta le politiche relative agli account Windows, permettendo un amministrazione degli hosts UNIX e Linux, utilizzando un schema di gestione centralizzata. Un altro esempio è che gli hosts UNIX o Linux che hanno aderito a un dominio Active Directory sono soggetti alle politiche sugli account, come ad esempio le impostazioni di blocco, il cambiamento di password di cambiamento. Likewise Identity fornire le impostazioni relative, ai criteri di gruppo per gli hosts UNIX e Linux, utilizzando lo stesso meccanismo di Active Directory che utilizza per applicare le politiche ai membri del dominio. Ciò include non solo le politiche relative agli utenti, ma anche per le macchine.

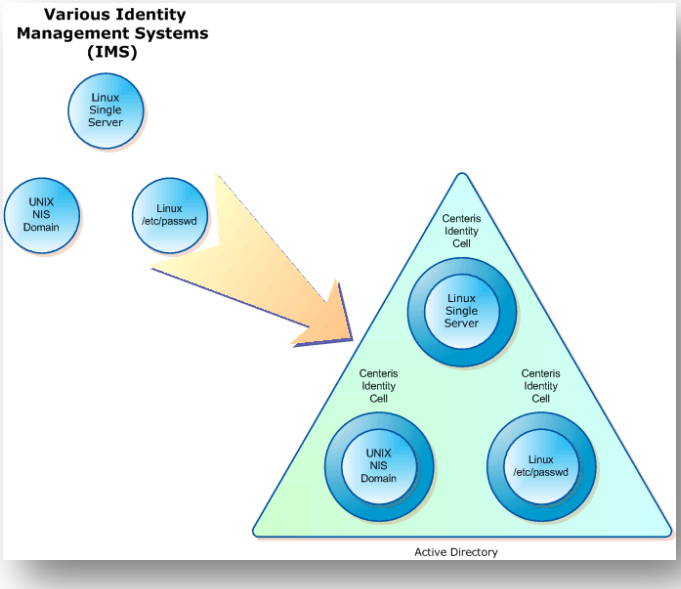
8.2 Organizzazione del Sistema di Likewise Identity

Likewise Identity opera attraverso due principali componenti il database di Active Directory, e l'agente Likewise Identity. Il database di Active Directory

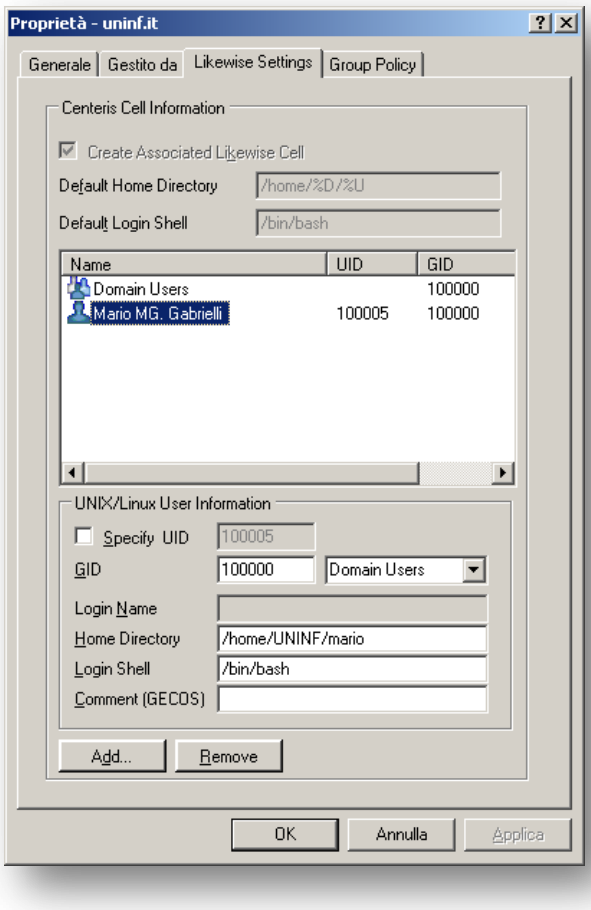
fornisce il punto in cui memorizzare le informazioni di mappatura tra gli UID e GID dei sistemi UNIX e Linux con gli SID di Active Directory. Allo stesso modo l'agente Likewise Identity è provvisto dei necessari servizi per implementare le autenticazioni e le autorizzazioni basate su Active Directory, così come prevede il supporto per la gestione dei criteri di gruppo.

8.2.1 Cellula Likewise e Unità Organizzative

Molte organizzazioni usano Likewise Identity per migrare tutti gli utenti UNIX in Active Directory e assegnare a questi utenti un UID e un GID che è coerente in tutti i computer UNIX che sono entrati a far parte di Active Directory. Questo è l'approccio preferito in quanto semplifica e riduce le questioni amministrative. Una *cellula* Likewise Identity è associata a una *unità organizzativa* (OU) in Active Directory. Le unità organizzative sono utilizzate in Active Directory come un meccanismo per raggruppare oggetti correlati in un contenitore amministrativo comune. Il contenitore OU può quindi essere gestito in maniera coerente. Dato il ruolo che svolgono le unità organizzative di Active Directory, l'associazione delle cellule di autenticazione di Likewise, con le unità organizzative è una scelta naturale.

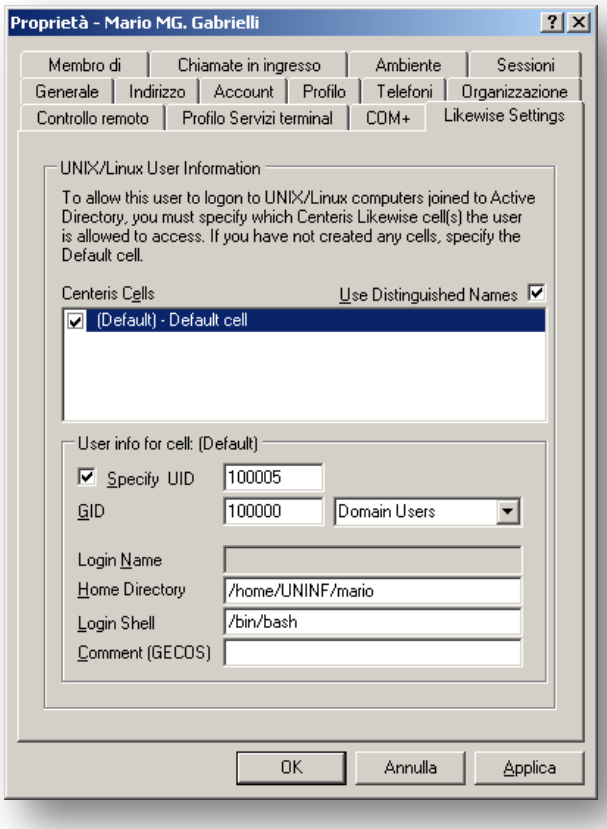


Likewise Centeris modifica lo snap-in "*Utenti e computer di Active Directory*" di Active Directory così l'amministratore può manipolare gli attributi e le informazioni relativea gli UID/GID per gli oggetti, come shell di default e home directory. Queste estensioni permettono anche la creazione e la gestione delle cellule di Centeris Likewise, che sono state descritte precedentemente. Una volta che l'unità organizzativa è stata impostata, l'utente può attivare l'OU di Centeris Likewise Identity come accesso. Questo viene fatto con lo snap-in "*Utenti e computer di Active Directory*" selezionando l'OU e impostando i giusti parametri. Spuntando la casella di controllo "*Create Associated Likewise Cell*" la cellula Likewise viene associata con l'unità organizzativa.



Ora che la cellula esiste, agli utenti possono essere assegnati specifici UID e GID nella cellula, utilizzando lo snap-in "*Utenti e computer di Active Directory*". Quindi si seleziona l'utente e si imposta i giusti paramentri. Questa proprietà

consente agli amministratori di specificare manualmente gli UID e GID oppure far assegnare automaticamente tali valori a Likewise.



Quando Likewise è abilitato un host UNIX si connette ad Active Directory, durante l'accesso dell'utente, esso determina di quale OU è membro. E poi guarda nell'OU per vedere se la cellula Likewise è associato con esso. Se non c'è una cellula associata con l'unità organizzativa, l'agente Centeris Likewise sulla macchina UNIX, se necessario, andrà a guardare l'unità organizzativa padre e nonno, fino a quando non si trova una unità organizzativa che ha una cellula ad esso associata. Infine, se nessuna di tali unità organizzativa viene trovata, il codice UNIX di Likewise, utilizzerà la cellula di default per eseguire la mappatura del nome utente con l'UID/GID. La cellula di default viene utilizzato per eseguire la mappatura per le macchine che non fanno parte di un'unità organizzativa, che ha la propria cellula associata con essa. Tutti gli utenti e le macchine che non sono contenute in una specifica cellula vengono automaticamente a far parte della

cellula di default. La cellula di default abbraccia anche la foresta di Active Directory, consentendo agli utenti di portare avanti la loro mappatura degli UID/GID del proprio dominio, quando si effettua l'accesso a risorse di un altro dominio. Ciò è facilitato dal partizionamento automatico degli UID/GID per diversi domini da parte di Likewise Identity (ad ogni dominio viene assegnato un unica gamma di valori UID/GID, al fine di grantire che non si verifichino dei conflitti di mappatura).

8.2.2 Modalità di Funzionamento del Likewise Identity

Le seguenti descrizioni spiegano le possibilità, che l'amministratore ha, di scegliere quale meccanismo usare per memorizzare le informazioni relative agli UID e GID relativi hai sistemi UNIX/Linux.

8.2.2.1 Centeris Quick-Install Mode

Questo modo di funzionamento non modificare i dati di Active Directory, ed è la modalità di base del funzionamento di Likewise Identity. In questa modalità, gli hosts UNIX e Linux vengono uniti al dominio. Non sono necessarie delle installazioni in Active Directory. L'unico cambiamento è che gli accounts per i computer UNIX/Linux sono aggiunti in Active Directory. Gli utenti di UNIX e Linux saranno in grado di usare le credenziali di Active Directory per il dominio a cui l'hosts fa parte. Questi utenti ottengono anche i benefici relativi alla politica di account di Active Directory, tuttavia le mappature personalizzate degli UID/GID non sono disponibili in questa modalità di funzionamento e UID/GID vengono mappati sui RID. Questa modalità di funzionamento è più adatta, per implementazioni di un singolo dominio.

8.2.2.2 Centeris Identity Active Directory Schema Mode

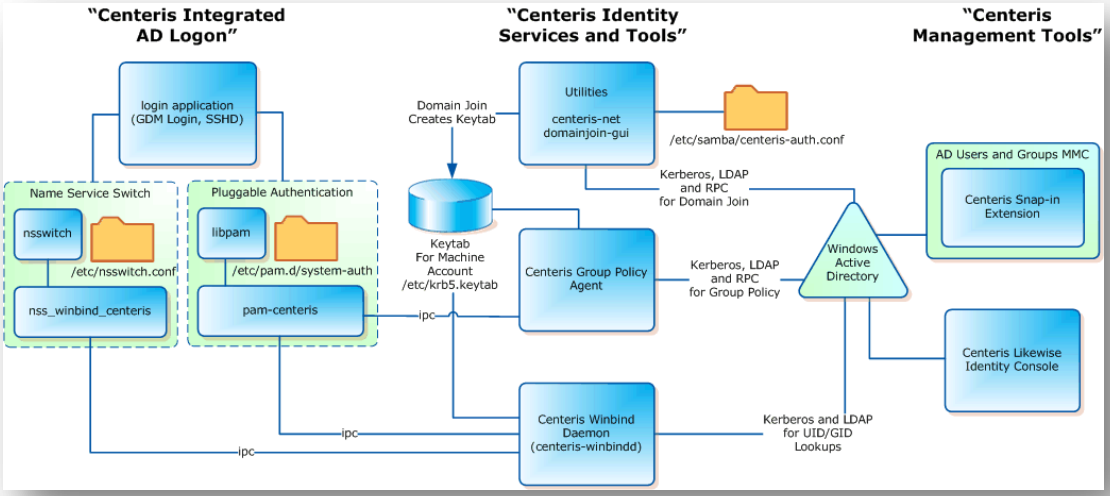
In questa modalità di funzionamento, Likewise Identity utilizza le classi oggetto *posixAccount* e *posixGroup* di Active Directory che includono gli attributi (*uidNumber* e *gidNumber*). Questa modalità eleva il livello del controller di dominio Active Directory e include funzionalità equivalenti a Windows 2003 R2. Questo modo di funzionamento utilizza appieno l'organizzazione delle cellule. E' particolarmente utile perché i dati come il prossimo UID/GID disponibile è memorizzato e assegnato automaticamente, e permette di partizionamento automatico la gamma degli UID/GID per diversi domini, per evitare conflitti di mappatura. Questa modalità è indicata per gli scenari di distribuzione in cui le attuali informazioni relative agli UID e GID è in fase di migrazione in Active Directory e nei casi in cui vi sono più domini che gli utenti UNIX e Linux, dovranno accedere.

