CREAZIONE PARTIZIONE, CLASSI E ATTRIBUTI ALL'INTERNO DELLO SCHEMA DI ACTIVE DIRECTORY

CREAZIONE CLASSE

Aprire lo Schema Snap-In come in figura 1

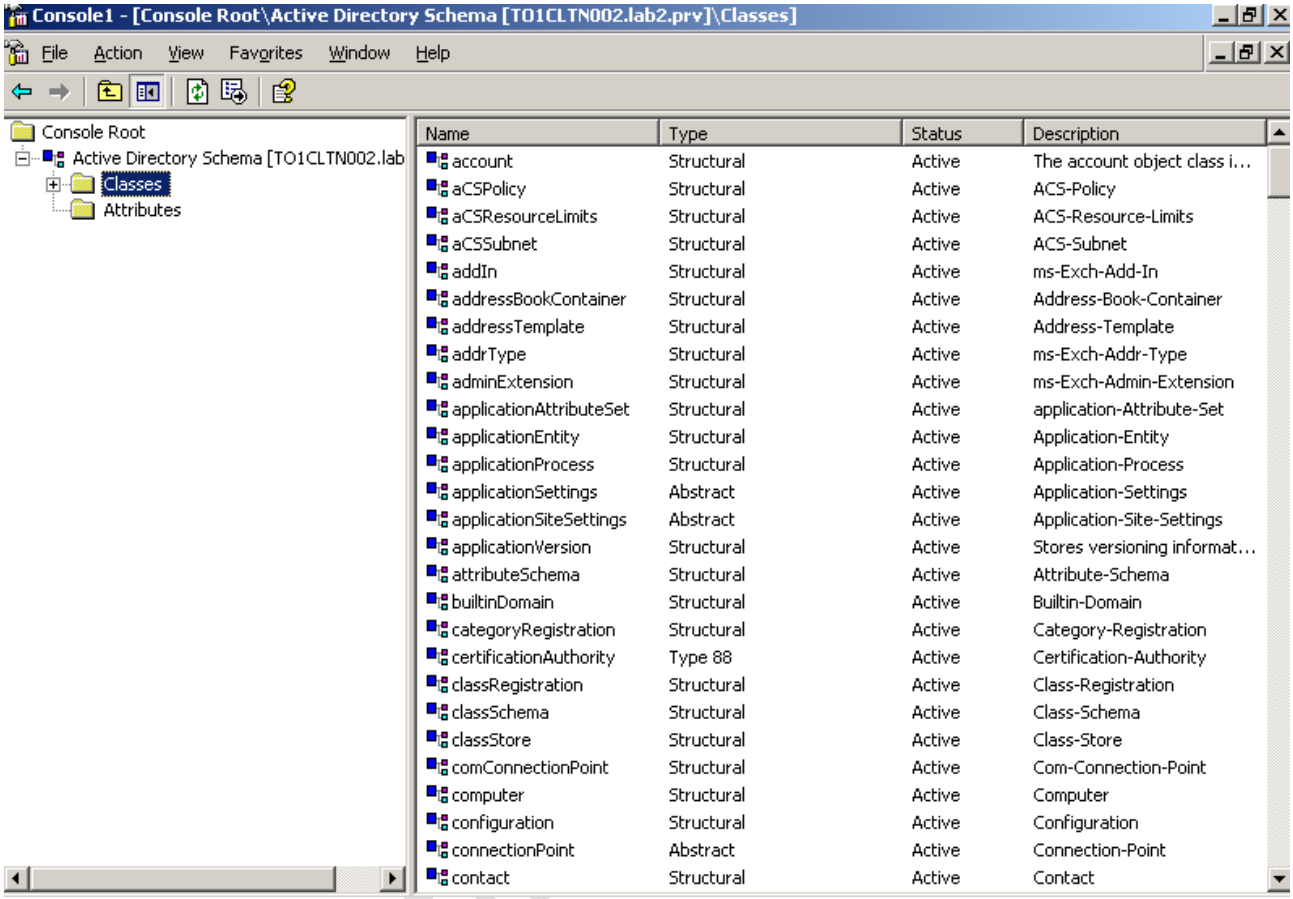

Fig.1

Ciccare col tasto destro su **Classes** e selezionare **Create Class**

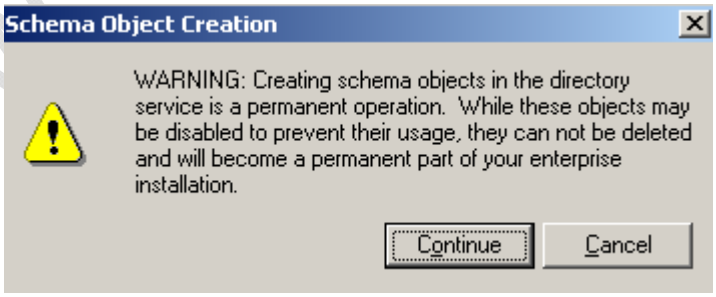

Fig.2

Ciccare su **Continue**

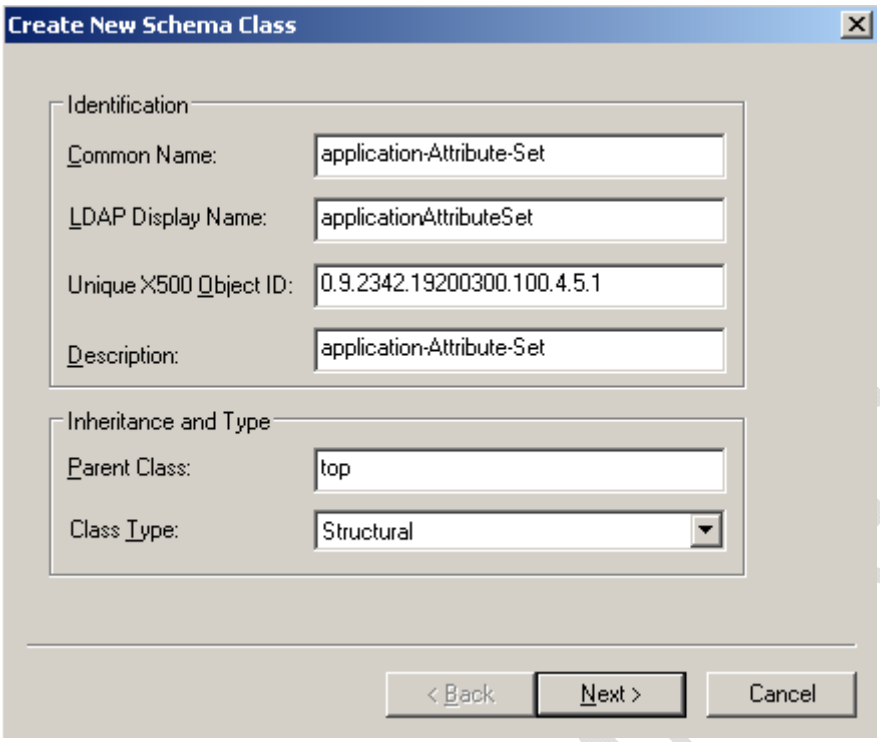

Fig.3

A questo punto valorizzare i seguenti campi:

- **Common Name** : di solito la prima parte indica il produttore (ms) la seconda parte il prodotto (exch) e la terza parte la descrizione del prodotto (Directory Connector). Le varie parti vanno separate con un trattino per seguire lo stile Microsoft
- **LDAP Display Name**: è il nome che viene visualizzato all'interno dell'elenco LDAP
- Inique X500 Object ID: è un SID generato da un programma reperibile nel Resource Kit di Windows 2000 (oidgen.exe)
- **Description**: di solito si inserisce lo stesso valore di Common Name
- **Parent Class**: top (è la classe primaria dalla quale discendono tutte le altre conviene mettere sempre questa se non si sa esattamente cosa si sta facendo)
- **Class Type**: Lasciare la classe Structural anche perchè Abstract non si può utilizzare.

