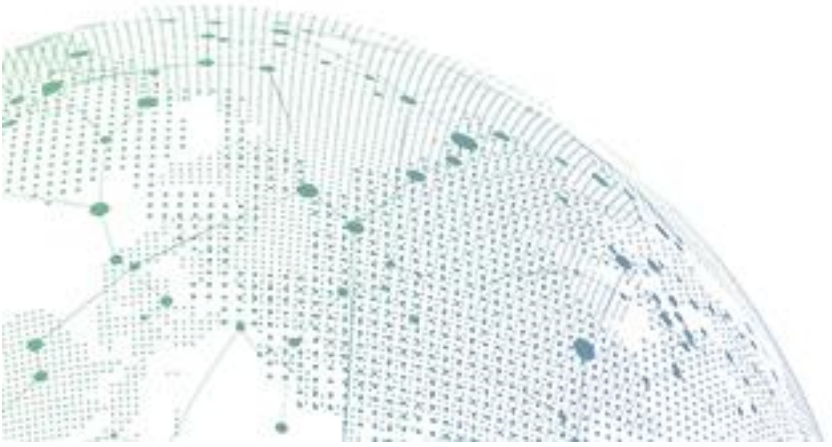
SANGFOR

IAM

LDAP Sync POC Guide

Version 4.0



CONTENT

Chapter 1 LDAP Sync POC Instructor

For LDAP synchronization policy, there are two synchronization modes: [Sync by OU] and [Sync by security group (AD domain only)]. Their respective features and functions are described in the following sections.

To synchronize the users, organizational units (OUs) or security groups from LDAP server to the IAM device, first, you need to configure the synchronization policy so that they will be synchronized according to the settings of the policy.

1.1 Synchronize by OU

The [Sync by OU] mode is applicable to all types of LDAP server. By this mode, the OUs on the LDAP server will be synchronized in the form of user groups to the IAM device and the organization structure of OUs synchronized in the same way, ensuring the users still belongs to their respective groups after the synchronization.

1.2 Synchronize by Security Group (AD Domain Only)

The [Sync by security group (AD domain only)] mode is only applicable to the Microsoft LDAP server, that is, AD domain. By this mode, the security groups on the AD domain server will be synchronized in the form of user groups to the IAM device. Since the security groups have no organization structure, all the security groups will be of the same level after being synchronized into the IAM device.

Chapter 2 Preparations

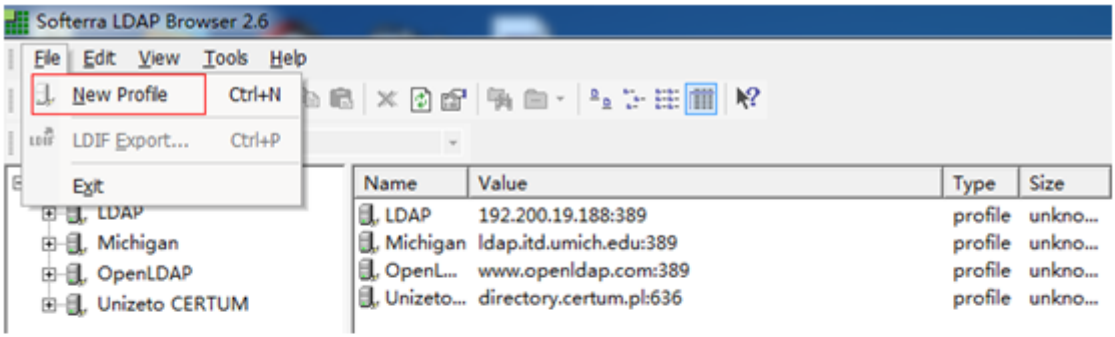
- A IAM4.0 device ,LDAP Sync can work on all kind of deployment, just confirm that IAM can communicate with LDAP server.
- Please patch the below KB firstly:
- /cms/a/IAM/Troubleshooting/2013/0926/107.html
- Prepare a PC installed LDAP browser software.
- Make sure customer requirment:does he want to sync by OU or by Security Group?
- A domain user that have the authority to browse all of domain organization structure.