8.2.2.3 Centeris Identity Active Directory Non-Schema Mode

Questo modo di funzionamento non modifica lo schema di Active Directory, ma invece mappa le informazioni degli UID/GID sui SID e vengono memorizzati utilizzando gli oggetti contenitori standard di Active Directory. Per questo motivo, questo è un metodo a basso impatto di distribuzione in quanto non è necessario che lo schema di Active Directory venga aggiornato. È funzionalmente equivalenti allo Schema Mode. Gli utenti in questo modo ottengono i benefici relativi all'adesione a un dominio Active Directory, come l'applicazione dei criteri di gruppo e la capacità di usare le credenziali di Active Directory. Questa modalità non prevede i metodi avanzati di ricerca, che la modalità schema prevede, in tal modo le prestazioni possono essere influenzate, quando ci sono un gran numero di oggetti in uso.

8.3 Componenti del Nucleo di Centeris Identity

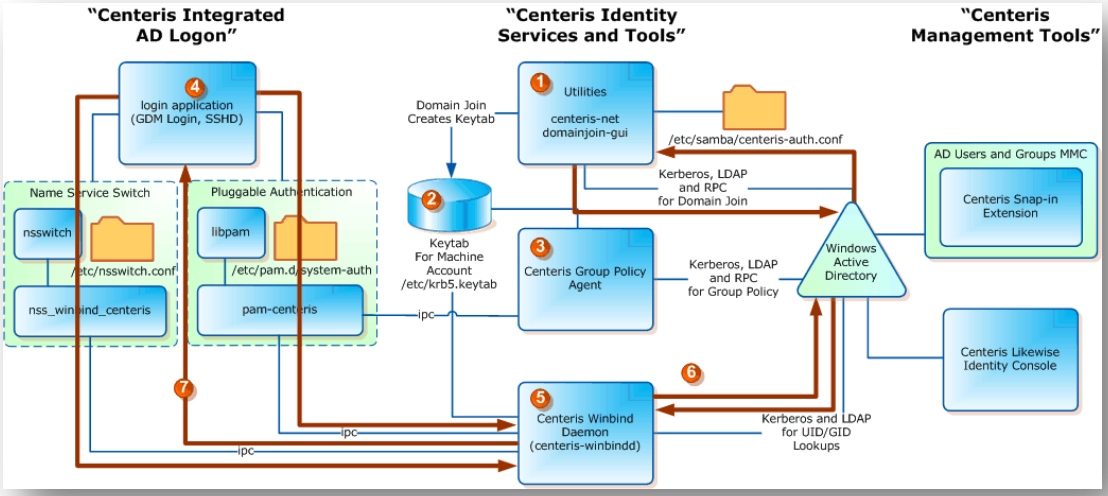
L'agente Centeris Identity agisce come un completo client, Kerberos v5 (KRB5) per l'autenticazione, e come un client LDAP per le funzioni di autorizzazioni. Questa sezione evidenzia i componenti del nucleo che comprende l'agente Centeris Identity, e fornisce informazioni sul loro funzionamento.



La tabella sottostante riporta i componenti di Centeris Identity.

Componente	Descrizione del Componente
Centeris Utilities	Comunica con Active Directory di Windows utilizzando Kerberos, LDAP, RPC e CIFS per completare il processo di adesione al dominio utilizzando le credenziali fornite dall'amministratore. **domainjoin** ottiene la chiave segreta del servizio e la chiave dell'account dalla macchina, dal server Windows in cui è in esecuzione Active Directory e lì scrive in una tabella delle chiavi situata nel file */etc/krb5.keytab*. Il servizio della chiave è utilizzato per autenticare le connessioni ssh in entrata e la chiave dell'account della macchina è usato per autenticare in senso contrario.
Centeris Winbind Daemon	Centeris Winbind è il componente di Centeris Identity, che consente l'integrazione tra gli hosts UNIX e Linux e Active Directory utilizzando una procedura unificata di accesso. Questo componente è il modulo principale, in cui

	pasa il traffico di autenticazione e autorizzazione tra UNIX e Active Directory. Questa implementazione utilizza una combinazione di chiamate CIFS e LDAP, e di risposte pam_centeris e libnss_centeris richieste per consentire agli utenti di un dominio Active Directory di utilizzare le proprie credenziali su un host UNIX o Linux e apparire come utenti nativi su tali sistemi. Questo componente elimina anche la necessità di immettere le proprietà per un account amonimo o pubblico, come in alcune soluzioni UNIX o Linux basate su LDAP.
pam_centeris	Questo è il *Pluggable Authentication Module* (PAM), che è responsabile per le macchine basate su KRB5 e per l'autenticazione dell'utente nell'host. Questo modulo testa i tentativi di accesso dell'utente di Active Directory (via centeris_winbind). Questo modulo utilizza le modifiche della configurazione PAM apportate nel dominio, dal processo di adesione (come in /etc/pam.d/system-auth)
libnss_centeris	Per sostenere la seconda fase dell'identificazione di mappatura UNIX, Centeris Likewise Identity utilizza nuovamente l'account della macchina. L'autenticazionedi Likewise è provvisto di un modulo *nsswitch* (**nss_winbind_centeris**), che viene invocato dal sistema operativo ogni volta che la mappatura nome-to-ID o ID-to-name è necessaria (ad esempio, utilizzando il comando UNIX **getent**). Questo modulo da l'accesso all'account della macchina e esegue la necessaria autenticazione di Active Directory per realizzare le queries di richiesta di mappatura.
Group Policy Agent	Questo componente consente l'amministrazione centralizzata degli hosts UNIX o Linux utilizzando oggetti di politiche di gruppo. I criteri di gruppo sono letti non solo per l'accesso degli utenti, ma per gli accounts delle macchine UNIX o Linux creati in Active Directory. Questo componente verifica l'aggiornamento dei criteri di gruppo ogni 30 minuti, tuttavia questa impostazione può essere modificata da un amministratore.



Ci sono due importanti processi funzionali che avvengono e che illustrano i percorsi di comunicazione tra i componenti in Likewise Identity. Il processo di adesione al dominio avviene una volta per stabilire l'adesione del computer in Active Directory e configurare localmente il computer per l'utilizzo di credenziali che risultano. Il processo di autenticazione e autorizzazione avviene ogni volta che un utente accede al computer con le credenziali del dominio.

Processo di adesione di un macchina UNIX o Linux, in un dominio

1. Il processo di adesione a un dominio inizia con il contattare Active Directory usando Kerberos, LDAP e RPC utilizzando le credenziali di amministratore di dominio. Le informazioni Hostname sono aggiornate tramite l'aggiornamento dinamico DNS;

2. L'adesione al dominio estrae la chiave dell'account della macchina da Active Directory KDC e la memorizza in /etc/krb5.keytab;

3. I dati delle politiche di gruppo viengono letti da Active Directory dopo l'adesione al dominio e la sua implementazione.

Processo di adesione di un macchina UNIX o Linux, in un dominio

4. L'applicazione di login (come /bin/login o gdmlogin/gdmgreeter) interroga i moduli standard pam_centeris e nss_winbind_centeris di sistemi UNIX o Linux;

5. Questi moduli chiamano centeris_winbind e richiedono l'autenticazione e l'autorizzazione da Active Directory;

6. Active Directory poi ritorna un ticket Kerberos (TGT) per l'utente, così come lo fornisce l'agente di Centeris Identity con alcuni oggetti assegnati ai criteri di gruppo per l'utente e/o gruppo;

7. Il successo o il fallimento del login è restituito all'applicazione di login.

8.3.1 Agente Likewise Identity per i Criteri di Gruppo

L'agente per i criteri di gruppo, viene eseguito continuamente come un demone e agisce per far rispettare i criteri di gruppo di Active Directory e per registrare le modifiche ai criteri di gruppo che sono configurati per il dominio o unità organizzativa, al quale il computer è membro. I criteri di gruppo dell'agente utilizza le credenziali, dell'account del computer, in modo sicuro per recuperare il file contenete le informazioni relative alle criteri di gruppo, nel dominio.

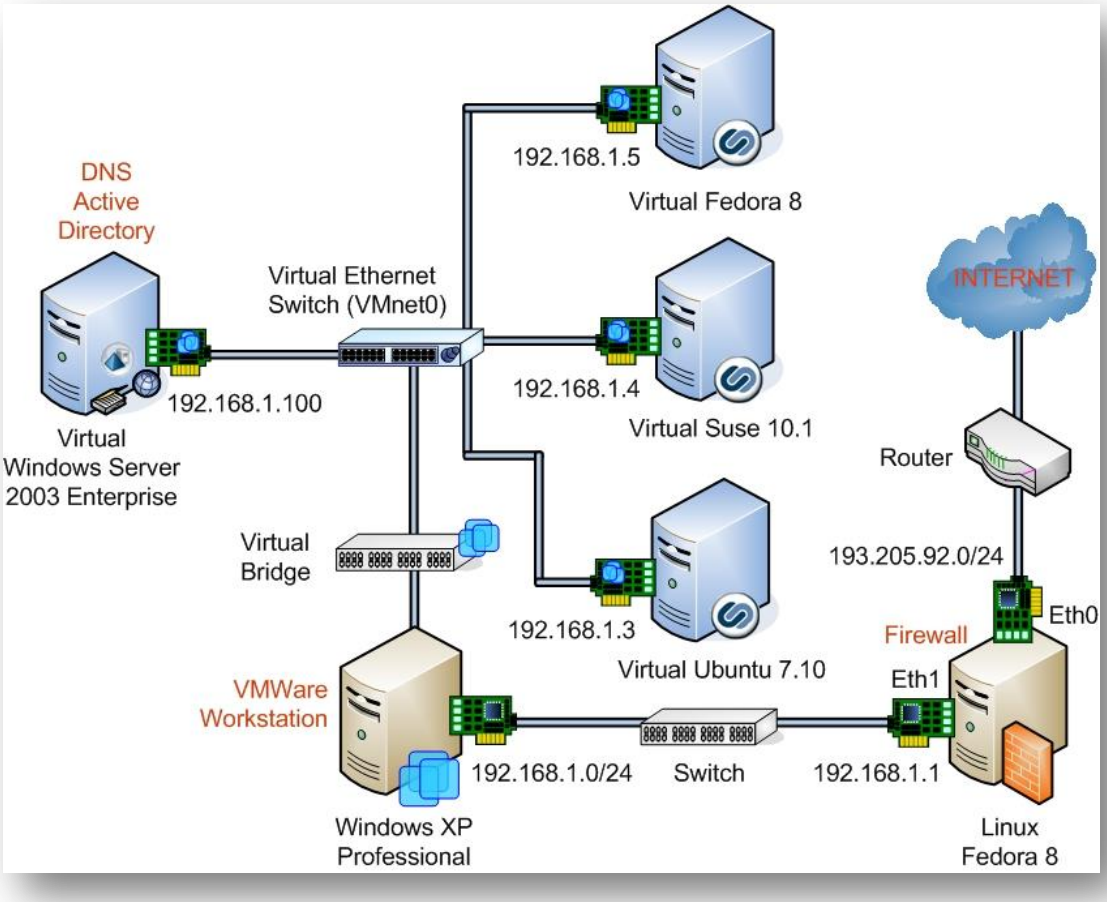
Un importante vantaggio fornito da con Centeris Likewise Identity è che offre oggetti per i criteri di gruppo (GPO) per le funzioni standard per i sistemi UNIX / Linux. Allo stesso modo gli oggetti GPO di Centeris Likewise Identity consentono ai dati di configurazione di essere spediti a più hosts UNIX/Linux. Un esempio fornito da Centeris Likewise Identity è un oggetto per i criteri di gruppo chiamato "sudoers". Tale oggetto GPO consente all'amministratore di prendere un unico file sudoers utilizzato per la gestione, che riceve l'accesso a livello di root sui propri hosts UNIX e Linux. Inoltre, l'amministratore può specificare le credenziali in stile Windows, in sudoers, come mostrato di seguito.

```
DOMAIN\\username ALL=(ALL) ALL
```

Consultare la pagina man per sudoers informazioni specifiche sulla sintassi di sudoer voci dei file. La combinazione di sudo, criteri di gruppo UNIX/Linux e Active Directory è in grado di produrre un potente sistema per la verifica e il controllo di accesso alle risosre UNIX/Linux.