Valorizzati i campi ciccare su **Next** (**ATTENZIONE una volta creata la classe non si potrà più cancellare dallo SCHEMA ma solamente disabilitare per recuperare il SID**)

Ciccare su **Next**

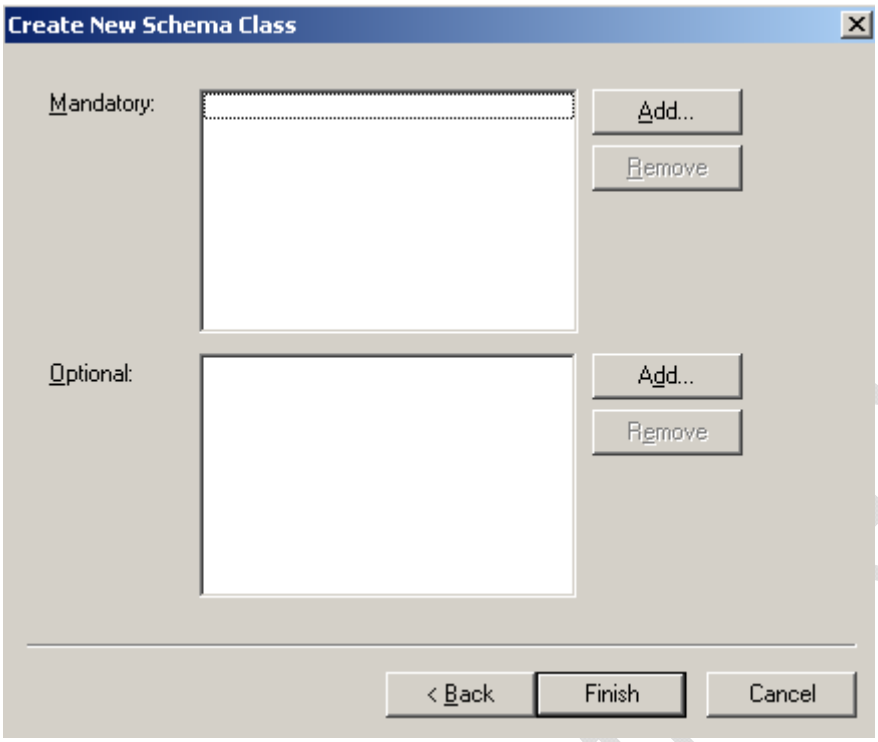

Fig.4

A questo punto bisogna inserire delle classi:

Mandatory: sono le classi mandatarie ed è possibile inserirle solo a questo punto della creazione della classe in seguito non sarà possibile inserire nessuna classe mandatoria aggiuntiva.
Optional: Questo campo possiamo lasciarlo anche vuoto visto che si può modificare successivamente.

Quindi clicchiamo su **Finish**

Se adesso selezioniamo la classe appena creata dovremmo avere una situazione come in figura 5

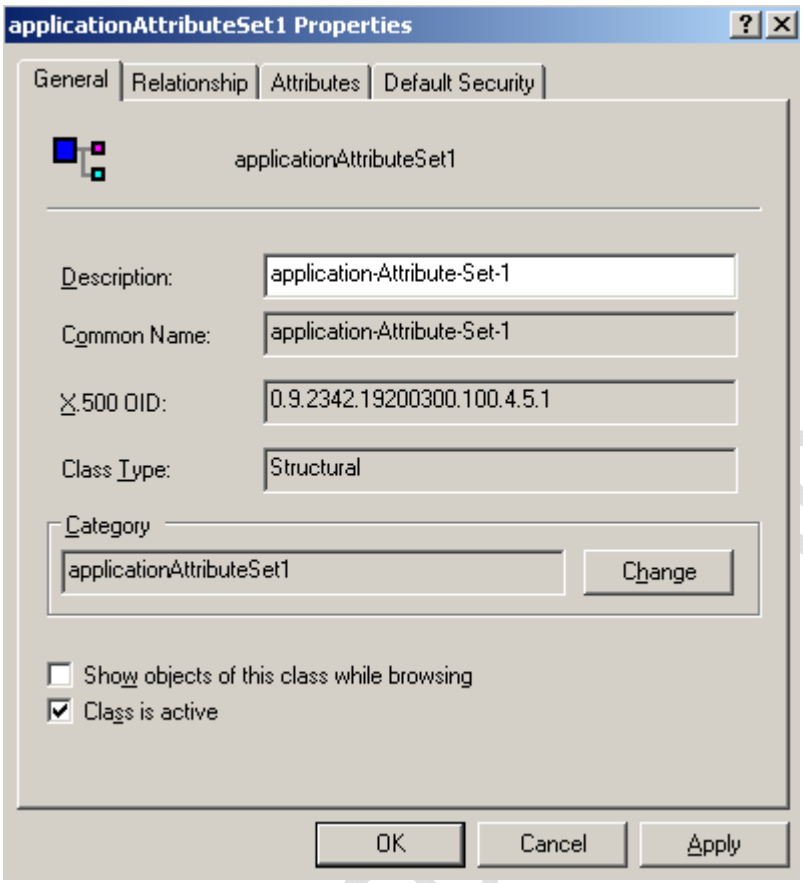

Fig.5

La classe per funzionare deve essere Attiva (la spunta Class is Active è messa di Defualt)

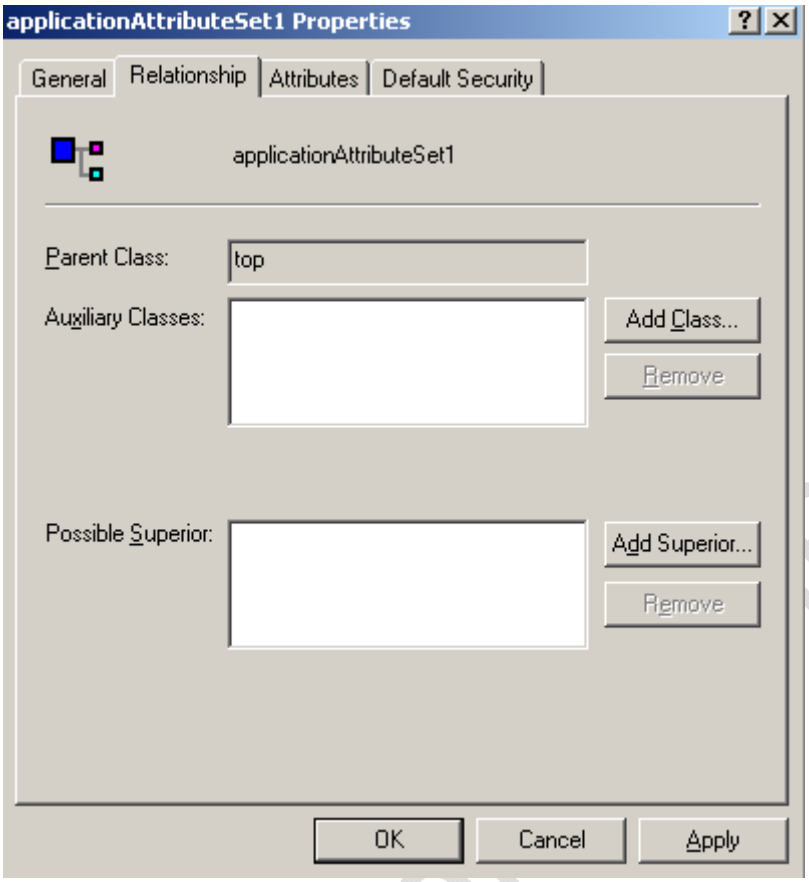

Fig.6

Nella sezione Relationship noteremo che solo il campo Parent Class è valorizzato con top.
Gli altri due campi sono vuoti.

Per il momento lasciamo tutto invariato torneremo su questi campi più tardi.

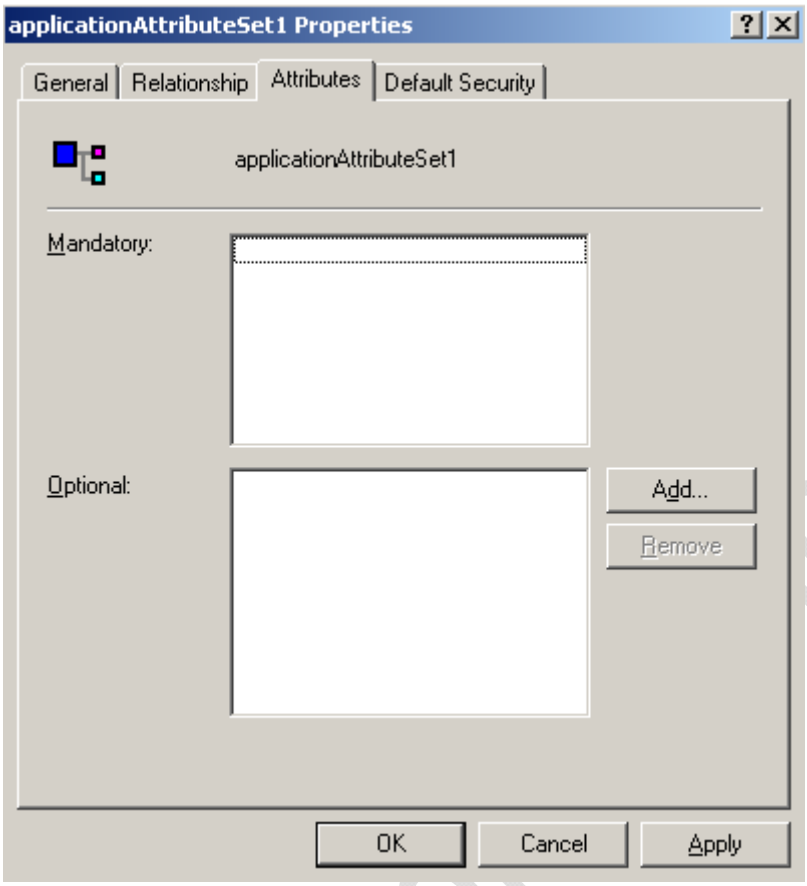

Fig.7

Nella sezione **Attributes** come da scelta effettuata precedentemente è tutto vuoto.