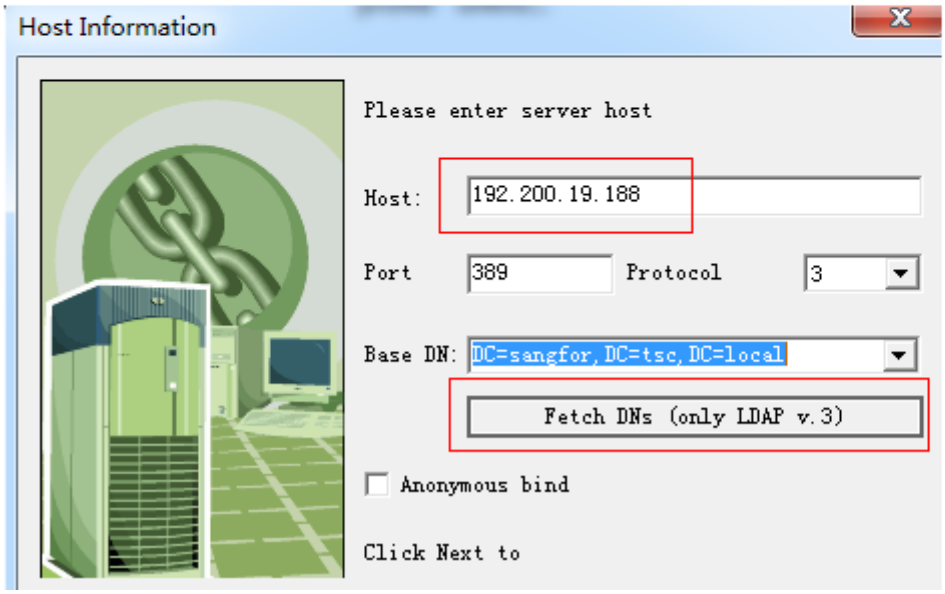
Chapter 3 Expected result

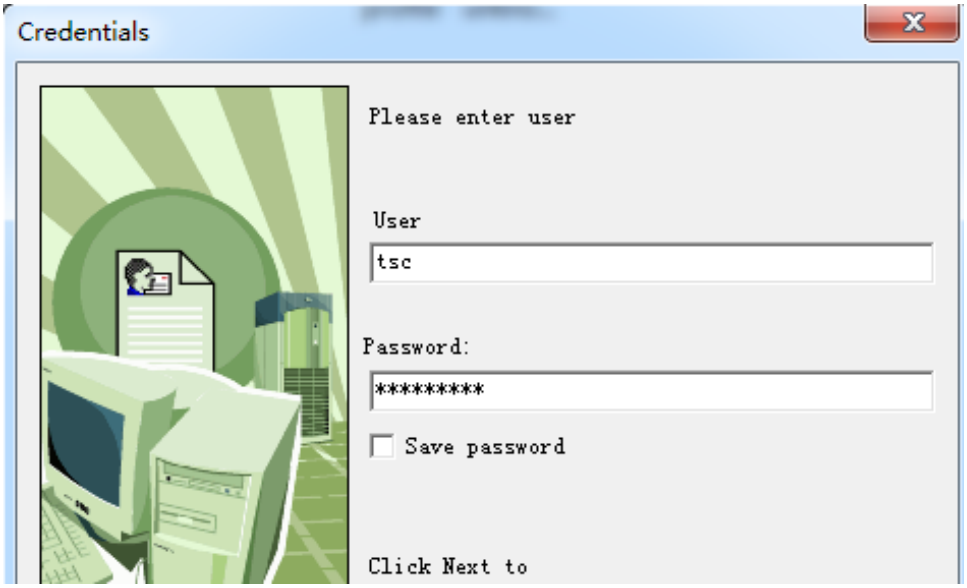
It can sync all domain users and organizations to IAM.

