SANGFOR

IAM

Petunjuk LDAP Sync POC

Versi 4.0

Daftar Isi

Bab 1 Instruksi LDAP Sync POC

Untuk LDAP synchronization policy, ada dua mode sinkronisasi: [Sync by OU] dan [Sync by security group (AD domain only)]. Fitur dan fungsinya masing-masing dijelaskan dalam bagian berikut.

Untuk menyinkronkan user, Organization Unit [OU], atau security group dari server LDAP ke perangkat IAM. pertama. Anda perlu melakukan konfigurasi synchronization policy agar mereka akan disinkronkan sesuai dengan pengaturan policy.

1.1 Sync by OU

Mode [Sync by OU] berlaku untuk semua jenis server LDAP. Dengan mode ini. OU di server LDAP akan disinkronkan dalam bentuk user group ke perangkat IAM dan struktur organisasi OU disinkronkan dengan cara yang sama. memastikan bahwa pengguna masih termasuk dalam grup yang sesuai setelah sinkronisasi.

1.2 Sync by security group (AD domain only)

Mode [Sync by security group (AD domain only)] hanya berlaku untuk server LDAP Microsoft, yang adalah, domain AD. Dengan mode ini, security group pada server domain AD akan disinkronkan dalam bentuk user group ke perangkat IAM. Dikarenakan security group tidak memiliki struktur organisasi, semua security group akan berada pada tingkat yang sama setelah sinkronisasi ke perangkat IAM.

Bab 2 Persiapan

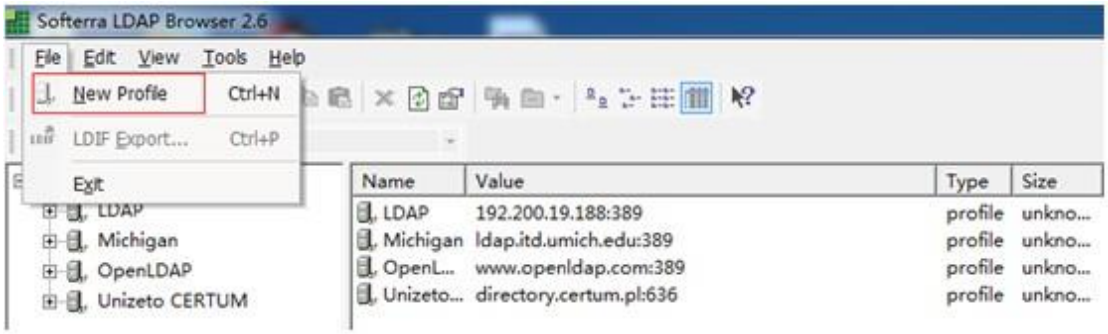
- Perangkat IAM4.0, Sinkronisasi LDAP dapat bekerja pada semua jenis penerapan, cukup konfirmasi bahwa IAM dapat berkomunikasi dengan server LDAP.
- Harap patch KB di bawah ini terlebih dahulu:
- /cms/a/lAM/Troubleshooting/2013/0926/107.html
- Siapkan PC yang sudah terinstall software browser LDAP.
- Pastikan kebutuhan costumer: apakah dia ingin sinkronisasi Sync by OU atau Sync by Security Group?
- Domain user yang memiliki wewenang untuk menelusuri semua struktur organisasi domain.