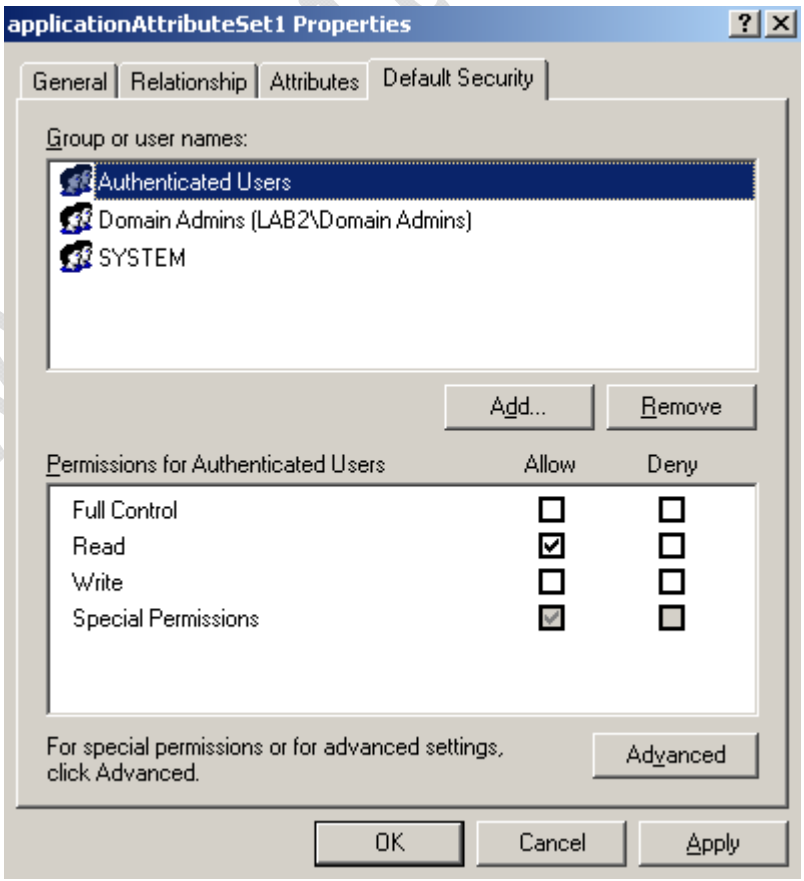

Fig.8

Nella sezione **Security** a meno di eventuali restrizioni o deleghe converrebbe lasciare tutto invariato

CREAZIONE ATTRIBUTO

Sempre all'interno dello Schema Sanp-In posizioniamoci sulla radice Attributes

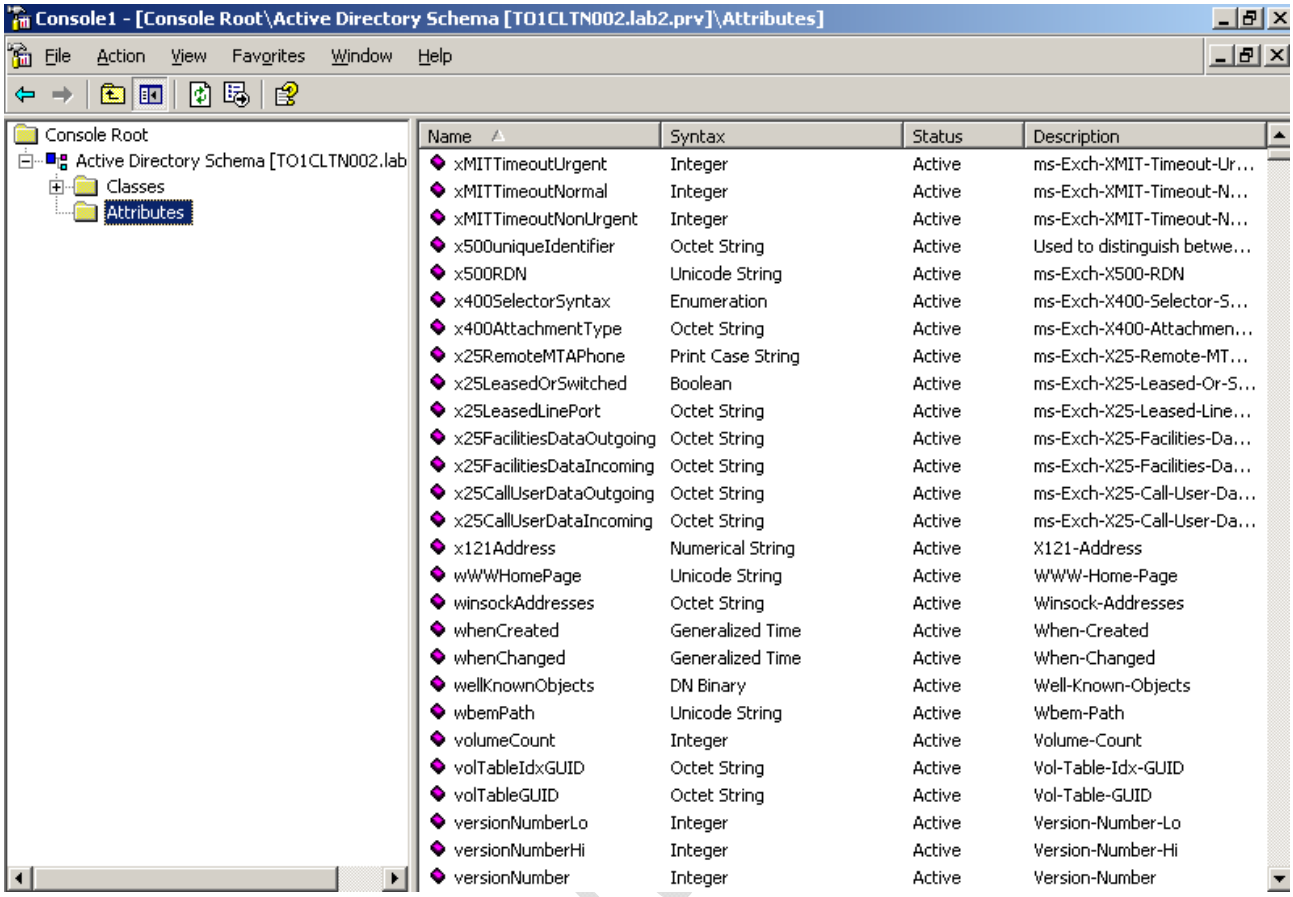

Fig.9

Quindi cliccando di destro selezioniamo create **Attribute**

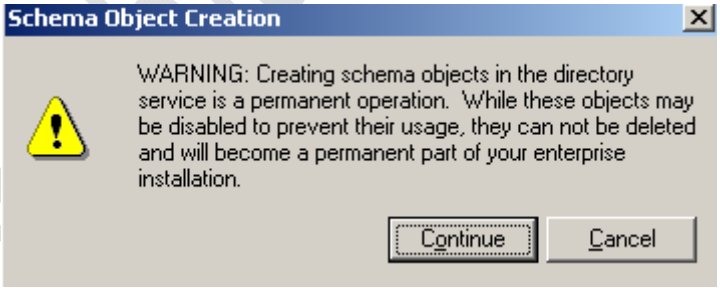

Fig.10

Clicchiamo su **Continue**

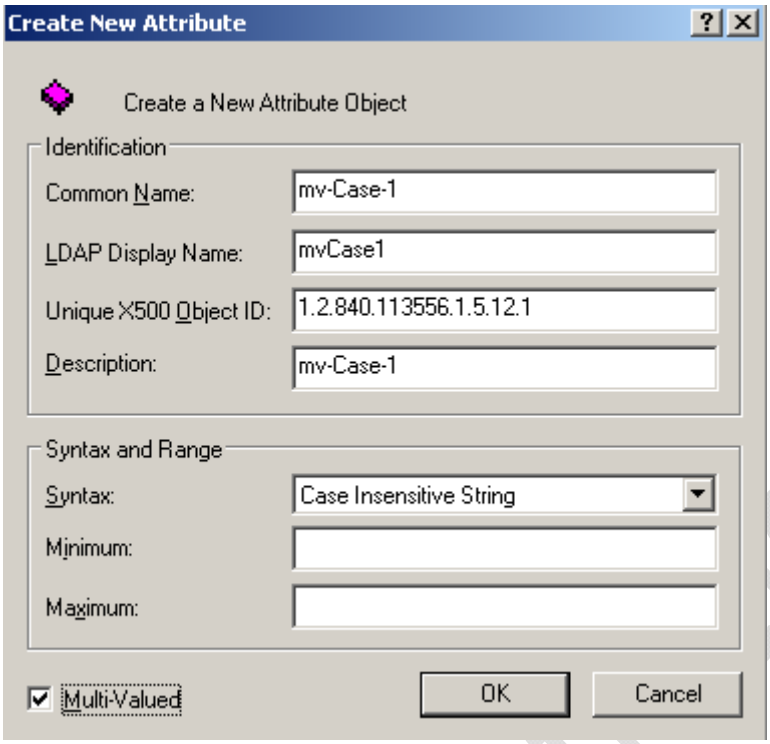

Fig.11

Vale un pò la stessa cosa come per le classi converrebbe mettere come OID un numero che abbia la stessa radice della classe con un .2 alla fine e cosi via per tutti gli attributi che dobbiamo creare.
Scegliamo la sintassi da usare (Case Sensitive String) quindi diamo un valore minimo e massimo (se a priori conosciamo un valore massimo e un minimo che può assumere la variabile inseriamoli altrimenti lasciamo tutto cosi)
Spuntare Multi-Valued se serve un attributo multi valori.
Di seguito le sintassi con le relative descrizioni possibili da utilizzare