3.1 Configure steps

3.1.1 'Use LDAP Browser to obtain domain informations':







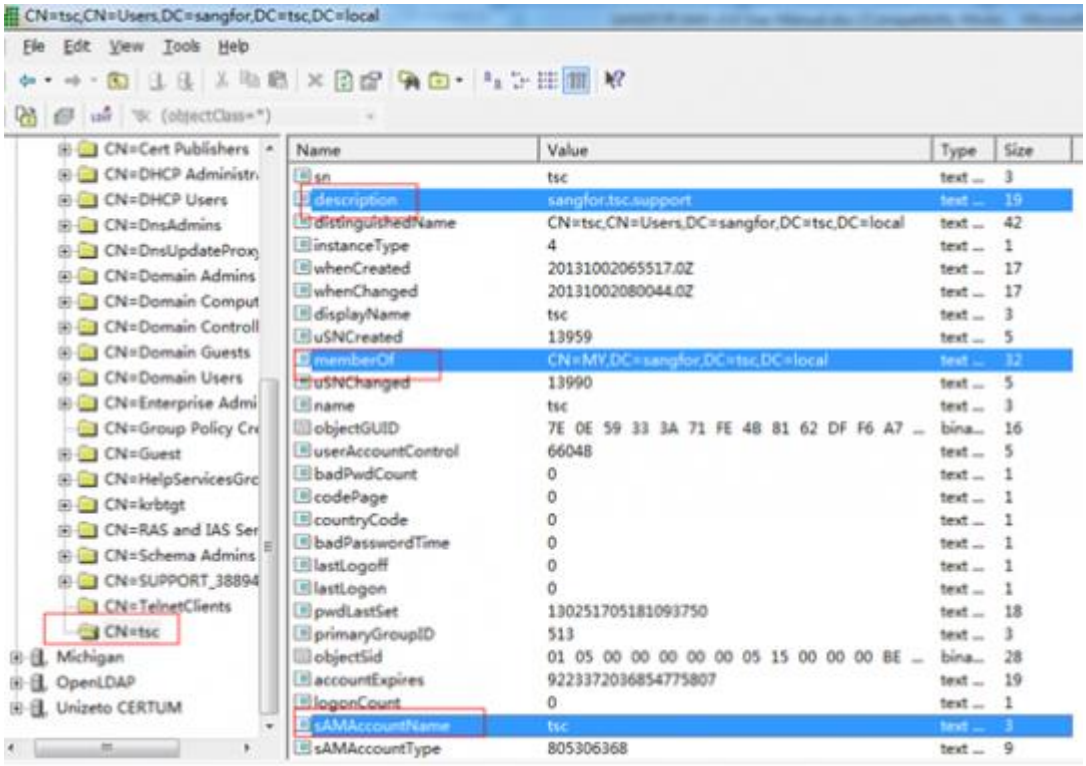
Why we should do this?

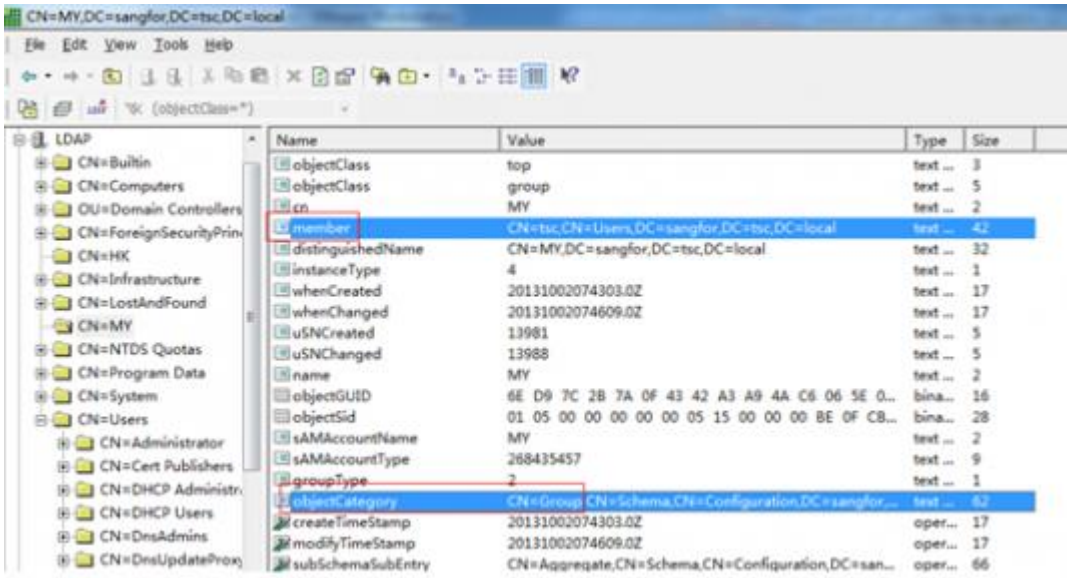
Purpose 1: To confirm the users have the authority to browse all of domain organization structure.