8.4 Installazione di Likewise Identity Agent

Vediamo innanzitutto, nella seguente immagine, come è organizzata organizziamo la struttura di rete all'interno della rete LAN, e i sistemi operativi installati.



Come risulta evidente dall'immagine precedente il sistema di rete che andremo a configurare, ha in più rispetto alla configurazione precedentemente analizzata, soltanto l'istallazione e la configurazione di tre macchine virtuali contenenti i sistemi operativi Linux: Fedora Core 8, Suse 10.1 e Ubuntu 7.10 e l'installazione delle utility di centeris per l'integrazione delle macchine Linux in un dominio di Active Directory.

L'agente Likewise Identity e gli strumenti che lo accompagnano sono contenuti in un unico file autoestraente. Rendere i sistemi UNIX e Linux in grado di funzionare in un dominio di Active Directory è un processo semplice, costituito da due operazioni.

1. *Installazione dell'agente likewisr indentity*: L'installazione dell'agente può essere eseguito da riga di comando. Questo tool standard di gestione dei pacchetti installa l'agente e gli strumenti sul sistema UNIX o Linux da aggiungere al dominio di Active Directory;

2. *Adesione al dominio di Active Directory*: Un strumento grafico viene fornito per far aderire il sistema al dominio di Active Directory, o in alternativa può essere usato un comando equivalente da shell.

8.4.1 Passi per l'installazione

Per l'installazione dell'agente likewise identity occorre scaricare ed eseguire l'appropriato file binario di installazione, sul sistema UNIX o Linux che occorre aggiungere al dominio di Active Directory.

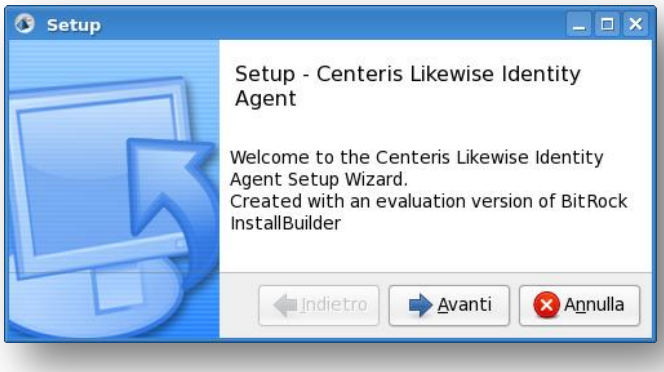
1. Occorre scaricare l'opportuno pacchetto di installazione dal sito http://centeris.com per il sistema Unix o Linux da includere nel dominio, utilizzando l'account *root*. Poi modifichiamo i permessi di esecuzione per il file scaricato, utilizzando il seguente comando da shell.

```
[root@fedora8 mario]# chmod go+x lwidentity-3.5.0.1225-linux-rpm-i386-
                      rpm.installer
```

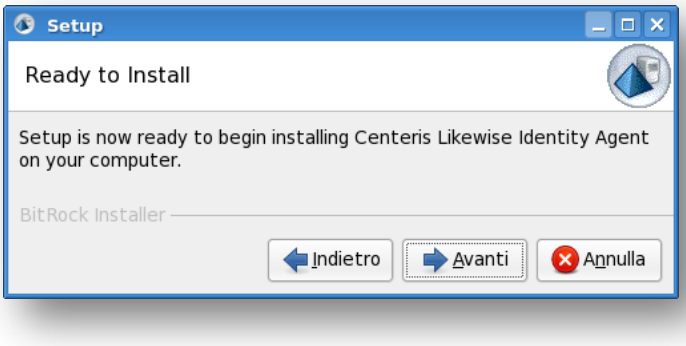
Quindi lanciamo la procedura di installazione con un doppio clic sull'icona per l'installazione o dalla linea di comando come segue.

```
[root@fedora8 mario]# ./lwidentity-3.5.0.1225-linux-rpm-i386-
                      rpm.installer
```

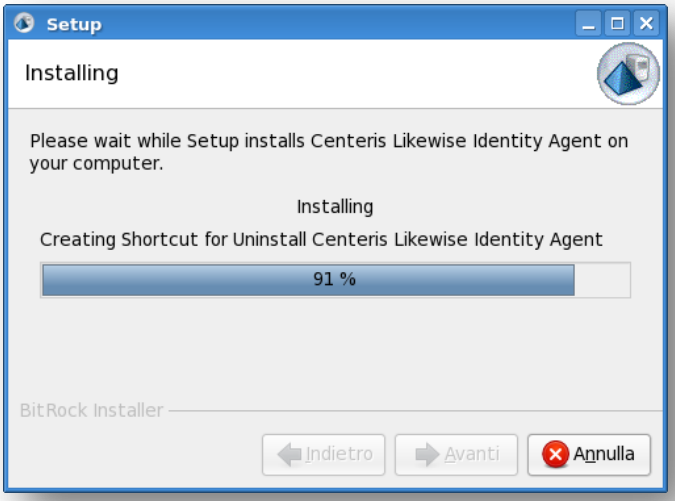
Viene mostrata la seguente finestra in cui clicchiamo su "*Avanti*".



Nella finesta successiva confermiamo i termini di licensa e quindi clicchiamo su "*Avanti*". Ci viene mostrata la seguente finestra in cui clicchiamo nuovamente su "*Avanti*" per installare l'agente sul sistema Linux.



Quindi lo stato dell'installazione viene visualizzato come visibile nell'immagine successiva.



Una volta terminato il processo di installazione viene visualizzata l'ultima schermata in cui dobbiamo cliccare su "*Fine*" per uscire dal programma di installazione. Arrivati a questo punto l'agente likewise Identity è stato installato correttamente sulla macchina Linux. Ora occorre aggiungere tale macchina al dominio di Active Directory.

8.5 Associare un Sistema UNIX/Linux a Active Directory

L'utility per l'adesione di un sistema UNIX/Linux in un dominio di Active Directory, è provvista di una comoda interfaccia grafica, compatibile con l'ambiente GTK. Per procedere all'adesione, per prima clicchiamo due volte sul "*Likewise Identity Domain*" oppure, in alternativa, da shell eseguiamo il seguente comando.

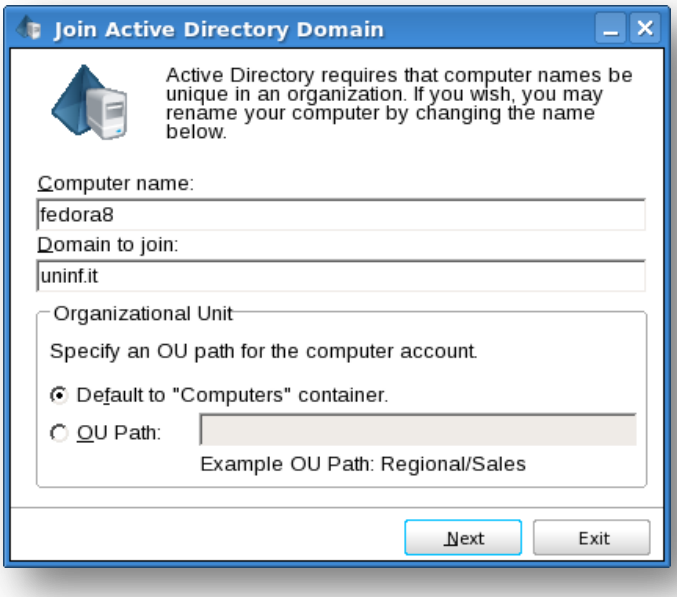
```
[root@fedora8 mario]# /usr/centeris/bin/domainjoin-gui
```

O in alternativa per i sistemi non forniti dell'ambiente GTK eseguiamo il seguente comando:

```
[root@fedora8 mario]# /usr/centeris/bin/domainjoin-cli
```

Ci viene mostrata la seguente finestra di dialogo, in cui clicchiamo su "*Next*" per proseguire.

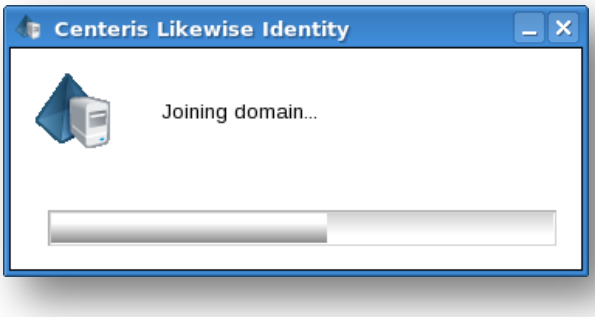
Nella successiva immagine, invece inseriamo le informazioni relative al nome del computer UNIX/Linux da associare a Active Directory nel campo "*Computer name:*", mentre nel campo "*Domain to join:*" inseriamo il nome del dominio, in cui è in esecuzione Active Directory. Per quanto riguarda invece il campo "*Organizational Unit*", lasciamo le impostazioni di default.



Una volta inseriti i giusti valori clicchiamo su "*Next*" e ci viene richiesto di

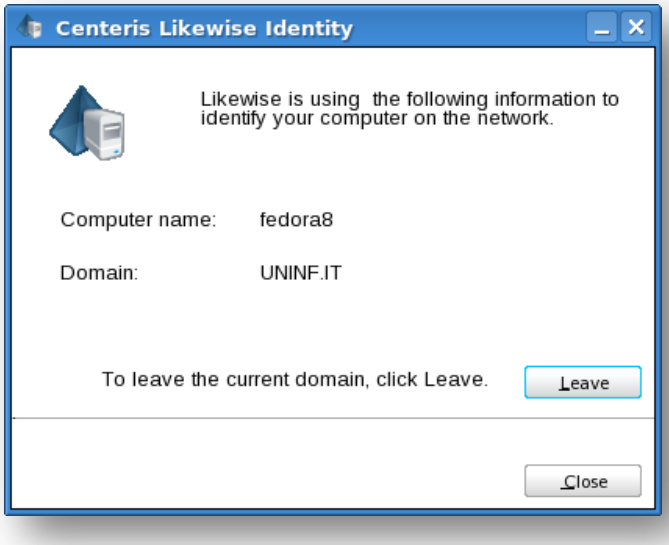
inserire le credenziali dell'amministratore del server in cui è in esecuzione Active Directory, come visibile nell'immagine successiva.

Una volta inserite le credenziali clicchiamo su "*Ok*" per confermarle, e quindi procedere con la creazione dell'associazione del computer nel dominio di Active Directory.

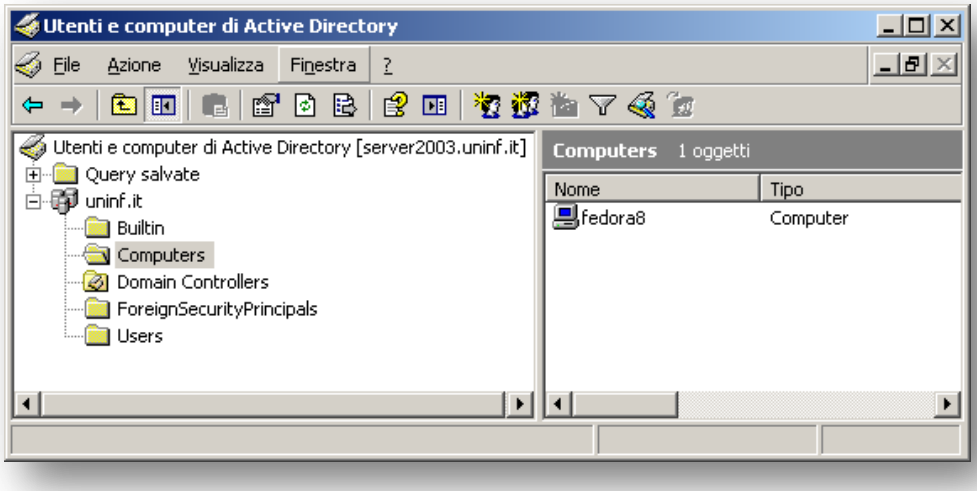


Appena conclusa la procedura di associazione ci viene mostrata la seguente schermata in cui è riportato l'esito dell'associazione.