Attributo	Common Name	LDAP Display name
Boolean	SV-Bolean-<numero progressivo> MV-Bolean-<numero progressivo>	sVBolean<numero progressivo> mVBolean<numero progressivo>
Enumeration	SV-Enumeration-<numero progressivo> MV-Enumeration-<numero progressivo>	sVEnumeration<numero progressivo> mVEnumeration<numero progressivo>
Integer	SV-Integer-<numero progressivo> MV-Integer-<numero progressivo>	sVInteger<numero progressivo> mVInteger<numero progressivo>
INTEGER8	SV-INTEGER8-<numero progressivo> MV-INTEGER8-<numero progressivo>	sVINTEGER8<numero progressivo> mVINTEGER8<numero progressivo>
CaseExactString	SV-CaseExtractString-<numero progressivo> MV-CaseExtractString-<numero progressivo>	sVCaseExtractString<numero progressivo> mVCaseExtractString<numero progressivo>
CaseIgnoreString	SV-CaseIgnoreString-<numero progressivo> MV-CaseIgnoreString-<numero progressivo>	sVCaseIgnoreString<numero progressivo> mVCaseIgnoreString<numero progressivo>
DirectoryString	SV-DirectoryString-<numero progressivo> MV-DirectoryString-<numero progressivo>	sVDirectoryString<numero progressivo> mVDirectoryString<numero progressivo>
IA5String	SV-IA5String-<numero progressivo> MV-IA5String-<numero progressivo>	sVIA5String<numero progressivo> mVIA5String<numero progressivo>

NTSecurityDescriptor	SV-NTSecurityDescriptor-<numero progressivo> MV-NTSecurityDescriptor-<numero progressivo>	sVNTSecurityDescriptor<numero progressivo> mVNTSecurityDescriptor<numero progressivo>
NumericString	SV-NumericString-<numero progressivo> MV-NumericString-<numero progressivo>	sVNumericString<numero progressivo> mVNumericString<numero progressivo>
OctetString	SV-OctetString-<numero progressivo> MV-OctetString-<numero progressivo>	sVOctetString<numero progressivo> mVOctetString<numero progressivo>
OID	SV-OID-<numero progressivo> MV-OID-<numero progressivo>	sVOID<numero progressivo> mVOID<numero progressivo>
PrintableString	SV-PrintableString-<numero progressivo> MV-PrintableString-<numero progressivo>	sVPrintableString<numero progressivo> mVPrintableString<numero progressivo>
Sid	SV-Sid-<numero progressivo> MV-Sid-<numero progressivo>	sVSid<numero progressivo> mVSid<numero progressivo>
GeneralizedTime	SV-GeneralizedTime-<numero progressivo> MV-GeneralizedTime-<numero progressivo>	sVGeneralizedTime<numero progressivo> mVGeneralizedTime<numero progressivo>
UTCTime	SV-UTCTime-<numero progressivo> MV-UTCTime-<numero progressivo>	sVUTCTime<numero progressivo> mVUTCTime<numero progressivo>
AccessPointDN	SV-AccessPointDN-<numero progressivo> MV-AccessPointDN-<numero progressivo>	sVAccessPointDN<numero progressivo> mVAccessPointDN<numero progressivo>
DN	SV-DN-<numero progressivo> MV-DN-<numero progressivo>	sVDN<numero progressivo> mVDN<numero progressivo>
DNWithBinary	SV-DNWithBinary-<numero progressivo> MV-DNWithBinary-<numero progressivo>	sVDNWithBinary<numero progressivo> mVDNWithBinary<numero progressivo>
DNWithString	SV-DNWithString-<numero progressivo> MV-DNWithString-<numero progressivo>	sVDNWithString<numero progressivo> mVDNWithString<numero progressivo>
ORName	SV-ORName-<numero progressivo> MV-ORName-<numero progressivo>	sVORName<numero progressivo> mVORName<numero progressivo>
PresentationAddress	SV-PresentationAddress-<numero progressivo> MV-PresentationAddress-<numero progressivo>	sVPresentationAddress<numero progressivo> mVPresentationAddress<numero progressivo>
ReplicaLink	SV-ReplicaLink-<numero progressivo> MV-ReplicaLink-<numero progressivo>	sVReplicaLink<numero progressivo> mVReplicaLink<numero progressivo>

Creato l'attributo possiamo inserirlo all'interno della classe.

Clicchiamo sulla classe quindi **Properties** nella sezione **Attributes**, notiamo che è possibile aggiungere solo attributi opzionali quindi clicchiamo su **Add** e selezioniamo l'attributo che abbiamo creato.
Quindi clicchiamo su **OK** per confermare. (vedi Figura 12)

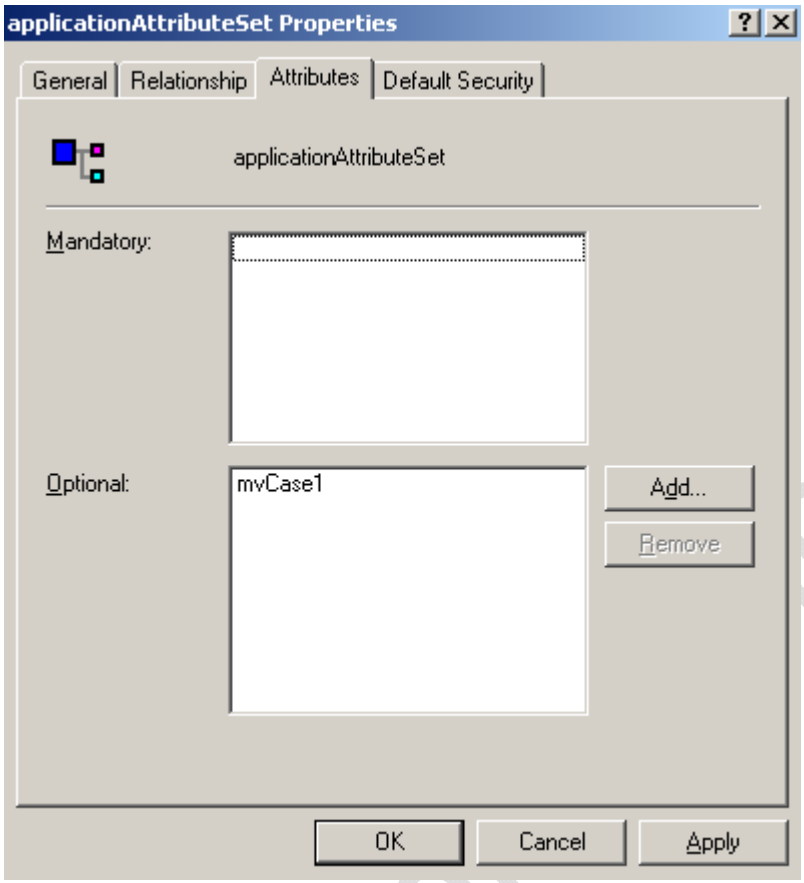

Fig.12

A questo punto dobbiamo cominciare a creare l'albero per questa classe.
Quindi andiamo nella sezione **Relationship** e nei **Possibile Superior** inseriamo la classe alla quale vogliamo rendere visibile la classe che abbiamo creato, inoltre inseriamo la classe che abbiamo creato in maniera tale da creare la struttura ad albero partendo da essa.

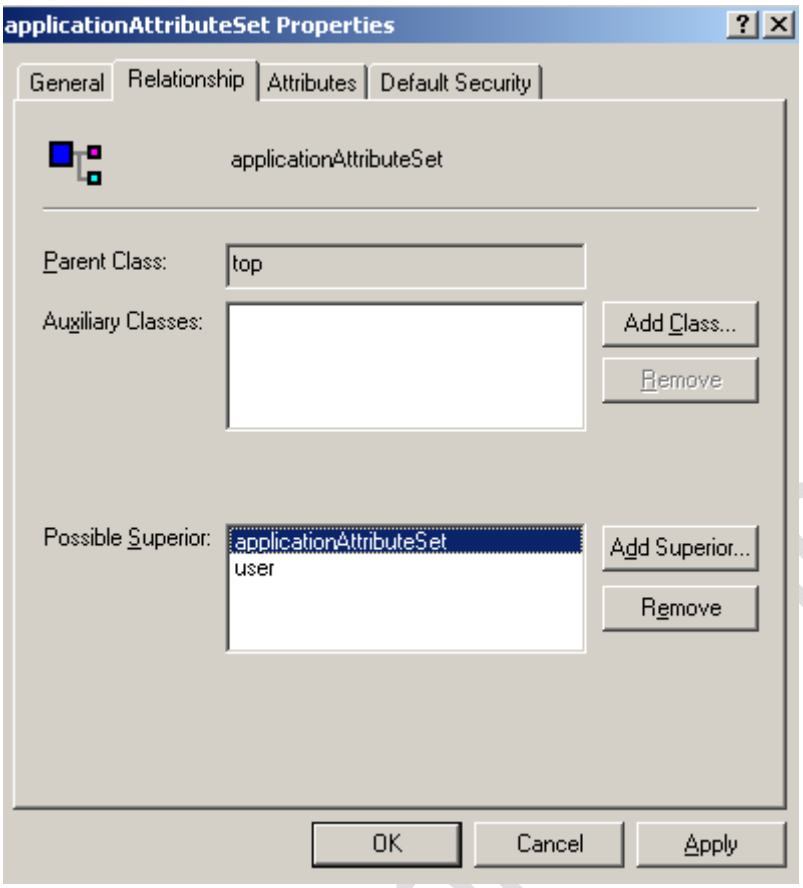

Fig.13

In questo caso abbiamo inserito la classe applicationAttributeSet che è se stessa e la classe User.
Quindi con **ADSI edit** è possibile fare quanto segue.
Apriamo **ADSI Edit** e colleghiamoci alla parition Domain come mostrato in figura 14.