Purpose 2:

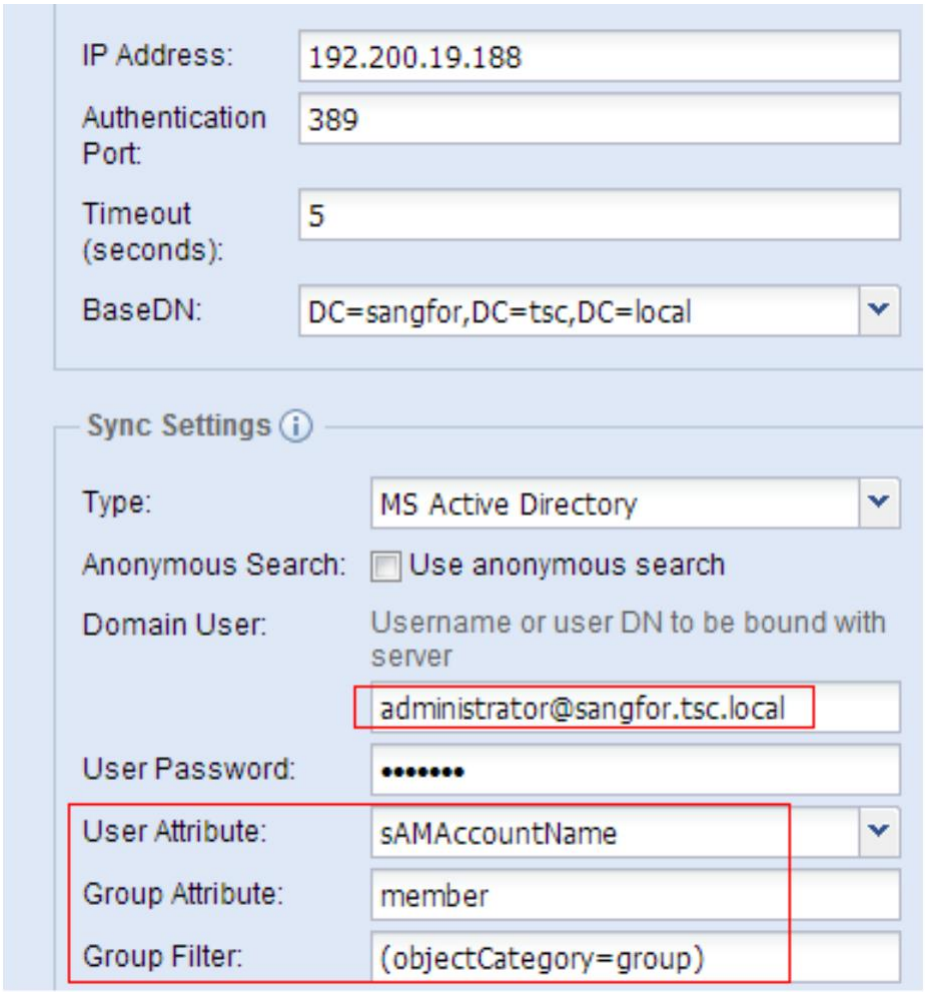
As below picture shown:

we can find out user "tsc" 's User attribute is " sAMAccountName ",and Description attribute is "description",Group attribute is "member" and Group Filter is