Quindi cliccando su "*Close*" ci viene mostrata la seguente finestra in cui vengono riassunte le informazione relative al computer aggiunto al dominio Windows, ed in più ci vine fornito un tasto "*Leave*" con il quale è possibile rimuovere tale computer dal dominio di Active Directory. Clicchiamo su "*Close*" per termiare la procedura.

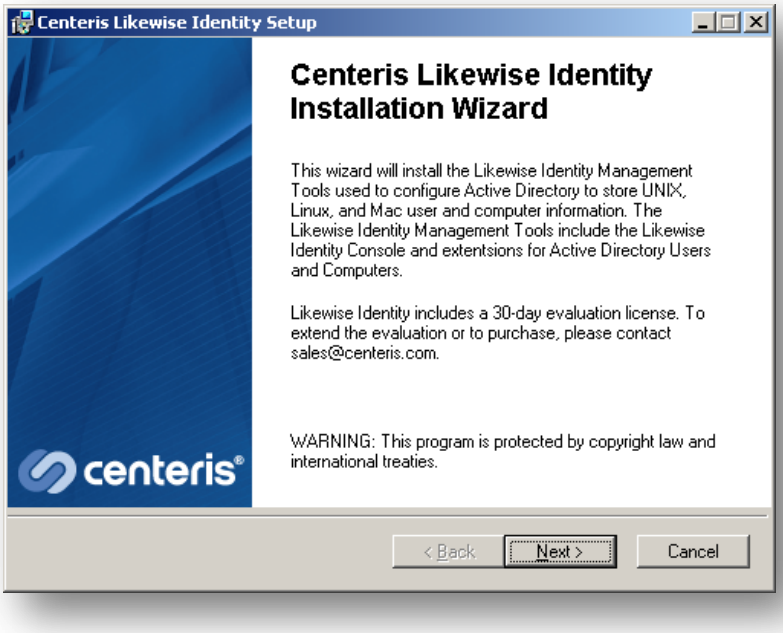


Vediamo l'inclusione di tale macchina al dominio di Active Directory, anche nella finestra Utenti e computer di Active Directory.

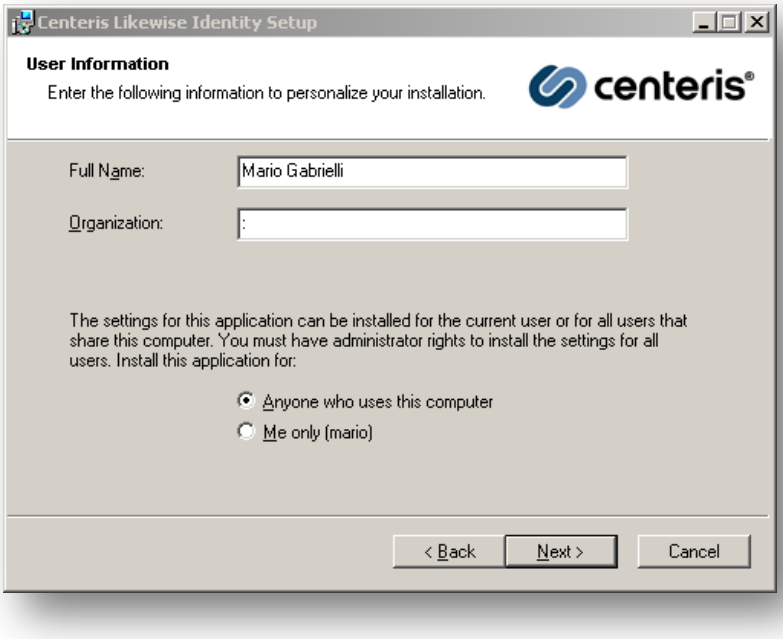


8.6 Installazione di Likewise Identity Management Tools

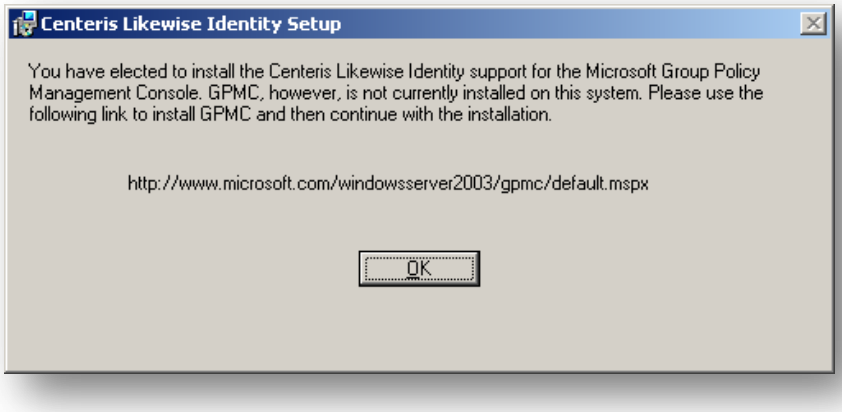
Centeris Likewise Identity Management Tools permette l'amministrazione del dominio, consentendo di gestire le migrazioni da altri sistemi di autenticazione e autorizzazione, come ad esempio NIS o LDAP; inoltre fornisce avanzati strumenti di diagnostica e di riparazione per il mantenimento della salute dello schema di Active Directory, e fornisce dettagliati strumenti per la gestione delle licenze dello stesso prodotto. Likewise Identity Management Tools può anche essere gestito da remoto dagli amministratori. E' possibile accedere alle impostazioni di Centeris Likewise, alla cellula, e alla configurazione dell'utente, tramite le estensioni MMC 3.0 dello snap-in, Utenti e computer di Active Directory. Nelle procedure riportate di seguito sono illustrati i passaggi necessari per ottenere e installare Likewise Identity Management Tools. Per prima cosa scarichiamo il Likewise Identity Management Tools dal sito http://www.centeris.com il file relativo è `CenterisLikewiseIdentity-3.5.1225.exe`, poi lo installiamo sulla macchina in cui è in esecuzione Active Directory, cliccando sul pacchetto eseguibile scaricato. Quindi l'istallazione inizia visualizzando la seguente schermata.



Per procedere clicchiamo su "*Next* >", ci viene richiesto di confermare i termini di licenza, dopo di che procediamo cliccando sempre su "*Next* >" e ci viene mostrata la seguente immagine, in cui inseriamo i nostri dati, per personalizzare l'installazionie e selezioniamo se vogliamo rendere disponibile tale applicazione a tutti gli utenti del computer, oppure soltanto all'utente corrente.



Una volta inseriti tutte le informazioni clicchiamo su "*Next* >" per continuare. Quindi, nella schermata successiva ci viene chiesto di specificare la cartella in cui verrà installato l'applicativo, lasciamo l'impostazione di default, e la confermiamo cliccando ancora su "*Next* >". Nella successiva schermata invece selezioniamo i componenti che vigliamo installare, l'asciamo le impostazioni di default, per installare tutti i componenti e confermiamo la scelta cliccando su "*Next* >". Arrivati a questo punto, nella successiva scermata, cliccando su "*Next* >" per proseguire nell'istallazione, ci viene aperta la seguente finestra che ci avverte della mancanza del programma *Microsoft Group Policy Management Console*, che occorre scaricare, dal sito della Microsoft, e installare sulla macchina prima di continuare con l'installazione.

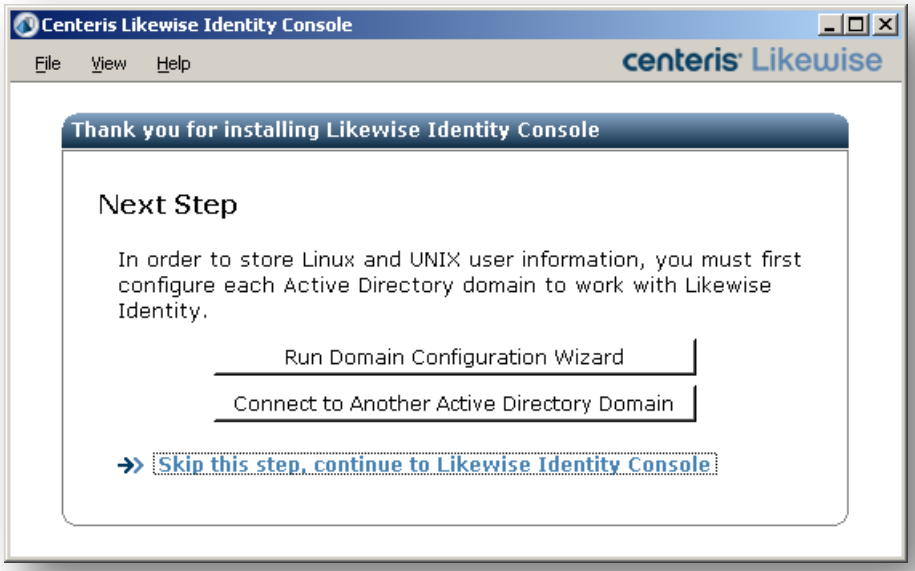


Quindi scarichiamo il file `gpmc.msi` e lo installiamo. A questo punto, per proseguire con l'installazione cliccando su "*Next* >". Alla successiva schermata, ci viene chiesto se vogliamo creare un collegamento sul desktop per eseguire l'applicativo, clicchiamo su "*Next* >" per confermare la scelta di default. Viene installato l'applicativo sulla macchina e una volta conclusa la procedura ci viene mostrata l'ultima schermata, prima della fine dell'installazione, in cui ci viene chiesto se vogliamo leggere il file relativo alle note di rilascio e lanciare l'applicativo dopo l'installazione. Quindi clicchiamo su "*Finish*", per confermare le scelte di default e terminare l'installazione.

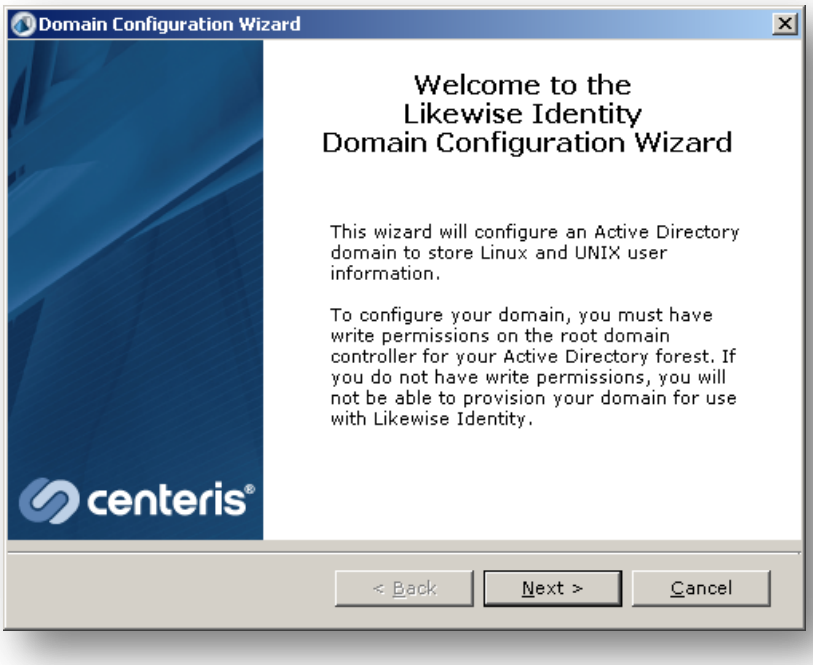
8.7 Prepare il Dominio di Active Directory

Per poter eseguire la console clicchiamo sull'icona presente sul desktop di nome "*Centeri Likewise Identity*".

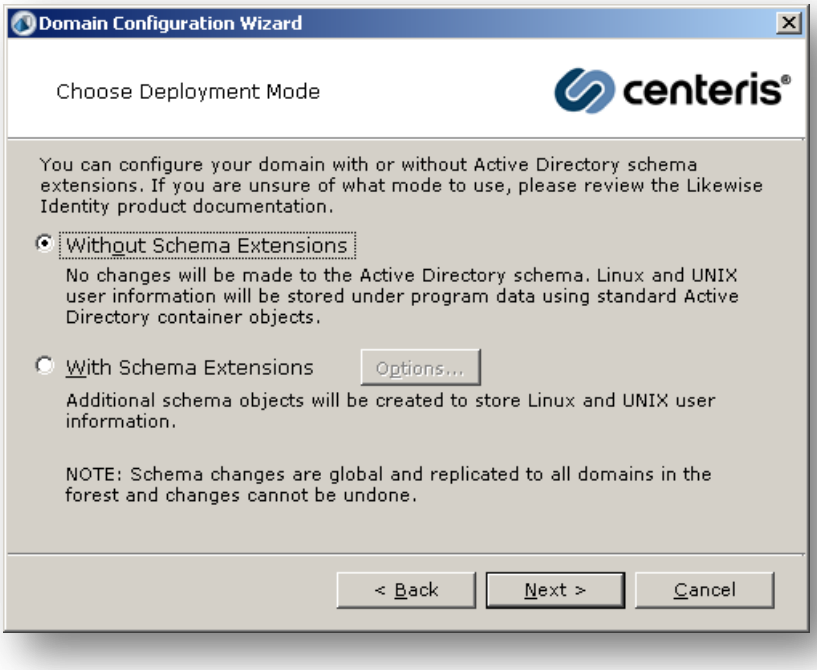
Con la prima esecuzione di Likewise Identity Console, selezioniamo "*Run Domain Configuration Wizard*" per preparare il dominio corrente, come visibile nell'immagine seguente.