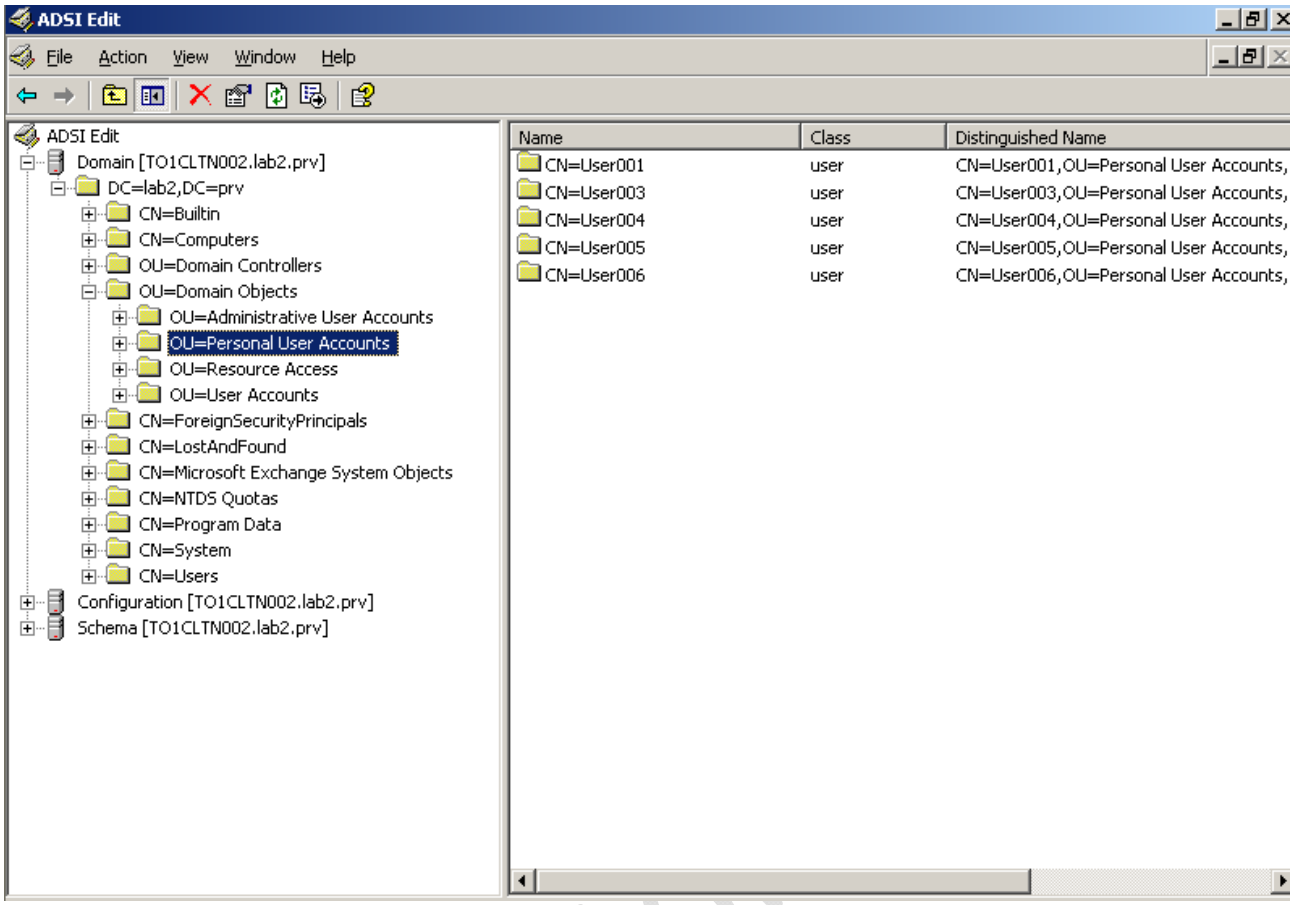

Fig.14

A questo punto sfogliamo l'albero e selezioniamo un utente del dominio.
Se clicchiamo di destro sull'utente Es.CN=User003 quindi **New** quindi **Object** noteremo che tra le classi possibili da caricare c'è anche quella precedentemente creata.

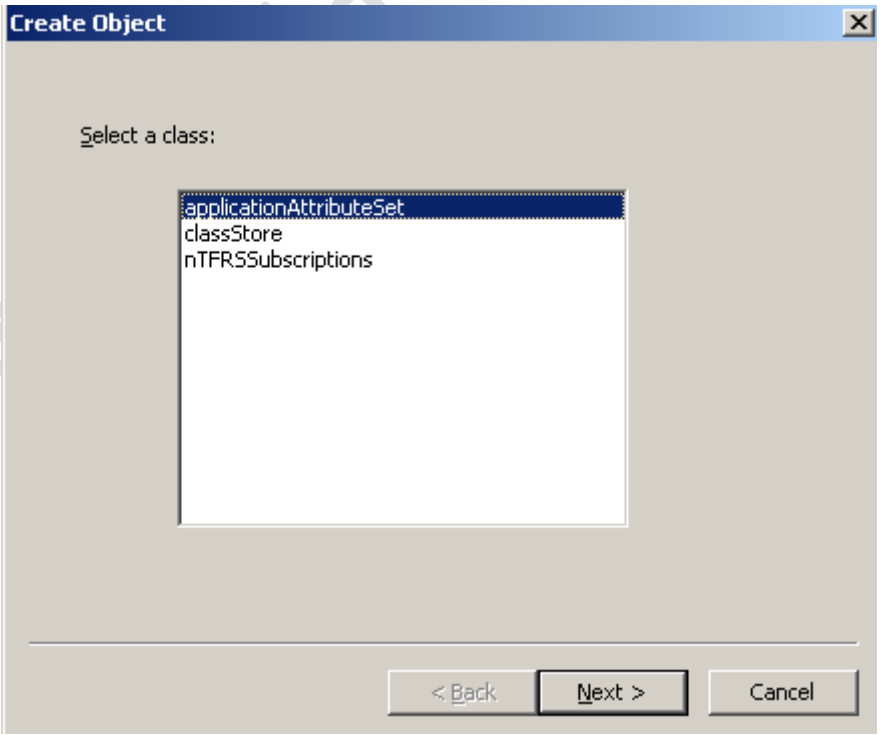

Fig.15

Selezioniamo la classe quindi clicchiamo su **Next** (figura 15)
A questo punto scriviamo il nome che intendiamo dare al CN (figura 16)