CN=MY,DC=sangfor,DC=tsc,DC=local
File Edit View Tools Help
(objectClass=*)
LDAP
CN=Builtin
CN=Computers
OU=Domain Controllers
CN=ForeignSecurityPrin
CN=HK
CN=Infrastructure
CN=LostAndFound
CN=MY
CN=NTDS Quotas
CN=Program Data
CN=System
CN=Users
CN=Administrator
CN=Cert Publishers
CN=DHCP Administr
CN=DHCP Users
CN=DnsAdmins
CN=DnsUpdateProx
Name
Value
Type
Size
objectClass top text ... 3
objectClass group text ... 5
cn MY text ... 2
member CN=tsc,CN=Users,DC=sangfor,DC=tsc,DC=local text ... 42
distinguishedName CN=MY,DC=sangfor,DC=tsc,DC=local text ... 32
instanceType 4 text ... 1
whenCreated 20131002074303.0Z text ... 17
whenChanged 20131002074609.0Z text ... 17
uSNCreated 13981 text ... 5
uSNChanged 13988 text ... 5
name MY text ... 2
objectGUID 6E D9 7C 2B 7A 0F 43 42 A3 A9 4A C6 06 5E 0... bina... 16
objectSid 01 05 00 00 00 00 00 05 15 00 00 00 BE 0F CB... bina... 28
sAMAccountName MY text ... 2
sAMAccountType 268435457 text ... 9
groupType 2 text ... 1
objectCategory CN=Group,CN=Schema,CN=Configuration,DC=sangfor,... text ... 62
createTimeStamp 20131002074303.0Z oper... 17
modifyTimeStamp 20131002074609.0Z oper... 17
subSchemaSubEntry CN=Aggregate,CN=Schema,CN=Configuration,DC=san... oper... 66

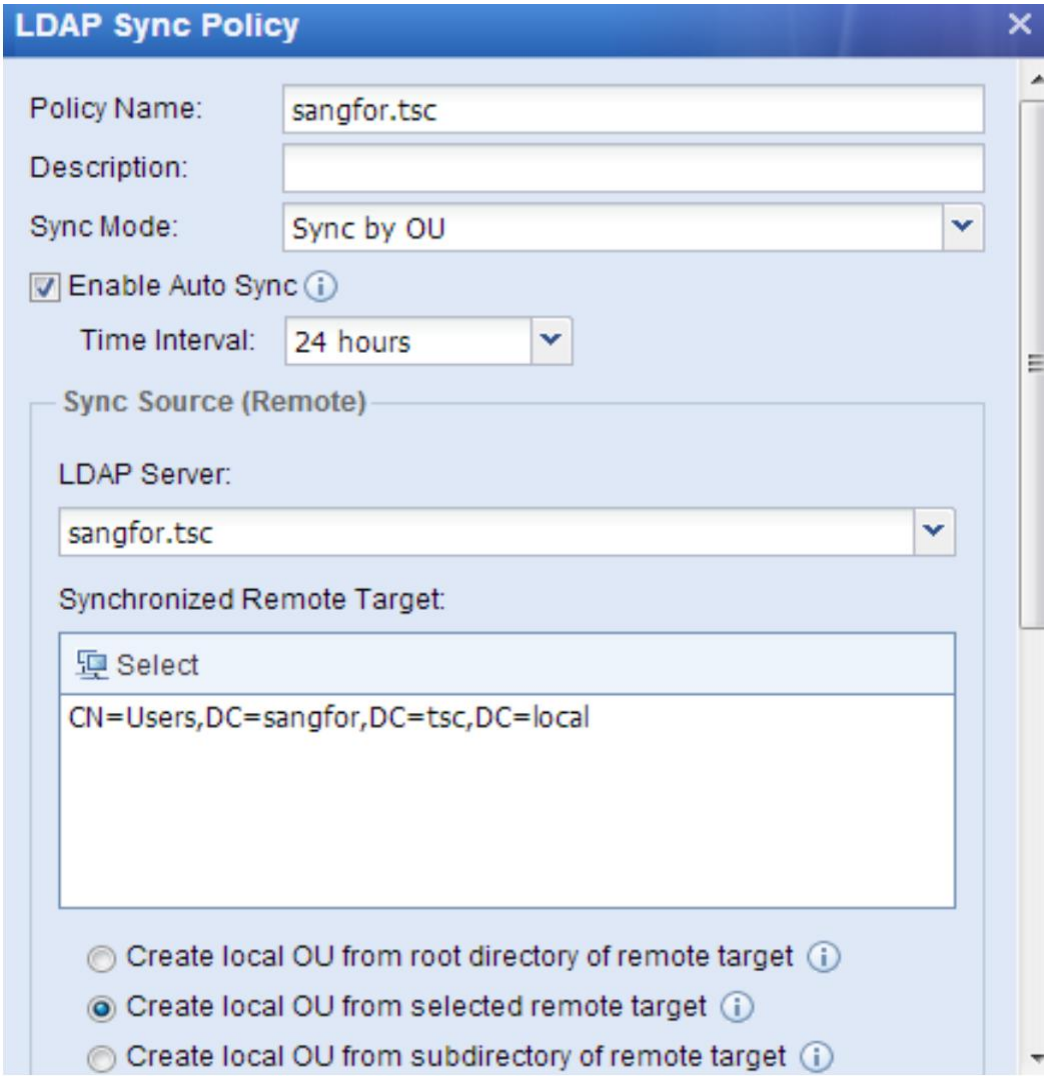
3.1.2 'Add LDAP Server':