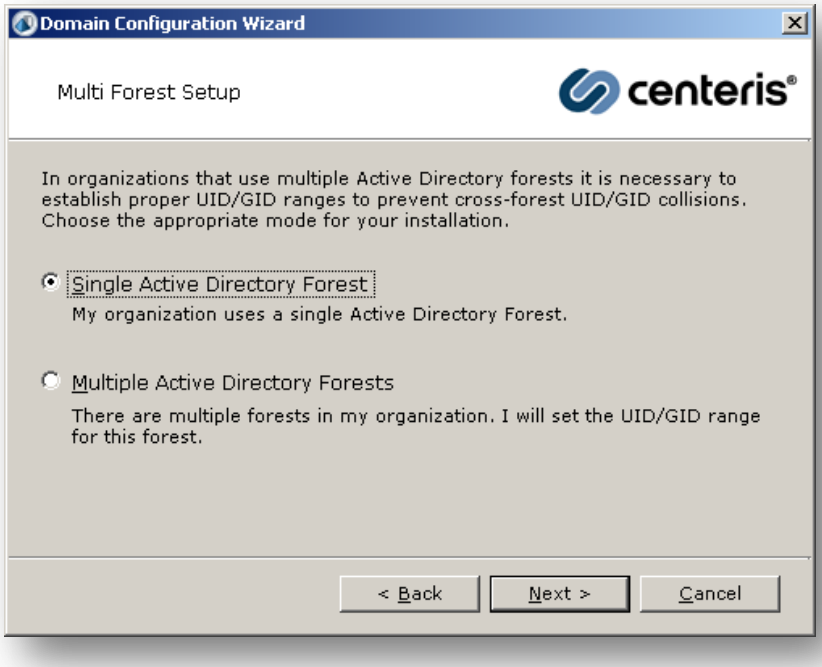
Ci viene aperta la seguente schermata in cui clicchiamo su "*Next* >" per continuare con la configurazione.



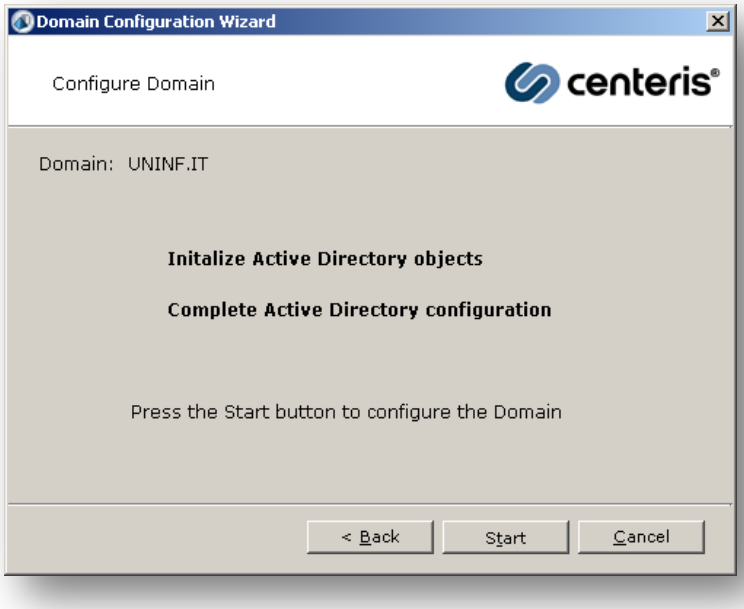
La successiva finestra di dialogo ci fa scegliere che tipo di configurazione vogliamo scegliere per quanto riguarda l'installazione, ho meno, delle estensione per lo schema di Active Directory.



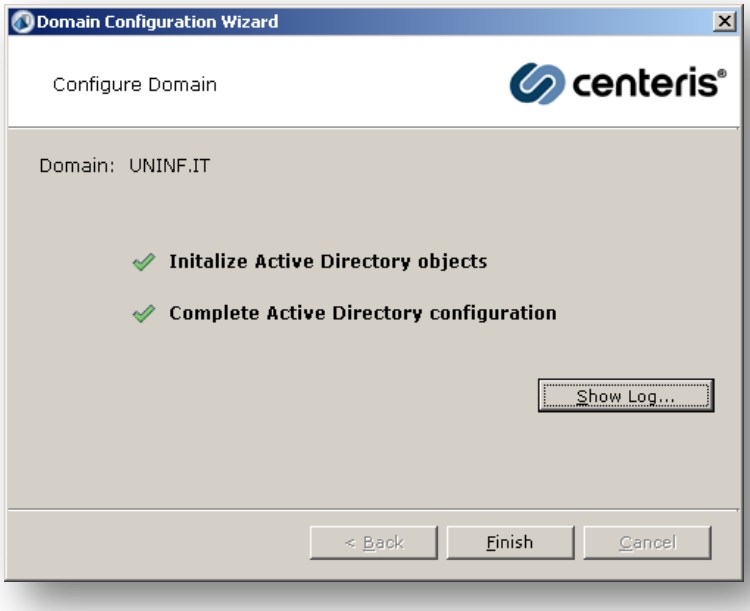
Lasciamo l'impostazione di default visibile nell'immagine precedente e quindi clicchiamo su "*Next* >" per continuare. La successiva schermata, che ci viene mostrata, ci fa scegliere se creare una singola foresta in Active Directory oppure una foresta multipla.



Lasciamo l'impostazione di default, quindi creiamo una singloa foresta in Active Directory e clicchiamo come al solito su "*Next* >" per confermare e andare avanti. A questo punto compare la seguente finestra di dialogo in cui clicchiamo su "*Start*" per confermare le azioni visibili nella finestra.



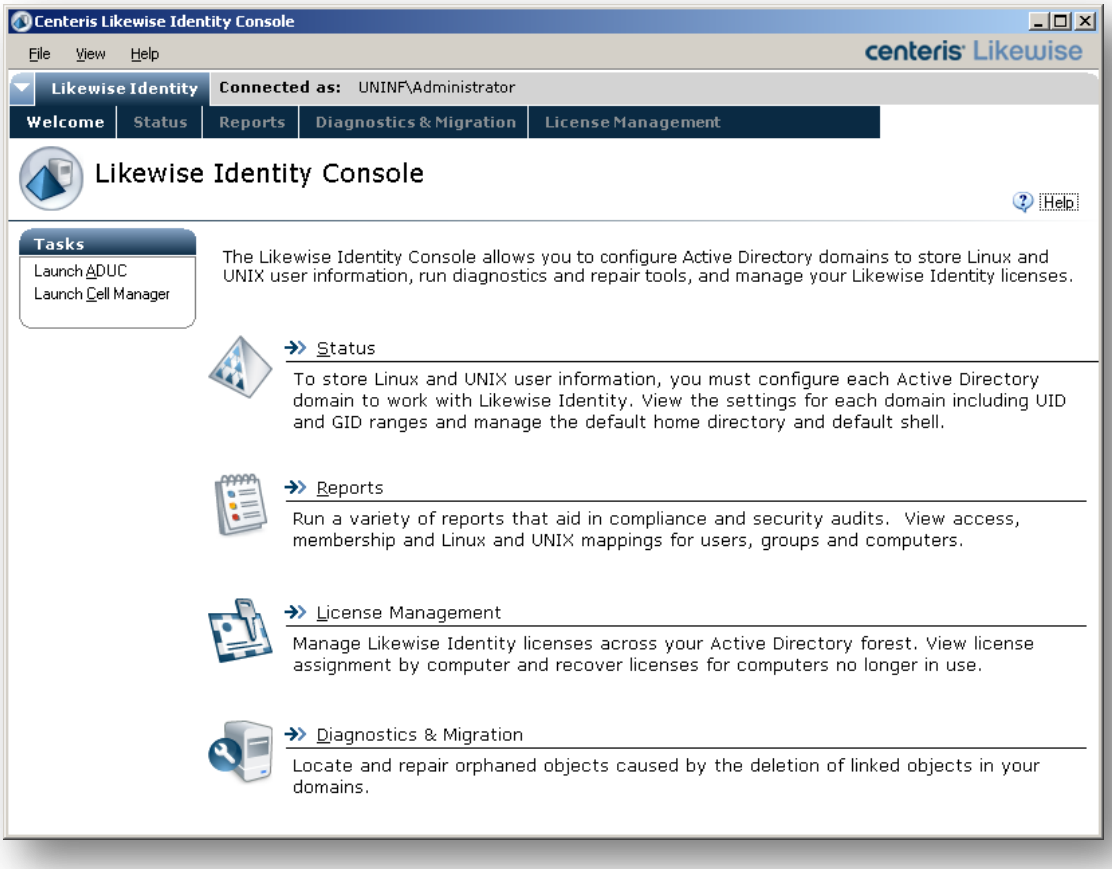
L'ultima schermata che ci viene mostrata conferma che l'applicazione della configurazione è avvenuta correttamente.



Opzionalmente, nella schermata precedente, è possibile cliccare sul tasto "*Show Log…*" per vedere le entries del file di log create dal wizard che prepara Active Directory. Quindi clicchiamo su "*Finish*" per completare la configurazione.

Il dominio di Active Directory è ora preparato e pronto per la gestione degli utenti e dei gruppi delle macchine UNIX e Linux.

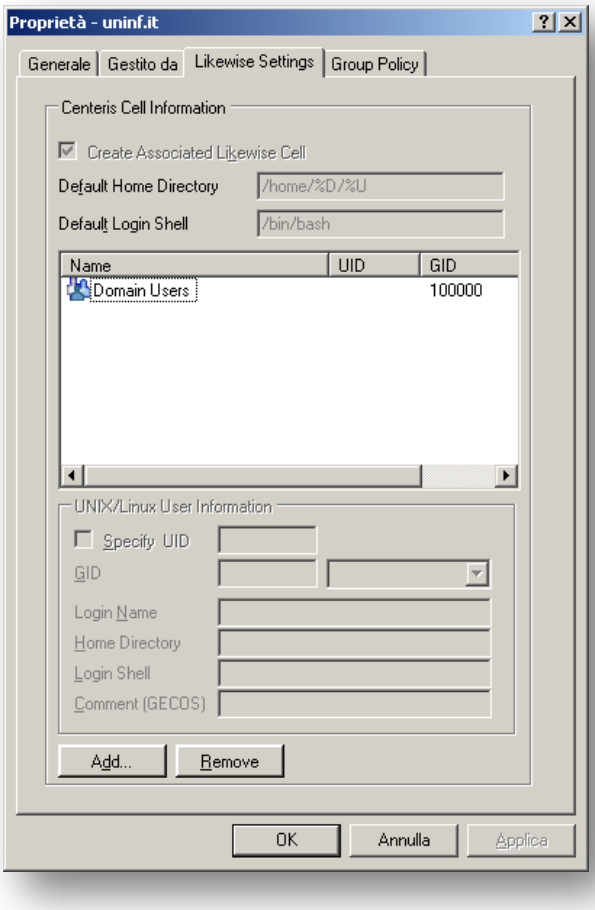
Nell'immagine successiva viene mostrata la console di Centeris Likewise Identity dopo essere stata configurata come descritto precedentemente.