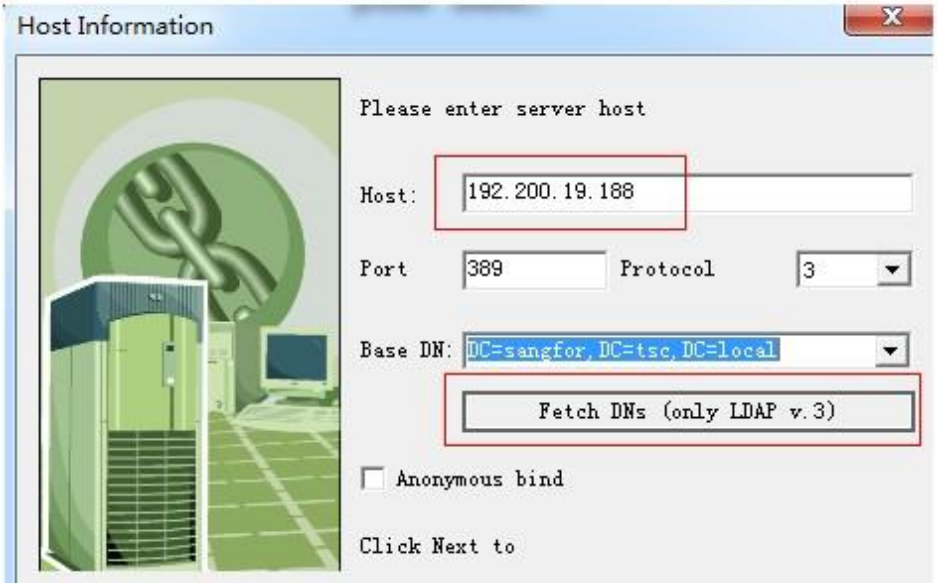
Bab 3 Hasil yang diharapkan

yaitu bisa sinkronisasi semua domain user dan organisasi ke IAM

3.1 Langkah Konfigurasi

3.1.1Gunakan LDAP browser untuk mendapatkan informasi domain



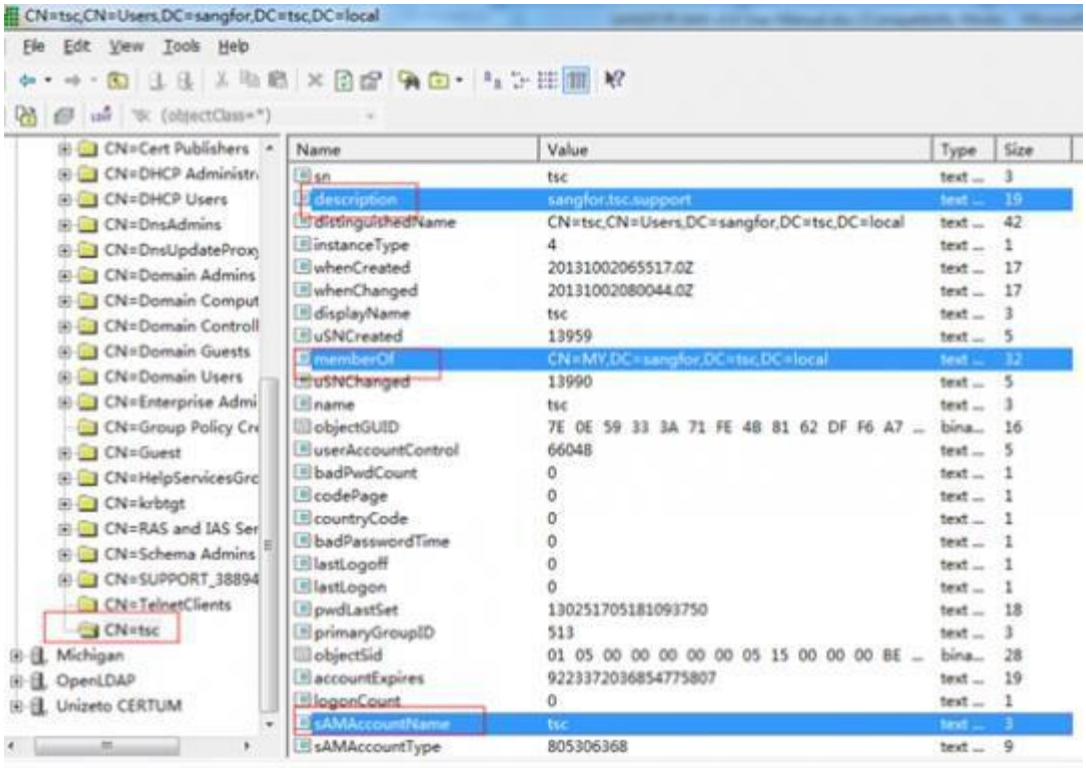


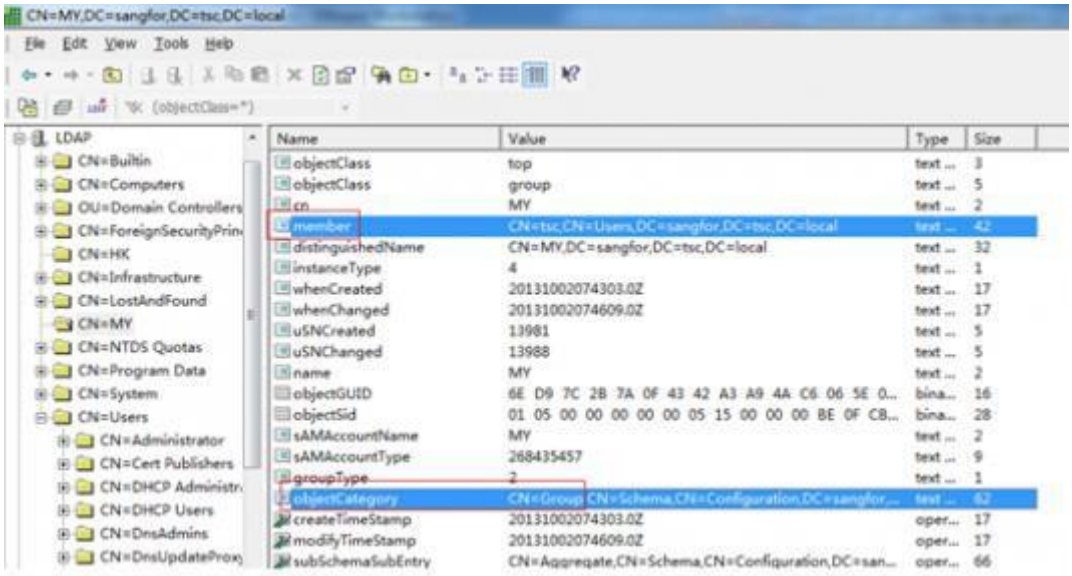
Mengapa kita harus melakukan ini?

Tujuan 1 : untuk konfirmasi bahwa user memiliki wewenang untuk menelusuri struktur organizasi domain

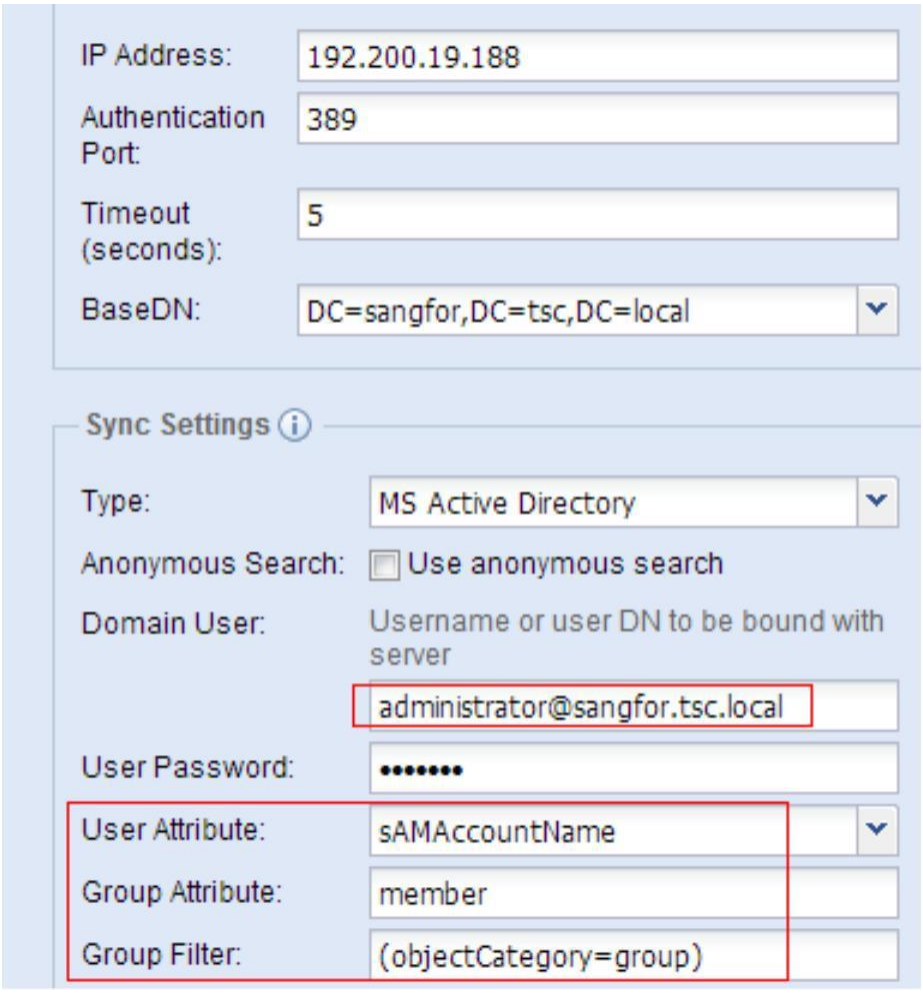
Tujuan 2:

Seperti yang ditunjukkan gambar dibawah:kita dapat mengetahui user "tsc" , user atribut " sAMAccountName ", dan deskripsi atributnya "description", Atribut grup yaitu "member" dan Filter Grup





3.1.2Menambah server LDAP

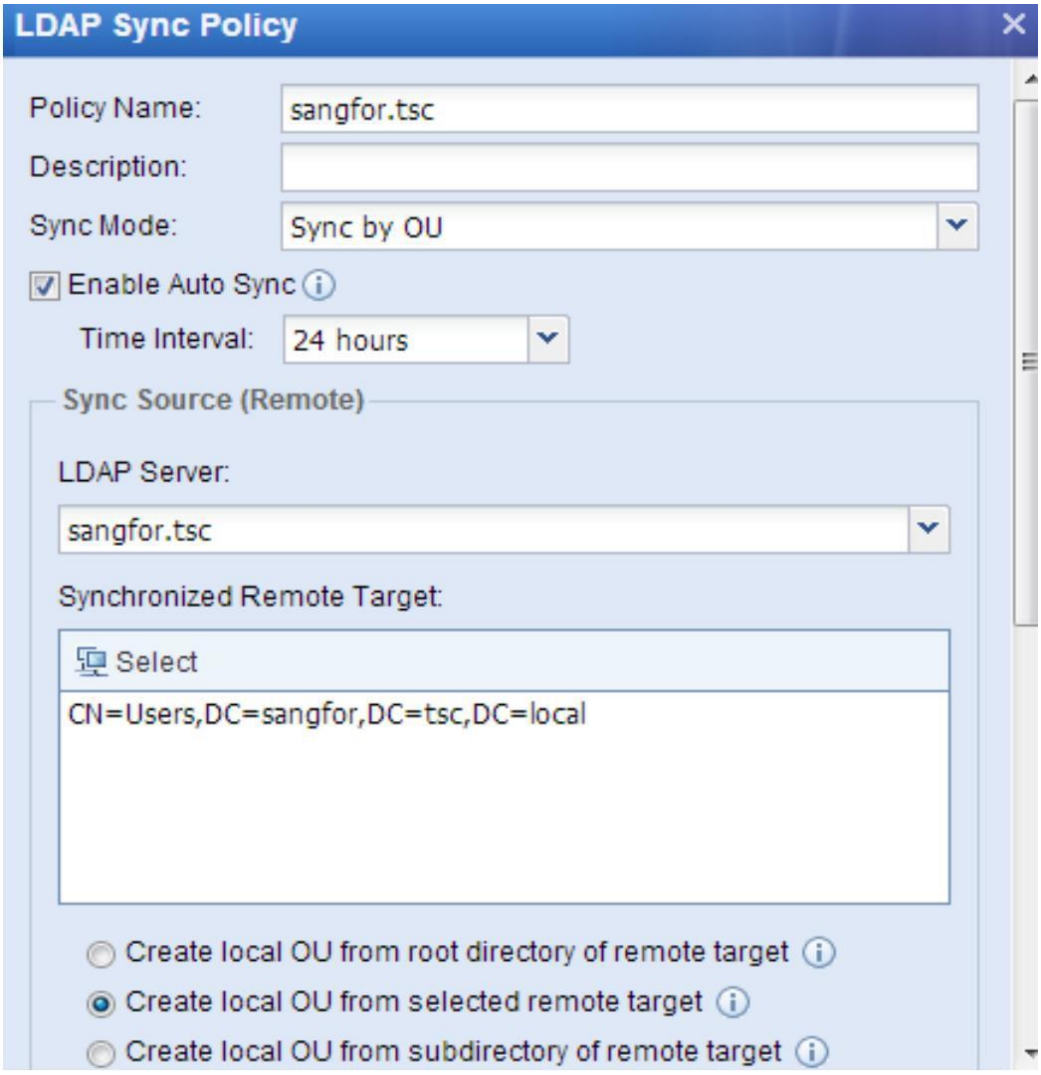


Perlu diketahui, jika jenis servernya adalah MS Active Director, kita tidak perlu

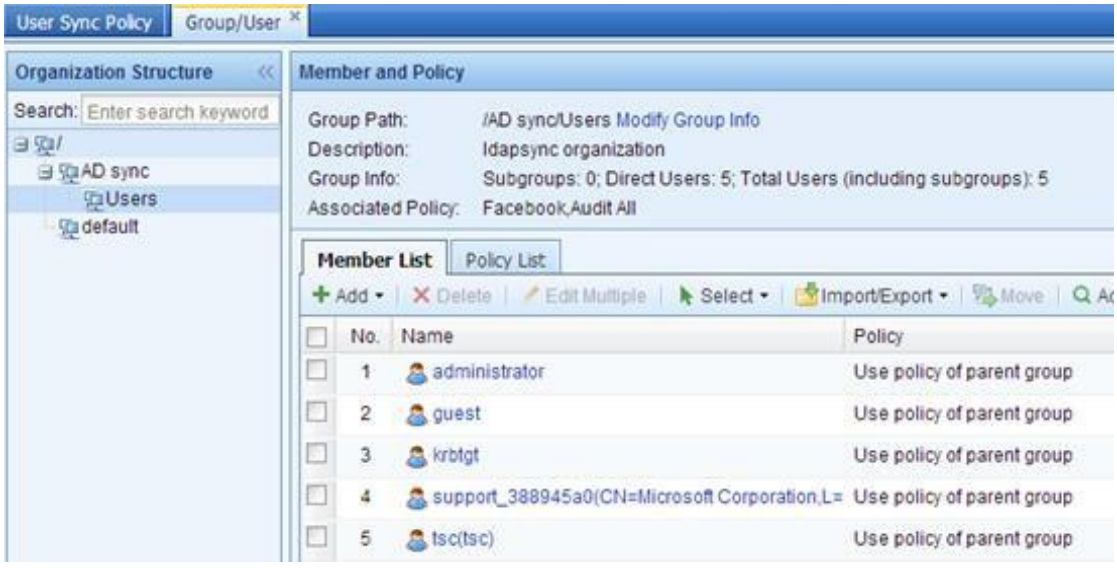
mengubah apa pun, cukup gunakan konfigurasi default. Jika jenis server yang lain, mungkin kita perlu menggunakan LDAP Browser untuk memastikan semua atribut sama dengan server.