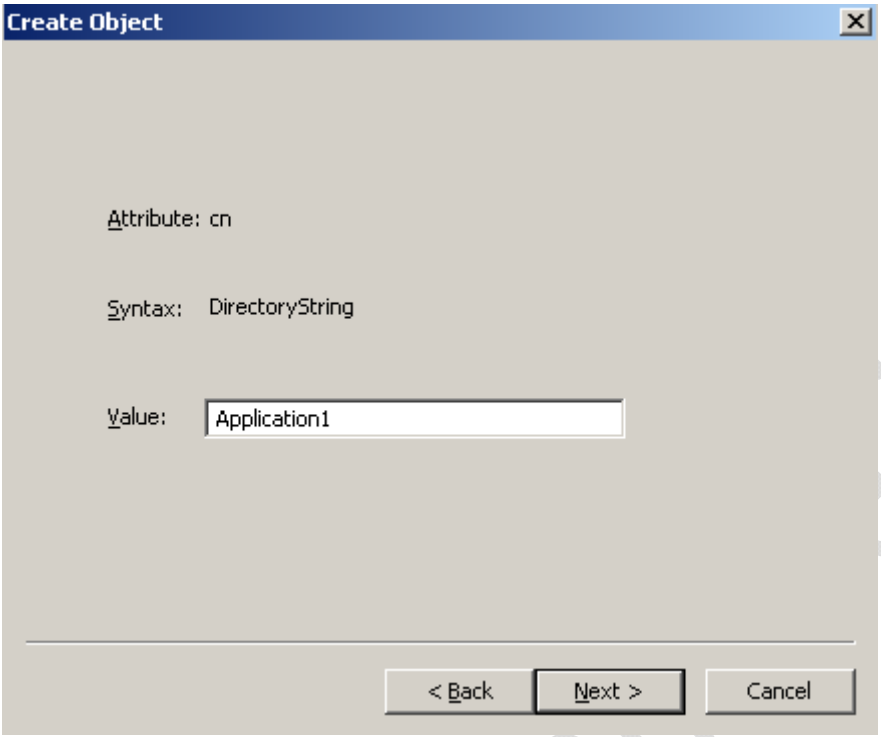

Fig.16

Quindi clicchiamo su **Next**

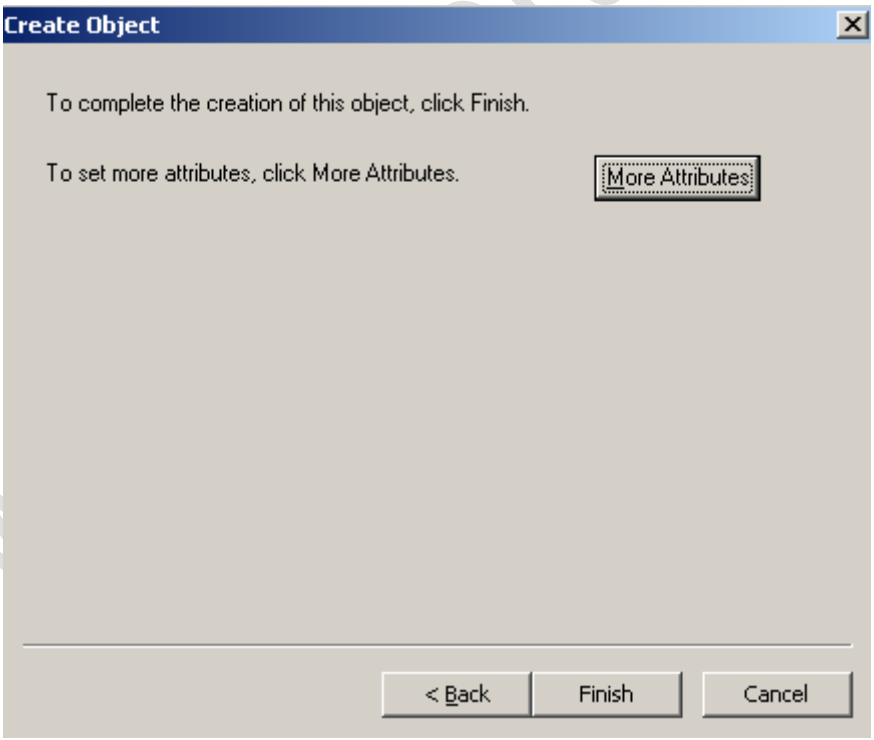

Fig.17

Quindi **Finish**

Adesso se proviamo a sfogliare l'albero noteremo che l'utente User003 ha un nuovo attributo che può essere valorizzato a nostro piacimento

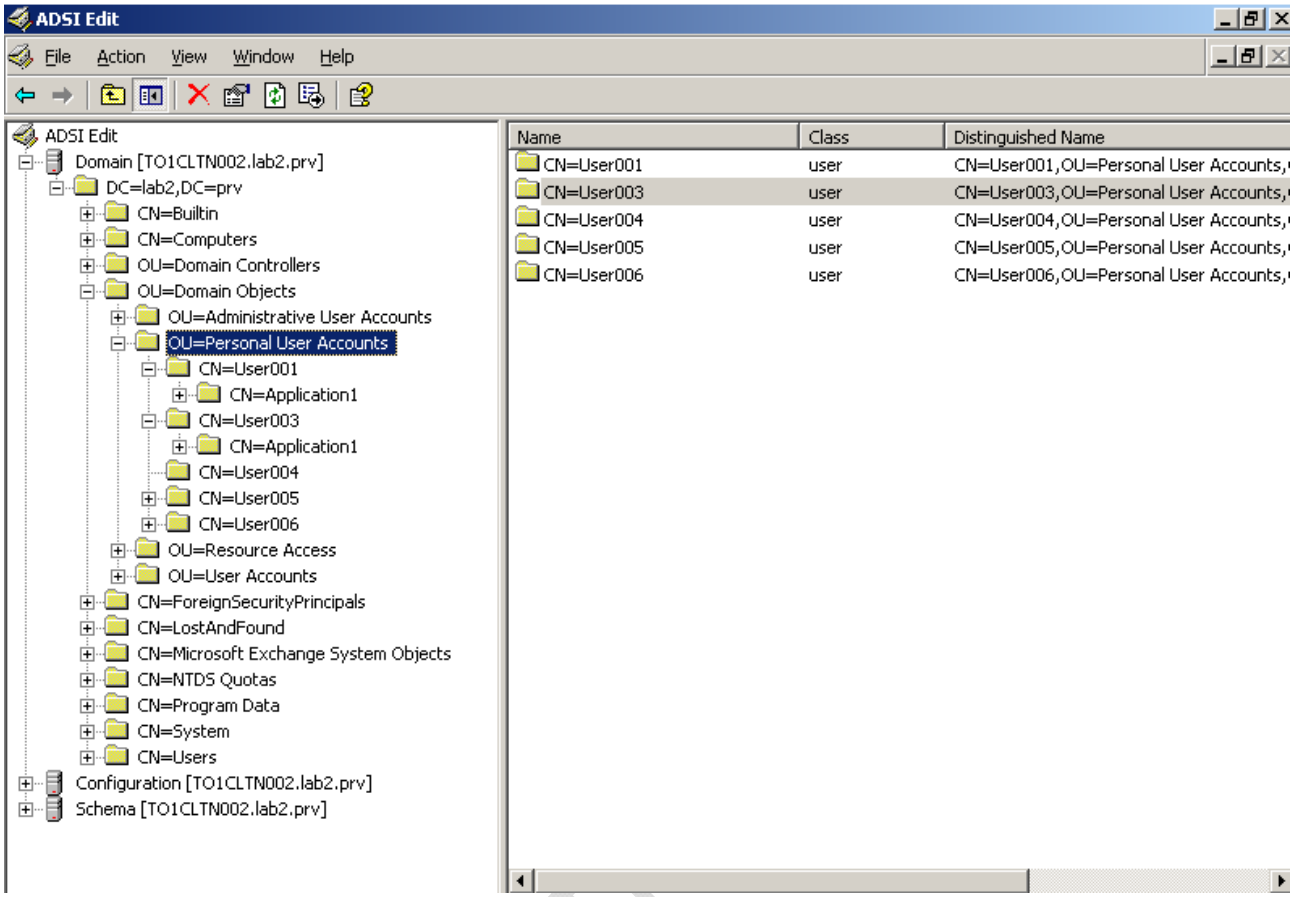

Fig.18

Naturalmente questa operazione fa fatta per tutti gli utenti a mano a meno di possedere un VBScript che faccia lo stesso lavoro ma in modo automatico.

CREARE PARTIZIONE

Per creare una partizione applicativa si può agire in due modi:

- ADSI Edit (Grafico)
- NTDSUTIL (Riga di comando)

- ADSI Edit (Grafico)

Con ADSI Edit basta lanciare l'applicativo quindi connettere la Partizione Domain. (figura 19)
Esplodere l'albero e selezionando l'attributo DC=lab2,DC=prv cliccare con tasto destro quindi New quindi Object.