8.8 Creazione di un Utente per il Login nel Dominio AD

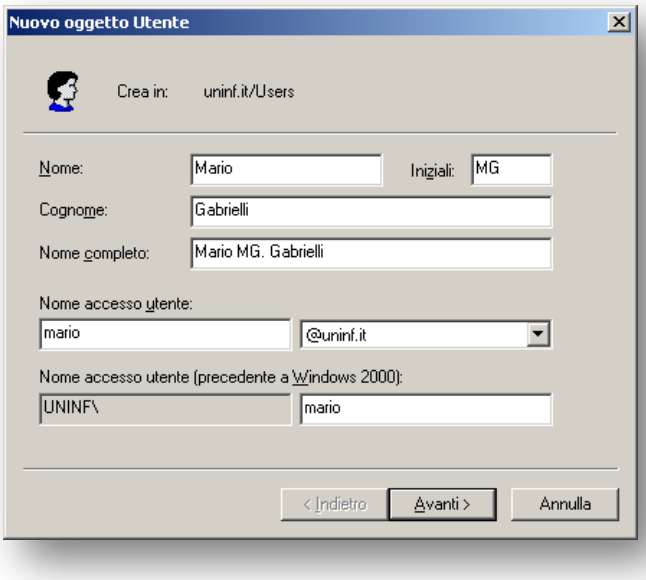
Per poter creare un utente che possa essere utilizzato per effettuare il login di macchine UNIX e Linux nel dominio di Active Directory, si procede nel seguente modo.

Per prima cosa spuntiamo la casella di controllo "*Create Associated Likewise Cell*" cosichè la cellula Likewise viene associata all'unità organizzativa. Per effettuare tale operazione, apriamo Active Directory e clicchiamo con il tasto destro sul nome di dominio, ci viene mostrato un menù nel quale clicchiamo su "*Proprietà*", quindi ci viene aperta una nuova finestra contenente diverse schede e noi selezioniamo "*Likewise Settings*", visibile nell'immagine successiva.

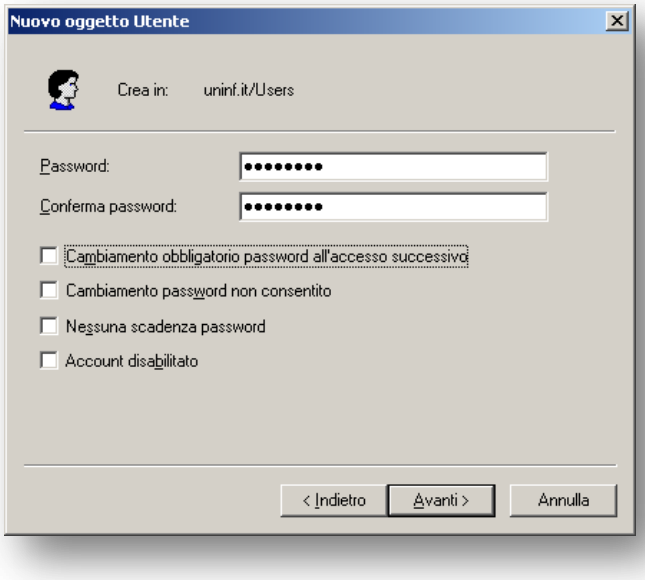


Ora che la cellula esiste, agli utenti possono essere assegnati specifici UID e

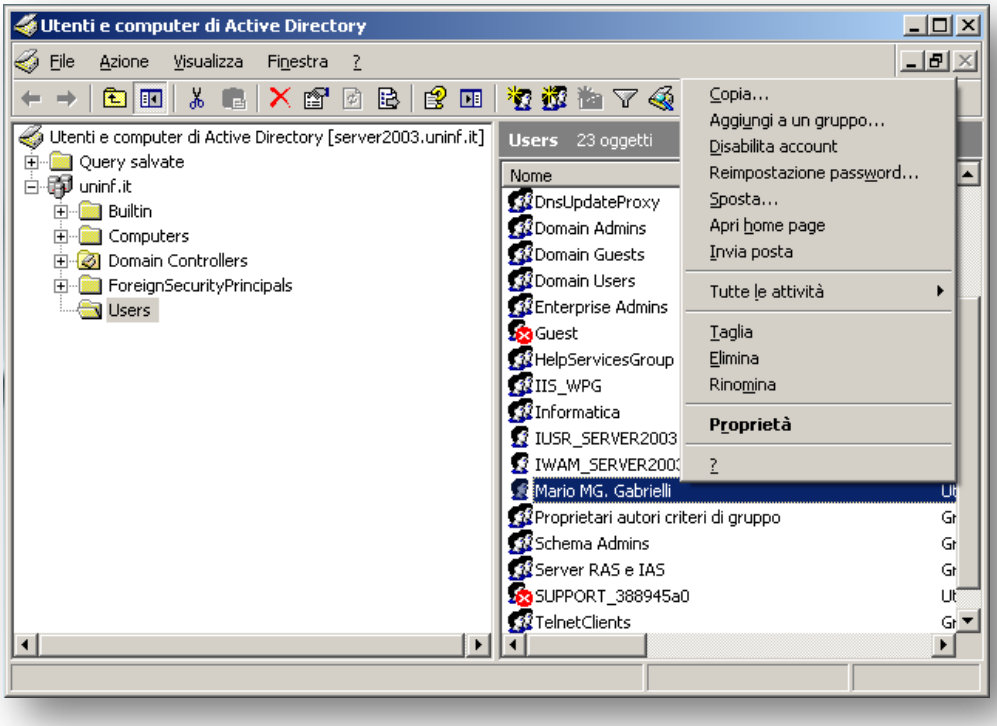
GID nella cellula, utilizzando lo snap-in "*Utenti e computer di Active Directory*". Quindi tramite quest'ultimo, creiamo un utente come visibile nell'immagine successiva.



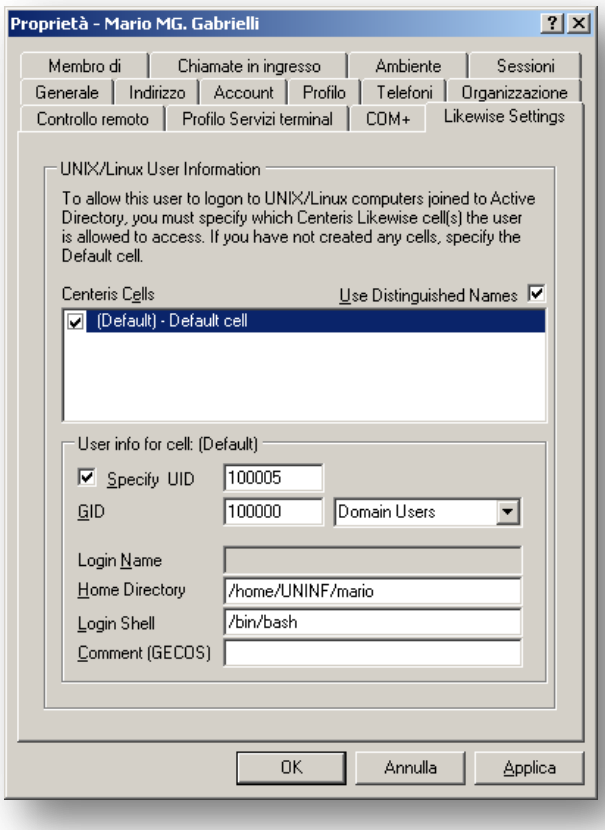
Si imposta la password per tale utente e si toglie la spunta su "*Cambiamento obbligatorio password all'accesso successivo*" in modo tale che quando andiamo ad effettuare il login non ci viene chiesto di cambiare password. Se invece si vuole che tale password venga cambiata occorre lasciare la spunta.



A questo punto per creare l'associazione tra l'UID e GID del sistema Linux e l'utente, di Active Directory, appena creato clicchiamo con il tasto destro sull'utente creato, ci viene aperto un menù nel quale selezioniamo "*Proprietà*", come evidente nell'immagine successiva.

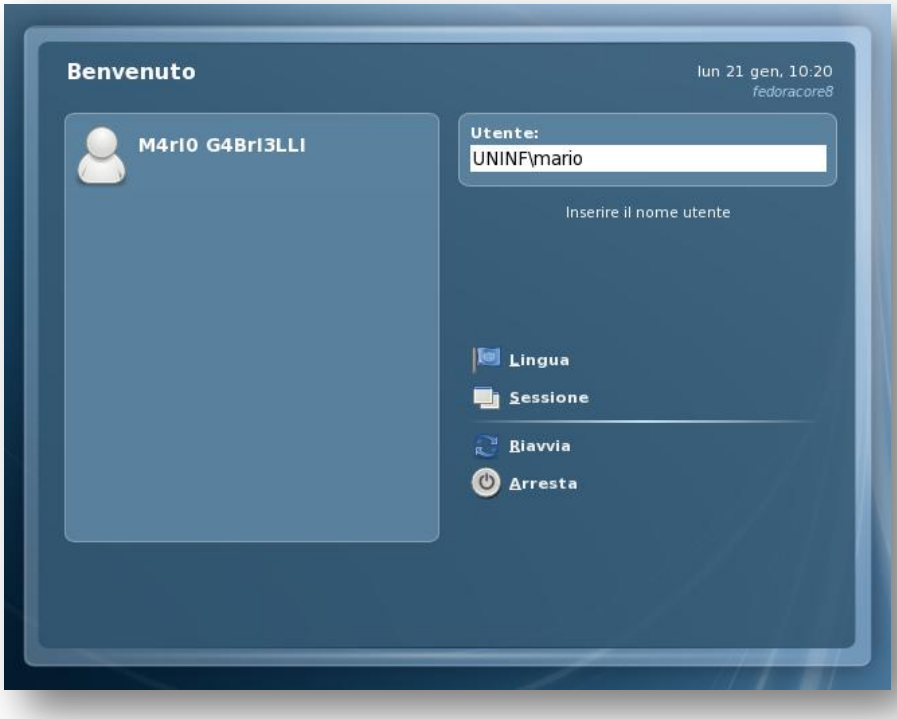


Una volta cliccato su "*Proprietà*" andiamo a selezionare la scheda "*Likewise Settings*", ci viene aperta la seguente finestra in cui andiamo ad impostare tutti i paramentri di associazione. Per prima cosa selezioniamo la cellula "*Default*"e gli altri valori ci vengono impostati in automatico, come l'UID, il GID, l'home directory e la shell di login, comunque è sempre possibile impostare tali valori a nostro piacimento.



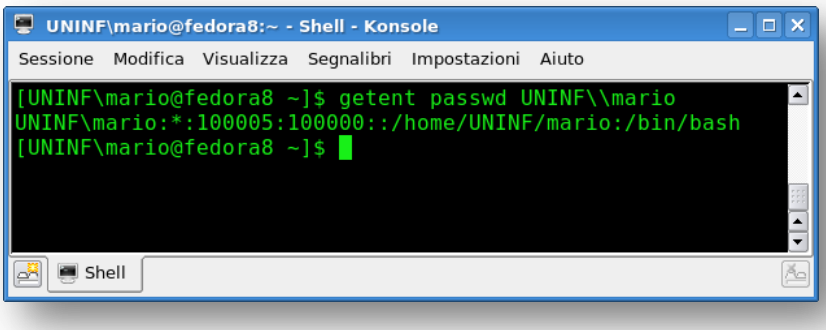
A questo punto clicchiamo sul tasto "*Applica*" per confermare le impostazioni, dopodiché se non ci vengono segnalati degli errori, clicchiamo su "*OK*" per completare la procedura.

Arrivati a questo punto possiamo provare se effettivamente l'account creato sia funzionante o meno. Per verificare il funzionamento ci spostiamo sulla macchina Linux e terminiamo la sessione corrente, quindi dalla finestra del login grafico, di fedora, andiamo a specificare l'account utente di Active Directory, appena creato, come evidente nell'immagine successiva.



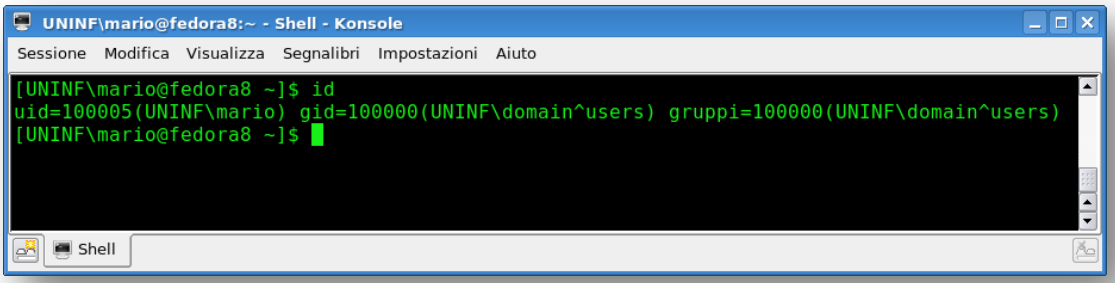
Per confermare premiamo il tasto invio e ci viene chiesto di specificare la password per tale utente, quindi forniamo la password precedentemente impostata durante la creazione dell'utente in Active Directory.