3.1.3User Sync Policy

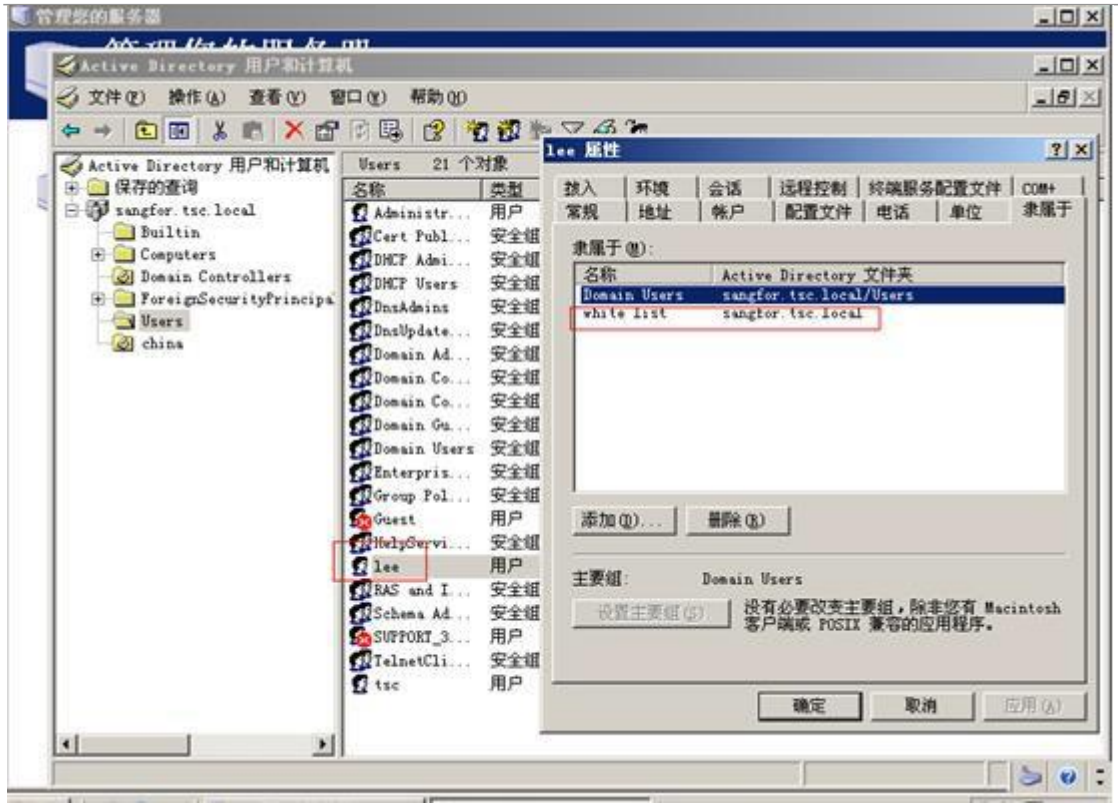
Synchronize by OU

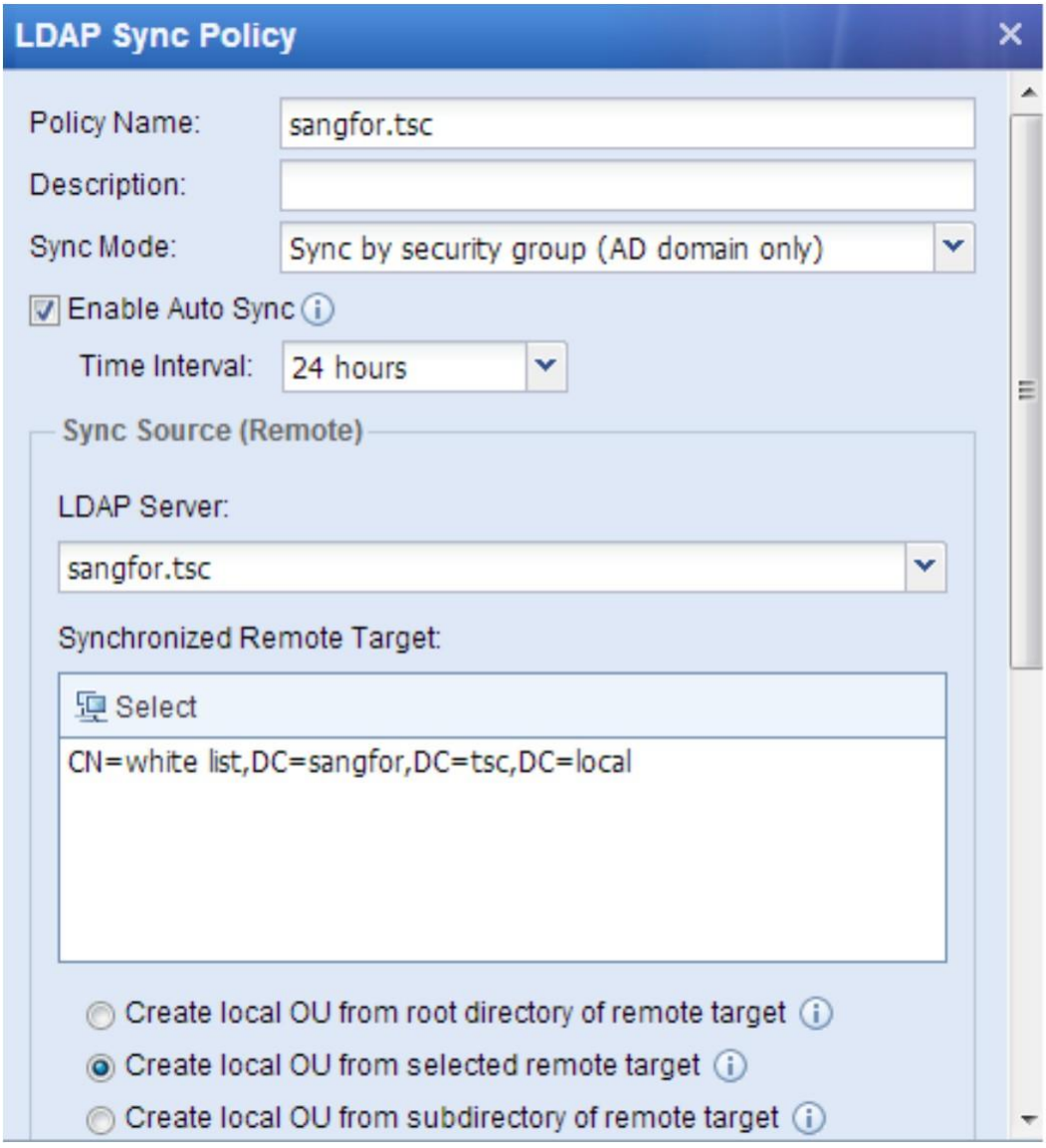


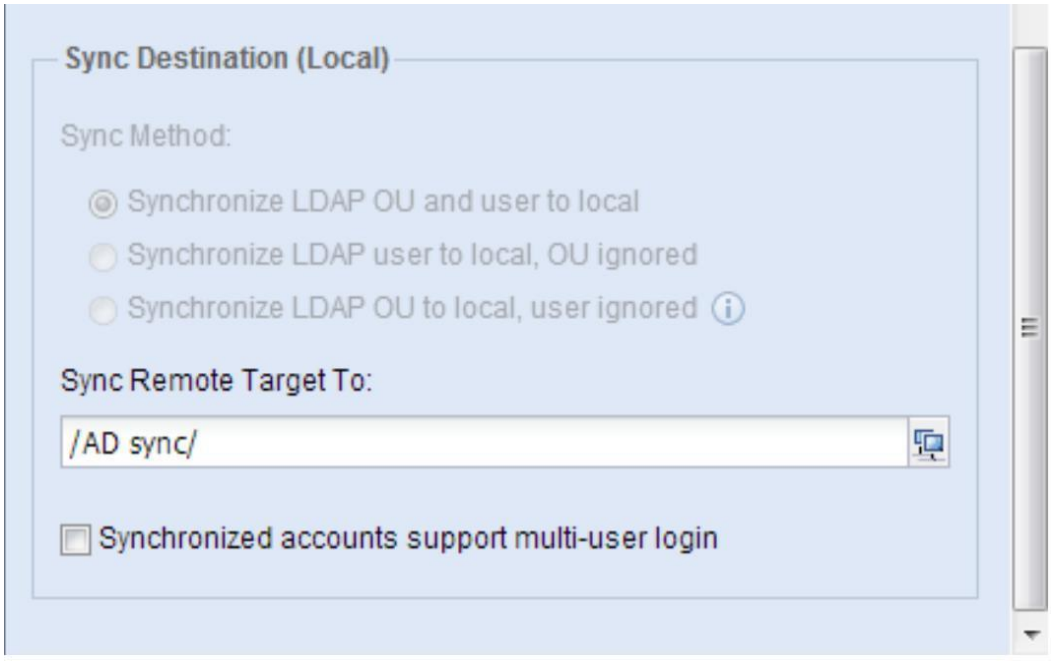
3.1.4Hasil



Synchronize by Security Group (AD Domain Only) :


管理您的服务器
Active Directory 用户和计算机
文件(F) 操作(A) 查看(V) 窗口(W) 帮助(H)
Active Directory 用户和计算机
保存的查询
sangfor.tsc.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipa
Users
china
Users 21 个对象
名称 类型
Administr... 用户
Cert Publ... 安全组
DHCP Admi... 安全组
DHCP Users 安全组
DnsAdmins 安全组
DnsUpdate... 安全组
Domain Ad... 安全组
Domain Co... 安全组
Domain Co... 安全组
Domain Gu... 安全组
Domain Users 安全组
Enterpris... 安全组
Group Pol... 安全组
Guest 用户
HelpServi... 安全组
lee 用户
RAS and I... 安全组
Schema Ad... 安全组
SUPPORT_3... 用户
TelnetCli... 安全组
tsc 用户
lee 属性
拨入 环境 会话 远程控制 终端服务配置文件 COM+
常规 地址 帐户 配置文件 电话 单位 隶属于
隶属于(M):
名称 Active Directory 文件夹
Domain Users sangfor.tsc.local/Users
white list sangfor.tsc.local
添加(D)... 删除(R)
主要组: Domain Users
设置主要组(S) 没有必要改变主要组，除非您有 Macintosh 客户端或 POSIX 兼容的应用程序。
确定 取消 应用(A)


LDAP Sync Policy
Policy Name: sangfor.tsc
Description:
Sync Mode: Sync by security group (AD domain only)
Enable Auto Sync
Time Interval: 24 hours
Sync Source (Remote)
LDAP Server:
sangfor.tsc
Synchronized Remote Target:
Select
CN=white list,DC=sangfor,DC=tsc,DC=local
Create local OU from root directory of remote target
Create local OU from selected remote target
Create local OU from subdirectory of remote target


Sync Destination (Local)
Sync Method:
Synchronize LDAP OU and user to local
Synchronize LDAP user to local, OU ignored
Synchronize LDAP OU to local, user ignored
Sync Remote Target To:
/AD sync/
Synchronized accounts support multi-user login