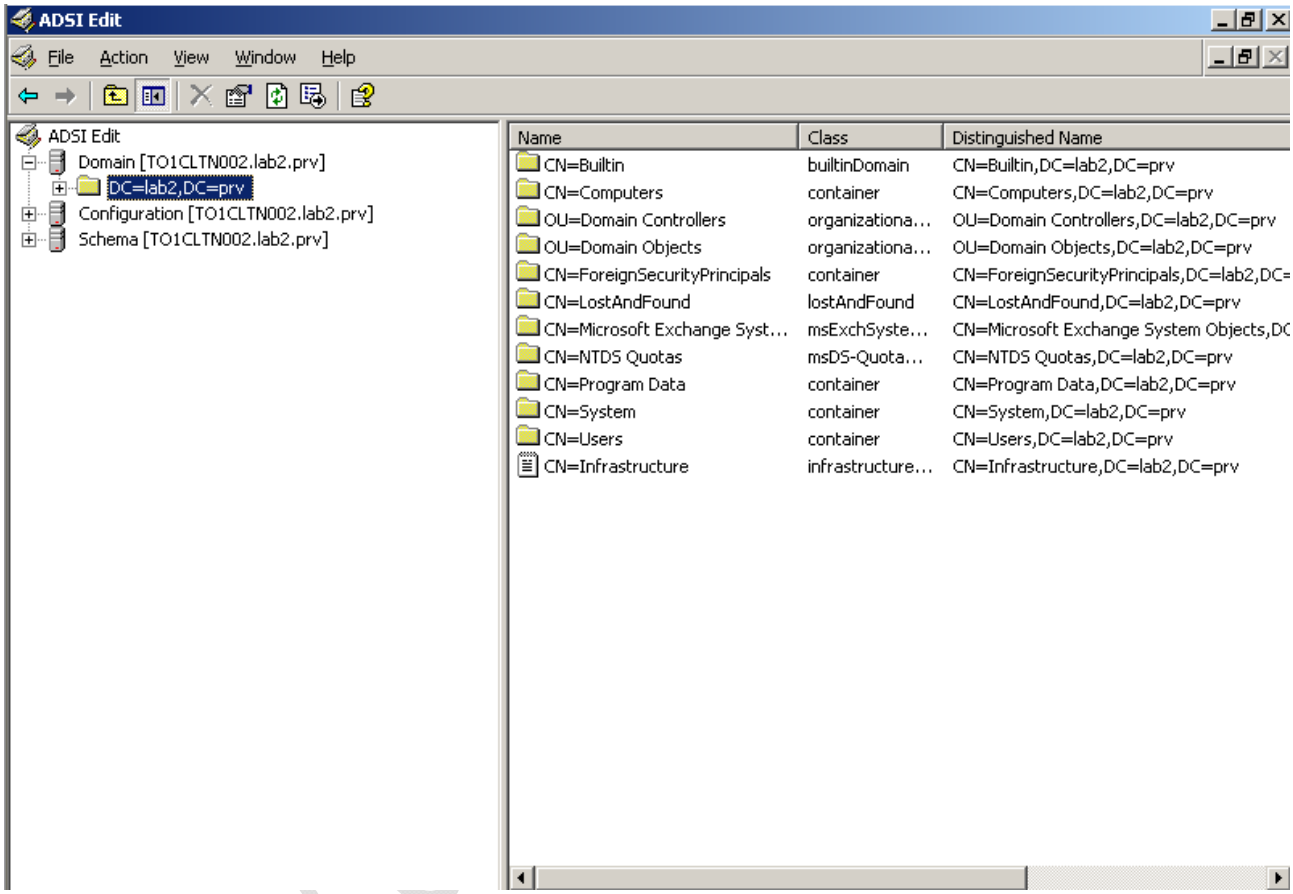

Fig.19

A questo punto ci verrà presentato una vasta scelta di oggetti da creare, quello da scegliere per la creazione di una Partizione è domainDNS come mostrato in figura 20

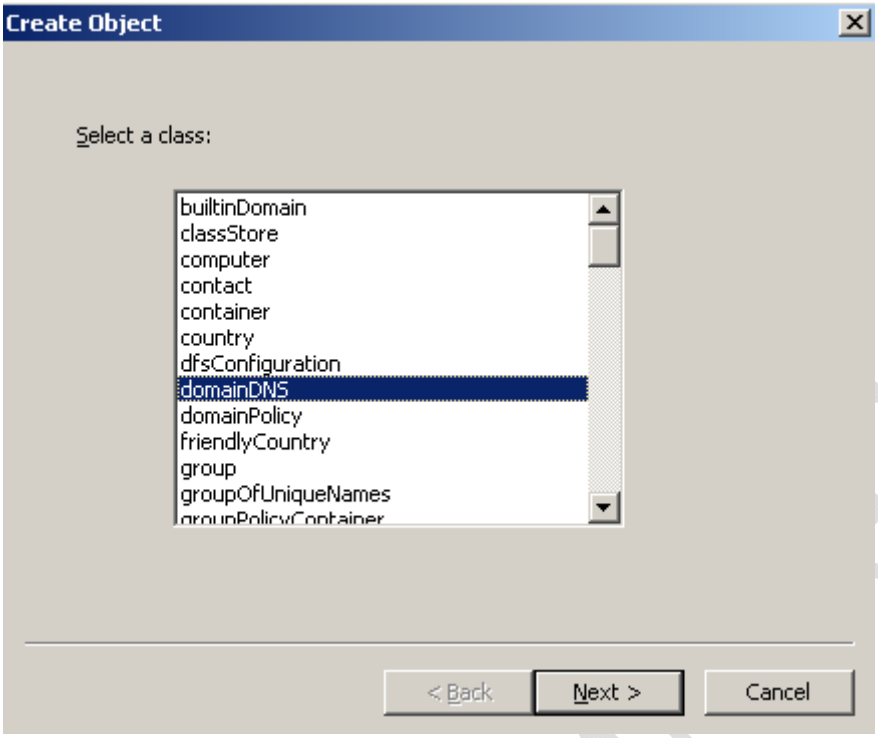

Fig.20

Selezioniamolo quindi clicchiamo su **Next**.

A questo punto inseriamo in nome DC da dare alla partizione. Es. DC=Partition1 (figura 21)

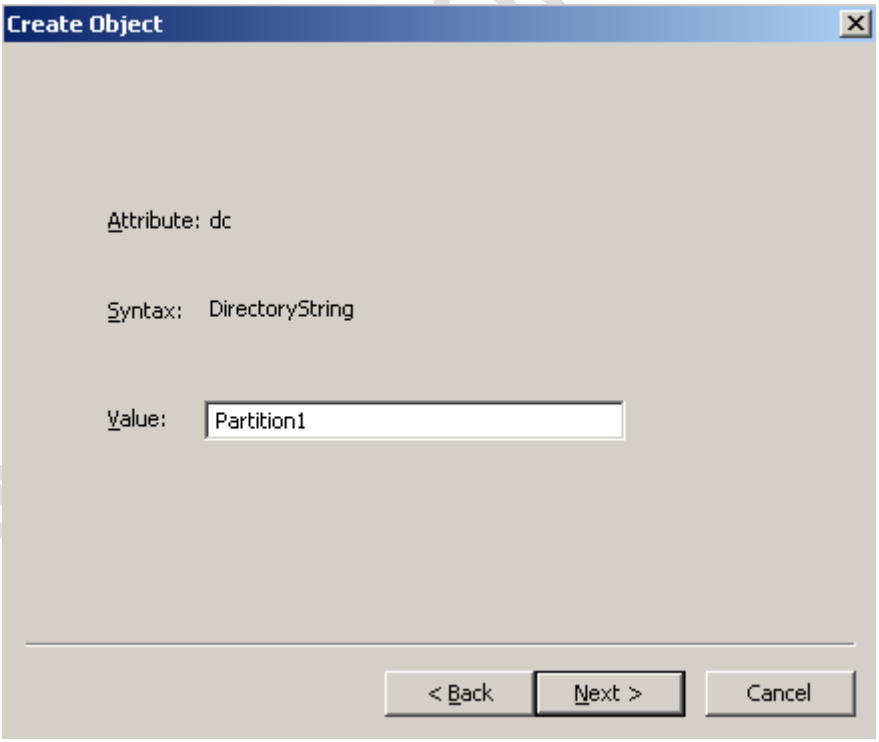

Fig.21

Clicchiamo su **Next** per proseguire

Clicchiamo su **More Attributes**

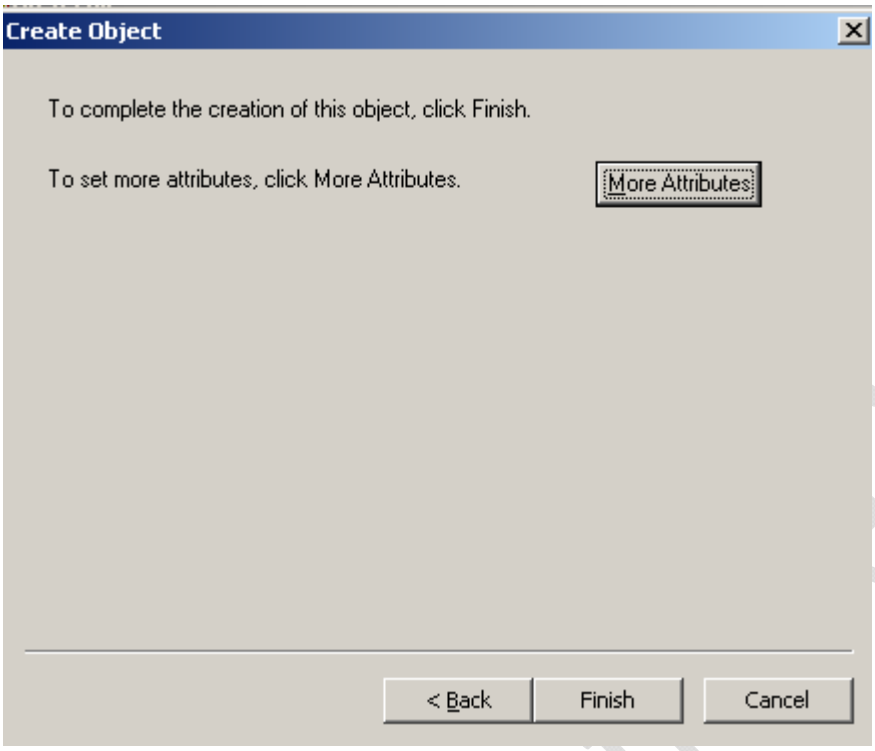

Fig.22

Selezioniamo come **Properties** : **Mandatory**, quindi **InstanceType**, in **Edit Attribute** inseriamo il valore **5** quindi clicchiamo su **Set**, quindi OK.