A questo punto se tutto è stato configurato adeguatamente la nostra macchina Linux aprirà il desktop grafico (KDE o GNOME) per tale utente. Una volta all'interno del desktop grafico possiamo visualizzare alcune informazioni relative all'account con il comando `getent` visibile nell'immagine successiva.

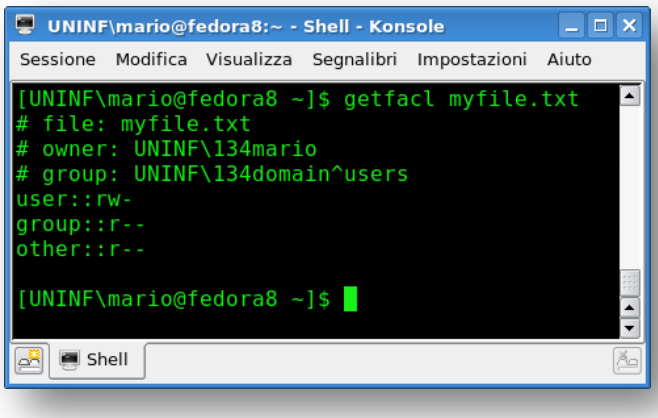


Possiamo anche osservare alcune proprietà dell'utente utilizzando il

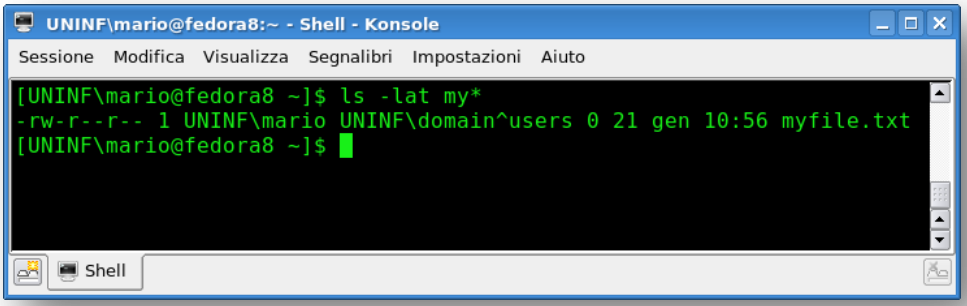
comando `id`, sempre visibile nell'immagine seguente.



Inoltre, tramite il comando `getfacl` è possiblie osservare la lista per i permessi di accesso (ACL) ad uno specifico file, nel nostro caso "*myfile.txt*" precedentemente creato con l'editor Vi, come evidente nell'immagine successiva.



Mentre con il comando `ls` vediamo le informazioni associate allo stesso file precedentemente creato.



CONCLUSIONI

APPENDICE A

Ho riportato in questa appendice lo script di configurazione di IPTables da me realizzato.

IPTables (/etc/sysconfig/iptables)

```
# Generated by iptables-save v1.3.8 on Mon Oct 29 18:39:49 2007
*nat
:PREROUTING ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A POSTROUTING -o eth0 -s 192.168.1.0/24 -j MASQUERADE
COMMIT
# Completed on Mon Oct 29 18:39:49 2007
*mangle
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
COMMIT
# Completed on Mon Oct 29 18:39:49 2007
# Generated by iptables-save v1.3.8 on Mon Oct 29 18:39:49 2007
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]

-A OUTPUT -p icmp -j ACCEPT
-A OUTPUT -p ALL -o lo -s 127.0.0.1 -j ACCEPT
-A OUTPUT -p TCP -o eth0 --dport 53 -j ACCEPT
-A OUTPUT -p UDP -o eth0 --dport 53 -j ACCEPT
-A OUTPUT -p TCP -o eth1 --dport 53 -j ACCEPT
-A OUTPUT -p UDP -o eth1 --dport 53 -j ACCEPT
-A OUTPUT -p TCP -o eth0 --dport 443 -j ACCEPT
-A OUTPUT -p TCP -o eth0 --dport 80 -j ACCEPT
-A OUTPUT -p TCP -o eth1 --dport 389 -j ACCEPT
-A OUTPUT -p TCP -o eth1 --dport 636 -j ACCEPT
```

```
-A OUTPUT -p TCP -o eth0 --dport ftp -j ACCEPT
-A OUTPUT -s 0/0 -p tcp ! --syn --sport ftp -j ACCEPT
-A OUTPUT -s 193.205.92.0/24 -p tcp --sport 1024: -d 0/0 --dport 1024: -
j ACCEPT
-A OUTPUT -s 0/0 -p tcp ! --syn --sport 1024: -d 193.205.92.0/24 --dport
1024: -j ACCEPT
-A OUTPUT -p TCP -m state --state RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -p UDP -m state --state RELATED,ESTABLISHED -j ACCEPT

-A OUTPUT -j LOG --log-prefix="OUTPUT: "

-A INPUT -p icmp -j ACCEPT
-A INPUT -p ALL -i lo -d 127.0.0.1 -j ACCEPT
-A INPUT -p TCP -i eth1 --dport 80 -j ACCEPT
-A INPUT -p TCP -i eth1 --dport 53 -j ACCEPT
-A INPUT -p UDP -i eth1 --dport 53 -j ACCEPT
-A INPUT -p TCP -i eth1 --dport 443 -j ACCEPT
-A INPUT -p TCP -i eth1 --dport 389 -j ACCEPT
-A INPUT -p TCP -i eth1 --dport 636 -j ACCEPT
-A INPUT -p TCP -i eth0 --dport 389 -j ACCEPT
-A INPUT -p TCP -i eth0 --dport 636 -j ACCEPT
-A INPUT -p TCP -i eth0 --dport 23384 -j ACCEPT
-A INPUT -p TCP -i eth1 --dport 23384 -j ACCEPT
-A INPUT -p TCP -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p UDP -m state --state ESTABLISHED,RELATED -j ACCEPT


-A INPUT -j LOG --log-prefix="INPUT: "


-A FORWARD -p TCP -i eth1 -o eth0 --dport 53 -j ACCEPT
-A FORWARD -p UDP -i eth1 -o eth0 --dport 53 -j ACCEPT
-A FORWARD -p TCP -i eth1 -o eth0 --dport 80 -j ACCEPT
-A FORWARD -p TCP -i eth1 -o eth0 --dport 443 -j ACCEPT
-A FORWARD -s 0/0 -p tcp ! --syn --sport ftp -j ACCEPT
-A FORWARD -s 192.168.1.0/24 -p tcp --sport 1024: -d 0/0 --dport 1024: -
j ACCEPT
-A FORWARD -s 0/0 -p tcp ! --syn --sport 1024: -d 192.168.1.0/24 --dport
1024: -j ACCEPT
-A FORWARD -p icmp -i eth1 -o eth0 -j ACCEPT
-A FORWARD -i eth0 -o eth1 -m state --state ESTABLISHED,RELATED -j
ACCEPT
-A FORWARD -i eth1 -o eth0 -m state --state ESTABLISHED,RELATED -j
ACCEPT

-A FORWARD -j LOG --log-prefix="FORWARD: "


COMMIT
# Completed on Mon Oct 29 18:39:49 2007
# Generated by iptables-save v1.3.8 on Mon Oct 29 18:39:49 2007
```

APPENDICE B

Viene riportato in questa appendice la configurazione dettagliata del Fedora Directory Server.

```
[root@uninf /]# cd opt
[root@uninf opt]# cd fedora-ds/
[root@uninf fedora-ds]# cd setup
[root@uninf setup]# ./setup
INFO Begin Setup . . .

LICENSE AGREEMENT AND LIMITED PRODUCT WARRANTY
FEDORA(TM) DIRECTORY SERVER

This agreement governs the use of Fedora Directory Server,
Administration Server and Management Console (collectively, the
"SOFTWARE") and any updates to the Software, regardless of the
delivery mechanism.

1.  FEDORA DIRECTORY SERVER

1.1 LICENSE GRANT.  Fedora Directory Server ("FDS") is a modular
application consisting of hundreds of software components and is a
collective work under U.S. Copyright Law.  Subject to the following
terms, Red Hat, Inc. ("RED HAT") grants to the user ("LICENSEE") a
license to this collective work pursuant to the GNU General Public
License.  Please note that Administration Server and Management
Console, which are binary-only code used to configure and administer
FDS, are subject to the license terms in Section 2.  The end user
license agreement for each component of FDS is located in the
component's source code. The license terms for the components
permit LICENSEE to copy, modify, and redistribute the component, in
both source code and binary code forms.  This agreement does not limit
LICENSEE's rights under, or grant LICENSEE rights that supersede, the
license terms of any particular component.
```

1.2 LICENSE EXCEPTION. In addition, as a special exception, Red Hat gives LICENSEE the additional right to link the code of FDS with code not covered under the GNU General Public License ("NON-GPL CODE") and to distribute linked combinations including the two, subject to the limitations in this paragraph. Non-GPL Code permitted under this exception must only link to the code of FDS through those well defined interfaces identified in that file named EXCEPTION in the source code files for FDS (the "APPROVED INTERFACES"). The files of Non-GPL Code may instantiate templates or use macros or inline functions from the Approved Interfaces without causing the resulting work to be covered by the GNU General Public License. Only Red Hat may make changes or additions to the list of Approved Interfaces. LICENSEE must comply with the GNU General Public License in all respects for all of the FDS code and other code used in conjunction with FDS except the Non-GPL Code covered by this exception. If LICENSEE modifies FDS, LICENSEE may extend this exception to its version of FDS, but LICENSEE is not obligated to do so. If LICENSEE does not wish to provide this exception without modification, LICENSEE must delete this exception statement from LICENSEE's version of FDS and license FDS solely under the GPL without exception.

1.3 INTELLECTUAL PROPERTY RIGHTS. FDS and each of its components, including the source code, documentation, appearance, structure and organization are owned by Red Hat and others and are protected under copyright and other laws. Title to FDS and any component, or to any copy, modification, or merged portion shall remain with the aforementioned, subject to the applicable license.

2. ADMINISTRATION SERVER, AND MANAGEMENT CONSOLE

2.1 LICENSE GRANT. Subject to the provisions of this Section 2.1, Red Hat hereby grants LICENSEE a non-exclusive, non-transferable, worldwide, perpetual, fully paid right (without the right to sublicense) to use, reproduce and distribute Administration Server ("ADMIN SERVER"), and Management Console ("CONSOLE") in executable, machine-readable form. LICENSEE must reproduce all copyright and other proprietary notices on such copies. LICENSEE may only reproduce and distribute Admin Server or Console to another party if the other party agrees in writing to be obligated by the terms and conditions of this Section 2.1. Except as provided in this Section 2.1, LICENSEE may not modify, copy, transfer or otherwise use Admin Server, or Console, and all licenses granted in this Section 2 are automatically terminated if LICENSEE does so.

2.2 CHANGE IN LICENSING. It is Red Hat's intent to change the terms of the license granted in this Section 2 to that of an open source license. If such change is generally announced to the public, LICENSEE will have the option to elect to have Admin Server and Console governed by the terms of such open source license. If LICENSEE does not make such election, the terms of this Agreement will continue to govern LICENSEE's use of Admin Server and Console.

3. LIMITED WARRANTY. Except as specifically stated in this Section 3 or a license for a particular component, TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, THE SOFTWARE AND THE COMPONENTS ARE PROVIDED AND LICENSED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESSED OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE. Red Hat does not warrant that the functions contained in the Software will meet LICENSEE's requirements or that the operation of the Software will be entirely error free or appear precisely as described in the accompanying documentation.

4. LIMITATION OF REMEDIES AND LIABILITY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, RED HAT WILL NOT BE LIABLE TO LICENSEE FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING LOST PROFITS OR LOST SAVINGS ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE, EVEN IF RED HAT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

5. EXPORT CONTROL. As required by U.S. law, LICENSEE represents and warrants that it: (a) understands that the Software is subject to export controls under the U.S. Commerce Department's Export Administration Regulations ("EAR"); (b) is not located in a prohibited destination country under the EAR or U.S. sanctions regulations (currently Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria); (c) will not export, re-export, or transfer the Software to any prohibited destination, entity, or individual without the necessary export license(s) or authorizations(s) from the U.S. Government; (d) will not use or transfer the Software for use in any sensitive nuclear, chemical or biological weapons, or missile technology end-uses unless authorized by the U.S. Government by regulation or specific license; (e) understands and agrees that if it is in the United States and exports or transfers the Software to eligible end users, it will, as required by EAR Section 740.17(e), submit semi-annual reports to the Commerce Department's Bureau of Industry & Security (BIS), which include the name and address (including country) of each transferee; and (f) understands that countries other than the United States may restrict the import, use, or export of encryption products and that it shall be solely responsible for compliance with any such import, use, or export restrictions.