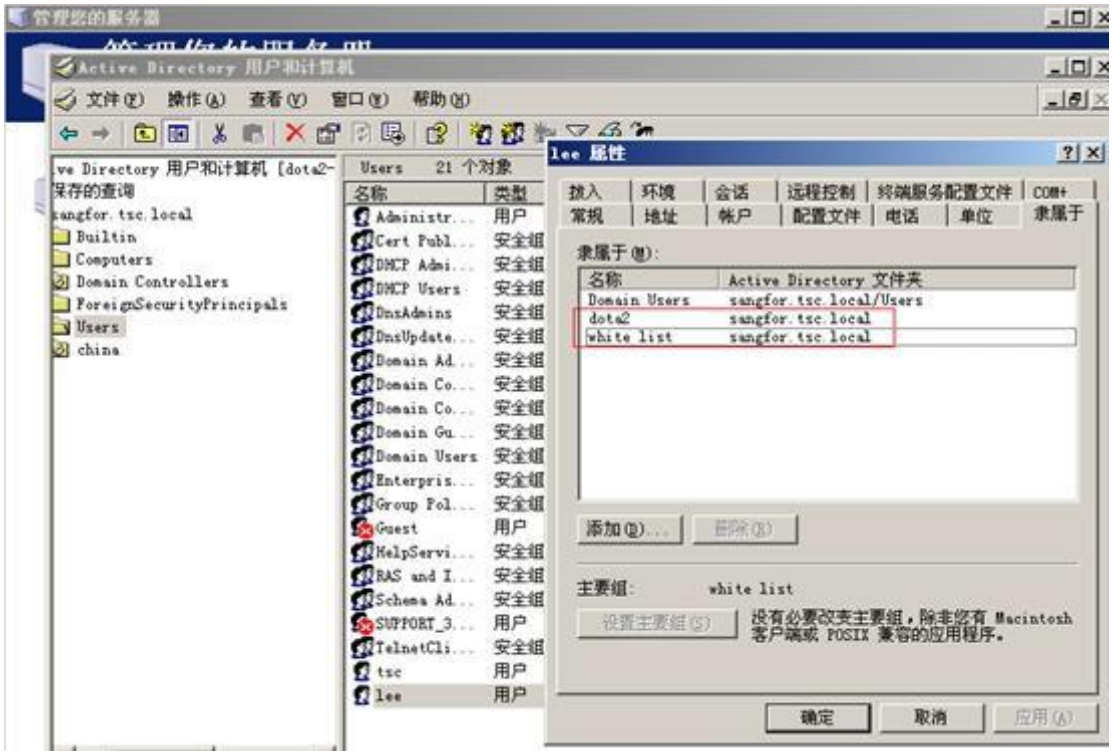
Hasil seperti yang ditunjukkan pada gambar dibawah

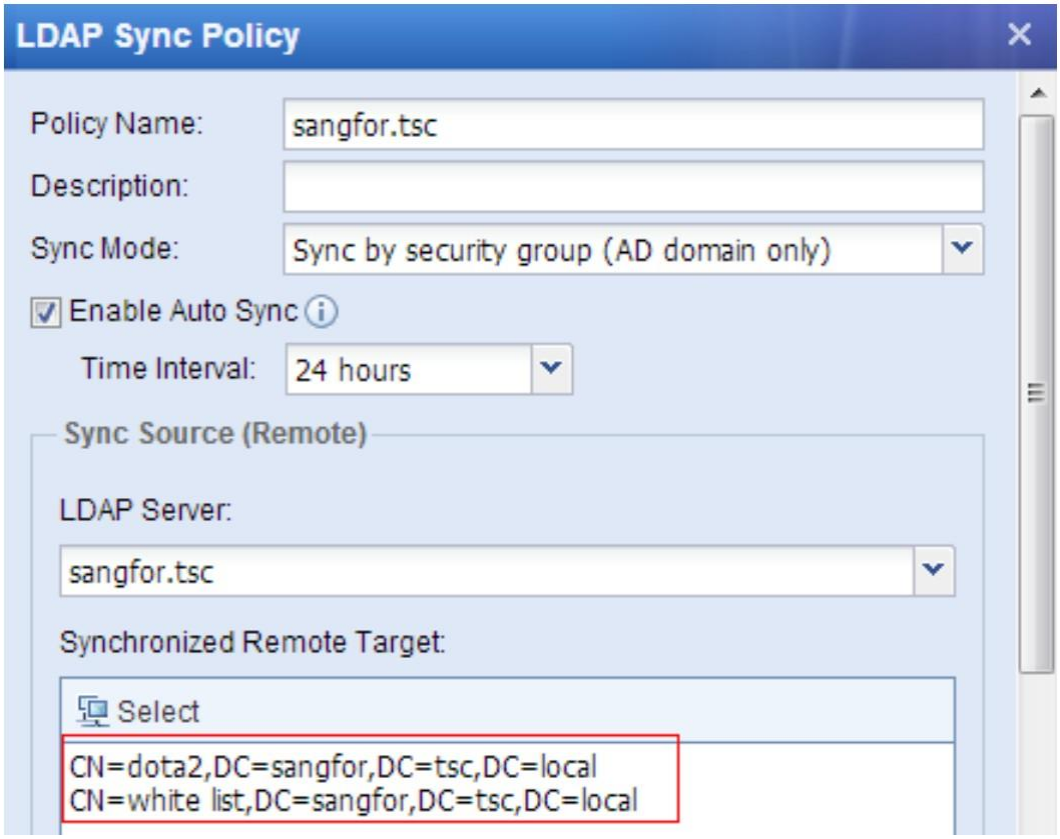
Perlu diketahui: Seperti yang dtunjukkan pada gambar, jika lee milik dua security group "dota2" dan "white list", bagaimana dengan hasil sinkronisasi?

Hasil:

Perhatikan: jika pelanggan ingin IAM mendukung sinkronisasi Multi-security group, Silakan kirim theappvension dan /etc/hwinfo ke CTI dan tanyakan costumize patch.

lAM tidak dapat menyinkronkan user yang hanya milik security group pada "Domain Users"





Bab 4 Troubleshooting

1. Pastikan Anda dapat telnet server tcp 389 port OK.
2. Gunakan browser LDAP untuk mengkonfirmasi atribut.
3. IAM hanya dapat mendukung sinkronisasi 65535 jumlah user dan maksimum OU import depth adalah 16 adalah.

4. IAM tidak mendukung StrongAuthRequired, kamu bisa mengkonfirmasi ini dengan tcpdump packets.

1. Tcpdump -i eth0 host iam ip dan ldap server ip and port 389 -50 -w /tmp/ ldap.cap
2. /etc/init.d/syncusrd stop
3. Klik sync now, tunggu sebentar sampai sinkronisasi gagal (sync failed)
4. Kirim ldap.cap dan /var/log/ldpsync.log ke CTI
5. /etc/init.d/syncusrd start
6. Ketika IAM sinkronisasi LDAP OU ke root group, dia akan secara otomatis menghapus users yang bukan domain user.