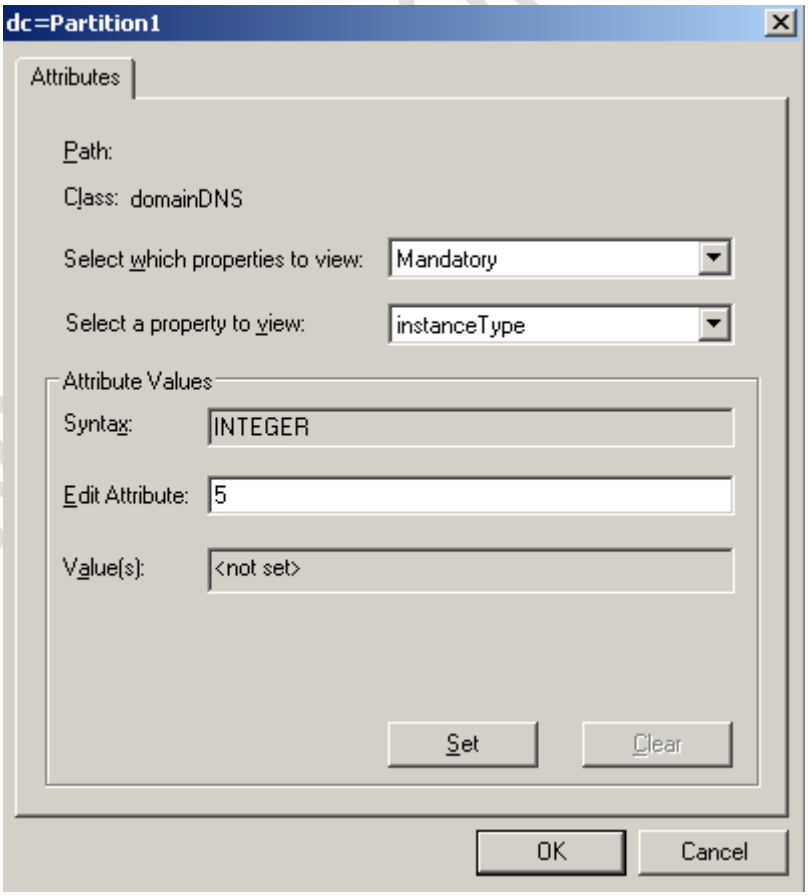

Fig.23

Clicchiamo su **Finish** per completare la creazione della partizione.

A questo punto da ADSI edit possiamo agganciare la partizione appena creata per verificarne la funzionalità

Quindi agganciamo la partizione scrivendo il seguente percorso

DC=Partition1,DC=lab2,DC=prv

Vedremo una situazione come in figura sottostante

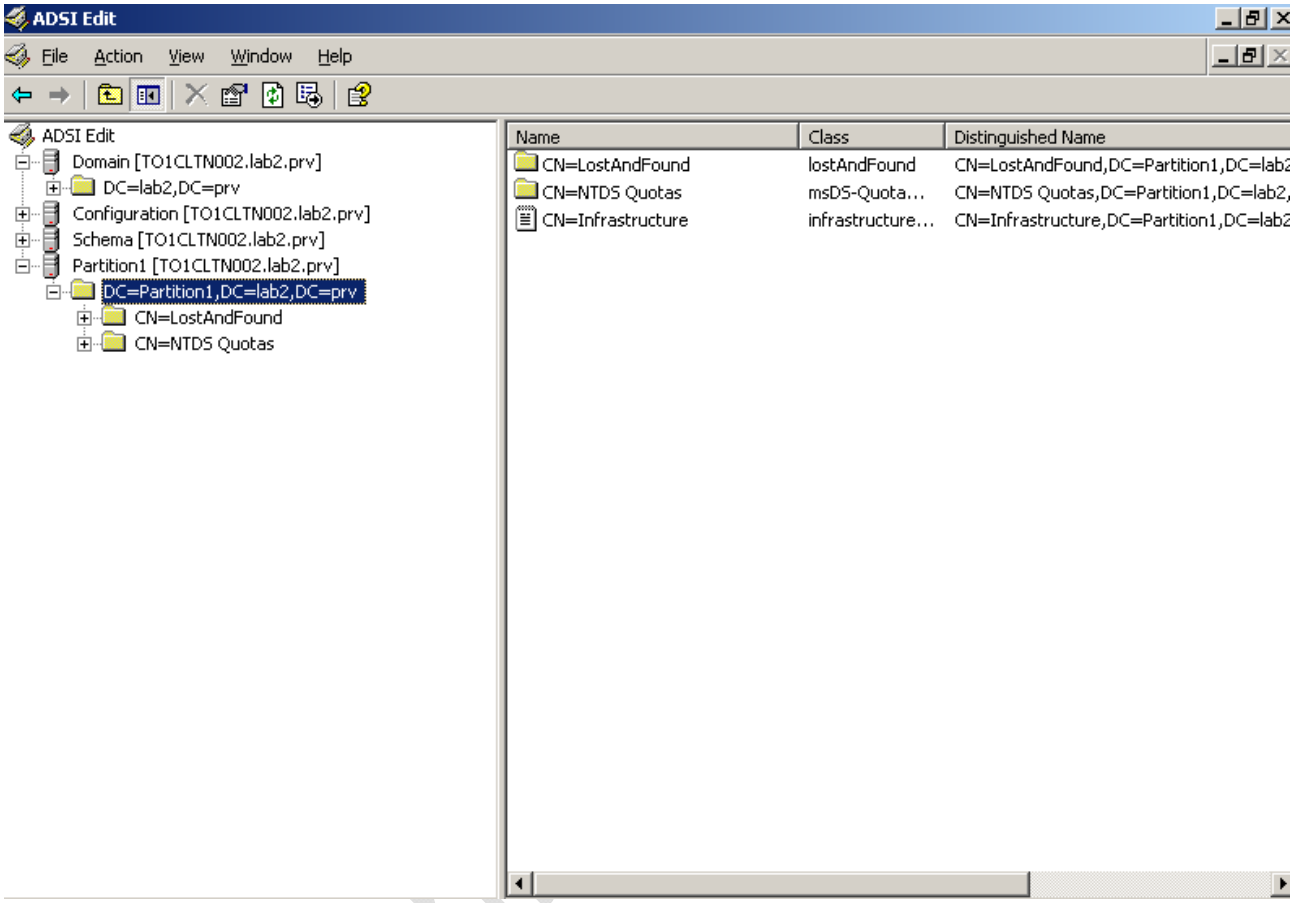

Fig.24

A questo punto all'interno della partizione è possibile inserire tutte le classi che creeremo in futuro con tutti gli attributi del caso.

NTDSUTIL (Riga di comando)

Esiste anche un metodo un po meno intuitivo am come tutti i metodi da riga di comando è sempre il più efficace e diretto.

Apriamo una command line quindi scriviamo il comando

Ntdsutil

Continuando scriviamo il comando domain management

A questo punto per poter dare comandi bisogna loggarsi.
Per loggarsi basta dare il seguente comando (Forma completa o Forma abbreviata)

connecting to server nome DNS del dominio in questione (Es: connecting to server to1nets001.lab1.prv)

co to se nome DNS del dominio in questione (Es: co to se to1nets001.lab1.prv)

Se l'autenticazione è andata a buon fine dovremmo ricevere a video il seguente messaggio

Binding to to1nets001.lab2.prv ...
Connected to to1cltn002.lab2.prv using credentials of locally logged on user.

Per la creazione della partizione basta digitare il seguente commando

create DC=Partition1,DC=lab2,DC=prv null

Se la creazione della partizione è andata a buon fine dovremmo visualizzare a video ils seguente messaggio

adding object DC=Partition2,DC=lab2,DC=prv

Adesso per una ulteriore verifica possiamo lanciare il commando list per avere la lista di tutte le partizioni presenti, dovremmo trovare anche Partition1
A video dovremmo vedere il seguente listato

Note: Directory partition names with International/Unicode characters will only display correctly if appropriate fonts and language support are loaded

Found 6 Naming Context(s)
0 - CN=Configuration,DC=lab2,DC=prv
1 - DC=lab2,DC=prv
2 - CN=Schema,CN=Configuration,DC=lab2,DC=prv
3 - DC=DomainDnsZones,DC=lab2,DC=prv
4 - DC=ForestDnsZones,DC=lab2,DC=prv
5 - DC=Partition1,DC=lab2,DC=prv

Adesso verifichiamo la replica della partizione appena creata con i Domain Controller.
Per farlo basta lanciare il seguente comando

list nc replicas DC=Partition2,DC=lab2,DC=prv

Dovremmo avere a video le seguenti righe

The application directory partition DC=Partition2,DC=lab2,DC=prv's Replicas are:

CN=NTDS Settings,CN=TO1NETS001,CN=Servers,CN=AUGUSTA,CN=Sites,CN=Configu
ration,DC=lab2,DC=prv

Per far si che la partizione creata si replichi anche con altri domain controller basterà eseguire ils seguente comando

add nc replica DC=Partition2,DC=lab2,DC=prv nome DNS del domain controller
(ES: add nc replica DC=Partition2,DC=lab2,DC=prv to1nets002.lab2.prv)

A questo punto se riprovate a lanciare il commando

list nc replicas DC=Partition2,DC=lab2,DC=prv

diovreste avere una situazione del genere
The application directory partition DC=Partition2,DC=lab2,DC=prv's Replicas are:

CN=NTDS Settings,CN=TO1NETS001,CN=Servers,CN=AUGUSTA,CN=Sites,CN=Configu

ration,DC=lab2,DC=prv

CN=NTDS Settings,CN=TO1NETS002,CN=Servers,CN=AUGUSTA,CN=Sites,CN=Configu
ration,DC=lab2,DC=prv