6. THIRD PARTY PROGRAMS. Red Hat may distribute third party software programs with the Software that are not part of the Software. These third party programs are subject to their own license terms. The license terms either accompany the programs or can be viewed at http://www.redhat.com/licenses/. If LICENSEE does not agree to abide by the applicable license terms for such programs, then LICENSEE may not install them. If LICENSEE wishes to install the programs on more than one system or transfer the programs to another party, then LICENSEE must contact the licensor of the programs.

7. GENERAL. If any provision of this agreement is held to be

```
unenforceable, that shall not affect the enforceability of the
remaining provisions.  This agreement shall be governed by the laws of
the State of North Carolina and of the United States, without regard
to any conflict of laws provisions, except that the United Nations
Convention on the International Sale of Goods shall not apply.

Do you accept the license terms? (yes/no) yes
===============================================================================
                        Fedora Directory Server 1.0.4
===============================================================================

The Fedora Directory Server is subject to the terms detailed in the
license agreement file called LICENSE.txt.

Late-breaking news and information on the Fedora Directory Server is
available at the following location:

    http://directory.fedora.redhat.com

Continue? (yes/no) yes
Fedora Directory Server system tuning analysis version 04-APRIL-2005.

NOTICE : System is i686-unknown-linux2.6.23.8-63.fc8 (2 processors).

WARNING: 1008MB of physical memory is available on the system. 1024MB is
recommended for best performance on large production system.

NOTICE : The net.ipv4.tcp_keepalive_time is set to 7200000 milliseconds
(120 minutes).  This may cause temporary server congestion from lost
client connections.

WARNING: There are only 1024 file descriptors (hard limit) available,
which
limit the number of simultaneous connections.

WARNING: There are only 1024 file descriptors (soft limit) available,
which
limit the number of simultaneous connections.


Continue? (yes/no) yes

Please select the install mode:
  1 - Express - minimal questions
  2 - Typical - some customization (default)
  3 - Custom - lots of customization

Please select 1, 2, or 3 (default: 2) 2

Hostname to use (default: localhost.localdomain) fedora8.uninf.it
```

```
Server user ID to use (default: nobody) nobody

Server group ID to use (default: nobody) nobody

Fedora server information is stored in the Fedora configuration
directory server, which you may have already set up.  If so, you
should configure this server to be managed by the configuration
server.  To do so, the following information about the configuration
server is required: the fully qualified host name of the form
<hostname>.<domainname>(e.g. hostname.domain.com), the port number,
the suffix, and the DN and password of a user having permission to
write the configuration information, usually the Fedora
configuration directory administrator.

If you want to install this software as a standalone server, or if you
want this instance to serve as your Fedora configuration directory
server, press Enter.


Do you want to register this software with an existing
Fedora configuration directory server? [No]: No


If you already have a directory server you want to use to store your
data, such as user and group information, answer Yes to the following
question.  You will be prompted for the host, port, suffix, and bind
DN to use for that directory server.

If you want this directory server to store your data, answer No.

Do you want to use another directory to store your data? [No]: No

The standard directory server network port number is 389.  However, if
you are not logged as the superuser, or port 389 is in use, the
default value will be a random unused port number greater than 1024.
If you want to use port 389, make sure that you are logged in as the
superuser, that port 389 is not in use, and that you run the admin
server as the superuser.

Directory server network port [389]: 389

Each instance of a directory server requires a unique identifier.
Press Enter to accept the default, or type in another name and press
Enter.

Directory server identifier [uninf.it]: uninf.it

Please enter the administrator ID for the Fedora configuration
directory server.  This is the ID typically used to log in to the
console.  You will also be prompted for the password.
```

```
Fedora configuration directory server
administrator ID [admin]: admin
Password: ********
Password (again): ********

The suffix is the root of your directory tree.  You may have more than
one suffix.

Suffix [dc=uninf, dc=it]: dc=uninf,dc=it

Certain directory server operations require an administrative user.
This user is referred to as the Directory Manager and typically has a
bind Distinguished Name (DN) of cn=Directory Manager.  Press Enter to
accept the default value, or enter another DN.  In either case, you
will be prompted for the password for this user.  The password must
be at least 8 characters long.


Directory Manager DN [cn=Directory Manager]: cn=Directory Manager
Password: ********
Password (again): ********

The Administration Domain is a part of the configuration directory
server used to store information about Fedora software.  If you are
managing multiple software releases at the same time, or managing
information about multiple domains, you may use the Administration
Domain to keep them separate.

If you are not using administrative domains, press Enter to select the
default.  Otherwise, enter some descriptive, unique name for the
administration domain, such as the name of the organization responsible
for managing the domain.

Administration Domain [uninf.it]: uninf.it

The Administration Server is separate from any of your application
servers since it listens to a different port and access to it is
restricted.

Pick a port number between 1024 and 65535 to run your Administration
Server on. You should NOT use a port number which you plan to
run an application server on, rather, select a number which you
will remember and which will not be used for anything else.

The default in brackets was randomly selected from the available
ports on your system. To accept the default, press return.

Administration port [28324]: 28324

The Administration Server program runs as a certain user on your
system. This user should be different than the one which your
```

```
application servers run as. Only the user you select will be
able to write to your configuration files. If you run the
Administration Server as "root", you will be able to use the Server
Administration screen to start and stop your application servers.

Run Administration Server as [root]: root

The Administration Server runs on the Apache web server. Please provide
the
directory where the Apache binary (httpd or httpd.worker) may be found.
The
Administration Server needs an Apache compiled with the worker model.

Apache Directory [/usr/sbin/]: /usr/sbin/

[slapd-fedora8]: starting up server ...
[slapd-fedora8]:        Fedora-Directory/1.0.4 B2006.312.1539
[slapd-fedora8]:        fedora8.uninf.it:389 (/opt/fedora-ds/slapd-
fedora8)
[slapd-fedora8]:
[slapd-fedora8]: [22/Dec/2007:14:08:46 +0100] - Fedora-Directory/1.0.4
B2006.312.1539 starting up
[slapd-fedora8]: [22/Dec/2007:14:08:47 +0100] - slapd started.
Listening on All Interfaces port 389 for LDAP requests
Your new directory server has been started.
Created new Directory Server
Start Slapd Starting Slapd server configuration.
Success Slapd Added Directory Server information to Configuration
Server.
Configuring Administration Server...
Setting up Administration Server Instance...
Configuring Administration Tasks in Directory Server...
Configuring Global Parameters in Directory Server...

You can now use the console.  Here is the command to use to start the
console:
cd /opt/fedora-ds

./startconsole -u admin -a http://fedora8.uninf.it:28324/

INFO Finished with setup, logfile is setup/setup.log
[root@uninf setup]#
```

BIBLIOGRAFIA

[1] "*Cenni generali su Active Directory*", 2006, education.mondadori.it/libri/Download/Capitoli/88-8331-209-0_Cap01.pdf

[2] Rocco De Marco, "*AAA in ambiente OpenSource PPPoE, LDAP, RADIUS*", 2005.

[3] Simone Piccardi, "*Integrazione sistemistica con LDAP*", 2006, http://www.truelite.it/node/40/pdf

[4] Antonio Anselmi "*OpenLDAP un completo directory service opensource*", "*Linux&C*", 2007.

[5] Luigi Genoni, "*Linux Firewall*", 2004.

[6] Sportolari Francesco, "*Reti LAN in pratica: la configurazione*", "*Linux partico*".

[7] Walter Cerroni, "IP Forwarding", 2007, www-tlc.deis.unibo.it/Didattica/CorsiCE/LabRetiLA/LabRetiLA_CE/03-IP_Forwarding.pdf

[8] OpenSkills, "*/etc/dhcpd.conf*", http://openskills.info/infobox.php?IDbox=749&boxtype=path

[9] Mario Gabrielli, "*Elementi di Progettazione di un Internet Firewall*", 2004.

[10] DigitalStorm, "*VMware*", http://www.digitalstorm.it/vmware.asp

[11] Sisnay, "*VMware Workstation*", http://www.virtualcenter.it/prodotti.aspx?pag=workstation

[12] Sysadmin, "*Networking con VMware Server*", http://www.sysadmin.it/pages/guide/guide.asp?ID=91

[13] S.Pinardi, E.Colombo, A.Aruanno, R.Bisiani, "*Active Directory come Directory Service*", Duke Italia, 2005.

[14] Visivagroup, "*[2003] Installare Active Directory*", http://www.visivagroup.it/showthread.php?t=8500

[15] Prof. Ing. Dino Molli, "*Installazione del servizio di Active Directory*", http://www.dinomolli.it/Modulo_C/PDF_Singoli/9_6a.pdf

[16] Dan Holme, Orin Thomas "*Upgrading your certification to Microsoft Windows Server 2003*", Mondadori Informatica, 2004.

[17] William R. Stanek, "*Windows Server 2003 Guida Pratica*", Mondadori Informatica, 2005.

[18] IBM, "Configuring Microsoft Active Directory for SSL access", http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.itame.doc/am60_install166.html

[19] Carla Schroder, "*Use Fedora Directory Server For Manageable LDAP*", 2006, http://www.enterprisenetworkingplanet.com/netos/article.php/3622486

[20] Jon Fautley, "*Fedora Directory Server*", 2005, fedoranews.org/tchung/FUDCon3/FUDCon3JFautley.pdf

[21] Red-Hat, "*Deployment Guide – Red Hat Directory Server*", 2005 http://www.redhat.com/docs/manuals/dir-server/pdf/ds71deploy.pdf

[22] Red-Hat, "*Red Hat Directory Server Installation Guide*", 2005 http://www.redhat.com/docs/manuals/dir-server/pdf/ds71install.pdf

[23] Ashley Chew, "*Fedora Directory Server 1.x Installation, Configuration & Client Binding*", 2006, http://www.csse.uwa.edu.au/~ashley/fedora-ds/fedora-ds-26072006.html

[24] Fedora, "*SysV Init scripts for Fedora DS*", 2007
http://directory.fedoraproject.org/wiki/Howto:SysVInit

[25] Dael Maselli, "*Fedora Directory Server*", 2006,
http://www.lnf.infn.it/~dmaselli/fds.php

[26] Red-Hat, "*Managing Servers with Red Hat Console*", 2005,
http://www.redhat.com/docs/manuals/dir-server/pdf/console71.pdf

[27] Fedora, "*Configuring SSL Enabled Fedora Directory Server*", 2007,
http://directory.fedoraproject.org/wiki/Howto:SSL

[28] Softerra, "*LDAP Administrator*", 2007,
http://www.ldapadministrator.com/

[29] Microsoft, "*Utilizzo di Ldap.exe per trovare i dati in Active Directory*", 2007
http://support.microsoft.com/kb/224543

[30] Microsoft, "*Elementi di base delle query LDAP*", 2007
http://www.microsoft.com/italy/technet/prodtechnol/exchange/2003/insider/ldapquery.mspx

[31] Mmgsecurity, "*LDAP Administration Tool*", 2007
http://dev.mmgsecurity.com/projects/lat/

[32] Red-Hat, "*Administrator's Guide Red Hat Directory Server*", 2005,
http://www.redhat.com/docs/manuals/dir-server/pdf/ds71admin.pdf

[33] Fedora, "*Sync With Active Directory*", 2007
http://directory.fedoraproject.org/wiki/Howto:WindowsSync

[34] Andrea Giorgini, "*Modifica di dati su Active Directory tramite PHP*", 2007
http://wiki.grusp.it/articoli:php_e_active_directory

[35] OpenSkills, "*Configurare BIND*", 2003,
http://openskills.info/topic.php?ID=113

[36] Nicolai Langfeldt, "*DNS HOWTO*", 2001,
http://www.pluto.it/files/ildp/HOWTO/DNS-HOWTO/DNS-HOWTO.html

[37] Internet System Consortium, "*BIND 9 Administrator Reference Manual*", 2007 http://www.isc.org/sw/bind/arm95/Bv9ARM.pdf

[38] Bob Carver, "*Linux to Windows Migration*", 2001, https://lb1.www.ms.akadns.net/technet/archive/interopmigration/linux/mvc/cfgbind.mspx?mfr=true

[39] Microsoft, "*Come attivare l'aggiornamento dinamico sopra Server DNS UNIX BIND*", 2007, http://support.microsoft.com/kb/275866/it