“Default setting adalah root group”

Solusi:

Buat grup utuk AD pada group/user dan sinkronkan salah satu target ke sebuah grup selain dari root group "/"

7. Kode Error

Error Code	Error	Deskripsi
0	LDAP_SUCCESS	Indikasi bahwa operasi klien yang diminta berhasil
1	LDAP_OPERATIONS_ERROR	Indikasi kesalahan internal. Server tidak dapat menanggapi error yang spesifik dan juga tidak dapat menanggapi permintaan dengan benar. Ini tidak menunjukkan bahwa klien telah mengirim kesalahan pesan. di N05 8.3x sampai NDS 7.xx. 'ini adalah kesalahan default untuk NDS error 'yang tidak dipetakan ke kode kesalahan LDAP. 'Untuk menyesuaikan dengan draf LDAP baru, NDS ‘8.5 menggunakan 80 [0x50] untuk kesalahan tersebut.

2	LDAP_PROTOCOL_ERROR	Indikasi bahwa server telah menerima permintaan yang invalid dari klien.
3	LDAP_TIMELIMIT_EXCEEDED	Indikasikan waktu operasi yang ditentukan baik oleh klien ataupun server telah melewati batas. Pada pencarian operasi, akan didapatkan incomplete return.
4	LDAP_SIZELIMIT_EXCEEDED	Indikasikan ada operasi pencarian, batas size yang ditentukan oleh klien atau server telah melewati batas. Hasil yang didapat nantinya adalah incomplete return.
5	LDAP_COMPARE_FALSE	Tidak mengindikasikan kondisi error. Indikasi bahwa hasil operasi perbandingan salah
6	LDAP_COMPARE_TRUE	Tidak mengindikasikan kondisi error. Indikasi bahwa hasil operasi perbandingan benar
7	LDAP_AUTH_METHOD_NOT_SUPPORTED	Indikasikan bahwa pada operasi pentautan yang klien minta, metode autentikasi tidak didukung oleh server LDAP
8	LDAP_STRONG_AUTH_REQUIRED	Indikasikan salah satu dari berikut: pada permintaan pentautan, server LDAP hanya menerima autentikasi kuat. Pada permintaan klien, klien meminta operasi seperti penghapusan yang membutuhkan autentikasi kuat. Pada pemberitahuan pemutusan, server LDAP menemukan keamanan yang menjaga komunikasi antara klien dan server tanpa disadari telah gagal
9		Reserved.
10	LDAP_REFERRAL	Tidak mengindikasikan kondisi error. Pada LDAPv3, mengindikasikan bahwa server tidak memiliki tujuan entry permintaan, tetapi mungkin tedapat pada referral field.
11	LDAP_ADMINLIMIT_EXCEEDED	Mengindikasikan bahwa kapasitas server LDAP yang diatur otoritas admin telah terlampaui

12	LDAP_UNAVAILABLE_CRITICAL_EXTENSION	Indikasikan server LDAP tidak dapat memenuhi permintaan karena satu atau beberapa ekstensi tidak tersedia. Baik itu server yang tidak mendukung atau kontrol yang tidak sesuai dengan jenis operasi.
13	LDAP_CONFIDENTIALITY_REQUIRED	Indikasikan bahwa sesi tidak ada proteksi protokol seperti Transport Layer Security (TLS), yang menyediakan kerahasiaan server.
14	LDAP_SASL_BIND_IN_PROGRESS	Tidak mengindikasikan kondisi error, tetapi server siap untuk proses selanjutnya. Klien harus mengirim mekanisme SASL yang sama ke server untuk melanjutkan proses
15		Tidak digunakan
16	LDAP_NO_SUCH_ATTRIBUTE	Indikasikan atribut yang ditentukan pada operasi modify atau compare tidak terdapat pada entry
17	LDAP_UNDEFINED_TYPE	Indikasikan atribut yang ditentukan pada operasi modify atau add tidak terdapat pada skema server LDAP
18	LDAP_INAPPROPRIATE_MATCHING	Indikasikan bahwa matching rule yang ditentukan pada filter pencarian tidak sesuai dengan rule yang sudah ditetapkan pada syntax atribut
19	LDAP_CONSTRAINT_VIOLATION	Mengindikasikan nilai atribut pada operasi modify, add, atau modify DN melanggar batasan yang ditetapkan pada atribut. batasan ini bisa berupa size ataupun konten (hanya string, tanpa binary)
20	LDAP_TYPE_OR_VALUE_EXISTS	Mengindikasikan nilai atribut yang ditentukan pada operasi modify atau add sudah tersedia sebagai nilai atau atribut itu
21	LDAP_INVALID_SYNTAX	Mengindikasikan nilai atribut yang ditentukan pada operasi add, compare, atau modify tidak teratur atau salah syntax pada atribut
22-31		Tidak digunakan
32	LDAP_NO_SUCH_OBJECT	Mengindikasikan objek target tidak ditemukan. Kode ini tidak terdapat pada operasi berikut: operasi pencarian search base

		entri manapun yang sesuai dengan filter pencarian operasi bind.
33	LDAP_ALIAS_PROBLEM	Indikasikan bahwa error terjadi ketika alias dereferensi
34	LDAP_INVALID_DN_SYNTAX	Indikasikan bahwa syntax DN tidak benar. Jika syntax benar, tapi struktur peraturan server LDAP tidak mengizinkan operasi, maka server akan memberikan pesan LDAP_UNWILLING _TO_PERFORM.)
35	LDAP_IS_LEAF	Indikasikan bahwa operasi tertentu tidak bisa dilakukan pada entri leaf. (Kode ini belum tersedia pada spesifikasi LDAP, tetapi tersimpan untuk situasi ini.
36	LDAP_ALIAS_DEREF_PROBLEM	Indikasikan bahwa selama operasi pencarian, baik itu klien tidak memiliki wewenang untuk melihat nama objek atau dereferensi tidak diperbolehkan
37-47		Tidak digunakan
48	LDAP_INAPPROPRIATE_AUTH	Indikasikan selama proses bind, klien berusaha untuk menggunakan metode autentikasi yang klien tidak bisa gunakan dengan tepat. Sebagai contoh, salah satu dari berikut ini menyebabkan error: Klien memasukkan data credential yang biasa dimana data yang kuat yang dibutuhkan, atau, klien memasukkan DN atau password untuk bind tetapi entri tidak memiliki pass- word yang jelas
49	LDAP_INVALID_CREDENTIALS	Mengindikasikan selama proses bind, salah satu dari berikut terjadi: Klien memberikan DN atau password yang salah, atau kesalahan password karena sudah expired, deteksi penyusup mengunci akun, atau beberapa alasan yang sama lainnya. Ini setara dengan kode error AD 52e.
49	ERROR_TOO_MANY_CONTEXT_IDS	Sesuai akun dengan kode data 568, indikasikan bahwa selama percobaan log-on, keamanan user mengakumulasi terlalu banyak security ID. Ini menjadi masalah pada akun LDAP tertentu yang seharusnya diinvestigasi oleh admin LDAP

50	LDAP_INSUFFICIENT_ACCESS	Indikasikan bahwa user tidak memiliki wewenang yang cukup untuk melakukan operasi yang diminta
51	LDAP_BUSY	Indikasikan bahwa server LDAP terlalu sibuk untuk melakukan proses permintaan klien saat ini, tetapi jika klien menunggu dan mengajukan permintaan lagi, server mungkin akan bisa memproses permintaan itu.
52	LDAP_UNAVAILABLE	Indikasikan bahwa server LDAP tidak bisa memproses pemintaan bind klien, dikarenakan dalam proses shutting down
52e	AD_INVALID CREDENTIALS	Indikasikan bahwa AD(Activer Directory) AcceptSecurityContexerror, yang terjadi karena username yang valid tetapi kombinasi password dan data pribadi yang tidak valid. AD ini setara dengan kode error LDAP 49.
53	LDAP_UNWILLING_TO_PERFORM	Indikasikan bahwa server LDAP tidak bisa memproses permintaan karena batasan yang ditentukan server. Error terjadi karena alasan berikut: permintaan add entry melanggar peraturan struktur server, atau permintaan modify atribut menspesifikasikan atribut yang tidak dapat diganti, atau batasan password mencegah proses, atau batasan koneksi mencegah proses selanjutnya
54	LDAP_LOOP_DETECT	Indikasikan bahwa klien menemukan loop alias atau referral, dan karenanya tidak bisa menyelesaikan permintaan.
55-63		Tidak digunakan
64	LDAP_NAMING_VIOLATION	Indikasikan bahwa operasi add atau modify DN melanggar peraturan struktur skema. Contoh, Permintaan menempatkan entri bawahan ke alias. Permintaan menempatkan entri bawahan ke tempat yang dilarang oleh aturan. RDN untuk entri menggunakan jenis atribut terlarang.
65	LDAP_OBJECT_CLASS_VIOLATION	Indikasikan bahwa operasi add, modify, atau modify DN melanggar kelas objek

		pada entri. Sebagai contoh, permintaan berikut akan menghasilkan error: Operasi add atau modify mencoba untuk menambahkan entri tanpa nilai yang sesuai dengan atribut. Operasi add dan modify mencoba untuk menambahkan entri dengan nilai untuk atribut yang definisi kelasnya tidak sesuai. Operasi modify mencoba untuk menghapus atribut yang dibutuhkan tanpa menghapus auxiliary class yang menentukan atribut yang dibutuhkan.
66	LDAP_NOT_ALLOWED_ON_NONLEAF	Indikasikan bahwa operasi yang diminta hanya dibolehkan pada entri leaf. Sebagai contoh, berikut adalah jenis permintaan yang akan menghasilkan error: Klien meminta operasi penghapusan pada parent entri. Klien meminta untuk mengubah operasi DN pada parent entri.
67	LDAP_NOT_ALLOWED_ON_RDN	Indikasikan bahwa operasi modify mencoba untuk menghapus nilai atribut yang membentuk nama relatif entri yang berbeda.
68	LDAP_ALREADY_EXISTS	Indikasikan bahwa operasi add mencoba untuk menambahkan entri yang sudah ada, atau operasi modify mencoba untuk mengganti nama entri yang sudah ada.
69	LDAP_NO_OBJECT_CLASS_MODS	Indikasikan bahwa operasi modify mencoba untuk mengubah struktur peraturan pada kelas objek
70	LDAP_RESULTS_TOO_LARGE	Disimpan untuk CLDAP
71	LDAP_AFFECTS_MULTIPLE_DSAS	Indikasikan bahwa operasi modify DN memindahkan entri dari server LDAP yang satu ke server yang lain dan membutuhkan lebih dari satu LDAP
72-79		Tidak digunakan
80	LDAP_OTHER	Indikasikan bahwa kondisi error yang tidak diketahui. Ini adalah nilai default untuk kode error NDS yang tidak dipetakan pada kode error LDAP lainnya.

525	USER NOT FOUND	Indikasikan Active Directory (AD) AcceptSecurityContextdata error ketika username yang dimasukkan invalid.
530	NOT_PERMITTED_TO_LOGON_AT_THIS_TIME	Indikasikan Active Directory (AD) AcceptSecurityContextdata error bahwa ada kesalahan login dikarenakan user tidak diperbolehkan login pada saat ini. kembali hanya jika sudah memiliki username an password yang valid.
531	RESTRICTED_TO_SPECIFIC_MACHINES	Indikasikan Active Directory (AD) AcceptSecurityContextdata error bahwa ada kesalahan login dikarenakan user tidak diperbolehkan login dari komputer ini. kembali hanya jika sudah memiliki username dan password yang valid.
532	PASSWORD_EXPIRED	Indikasikan Active Directory (AD) AcceptSecurityContextdata error bahwa ada kesalahan login. Password dari akun telah expired kembali hanya jika sudah memiliki username dan password yang valid.
533	ACCOUNT_DISABLED	Indikasikan Active Directory (AD) AcceptSecurityContextdata error bahwa ada kesalahan login. Akun sedang dikunci. kembali hanya jika sudah memiliki username dan password yang valid.
701	ACCOUNT_EXPIRED	Indikasikan Active Directory (AD) AcceptSecurityContextdata error bahwa ada kesalahan login. Akun user telah ex- pired. kembali hanya jika sudah memiliki username dan password yang valid.
773	USER MUST RESET PASSWORD	Indikasikan Active Directory (AD) AcceptSecurityContextdata mengalami error. Password dari user harus diganti sebelum log-in untu pertama kalinya. dan kembali jika sudah memiliki username dan password yang valid.