Noted if the server type is MS Active Director,we no need to change anything,just use the default configuration.If the server type is other,maybe wo need use LDAP Browser to make sure all attribute is the same with server.

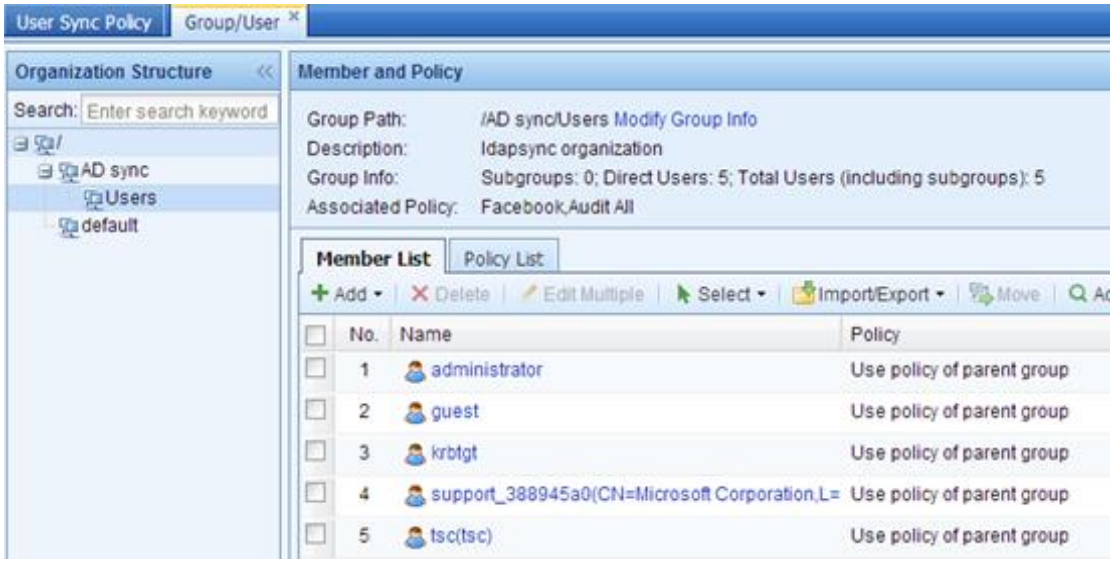
3.1.3 'User Sync Policy':

Synchronize by OU

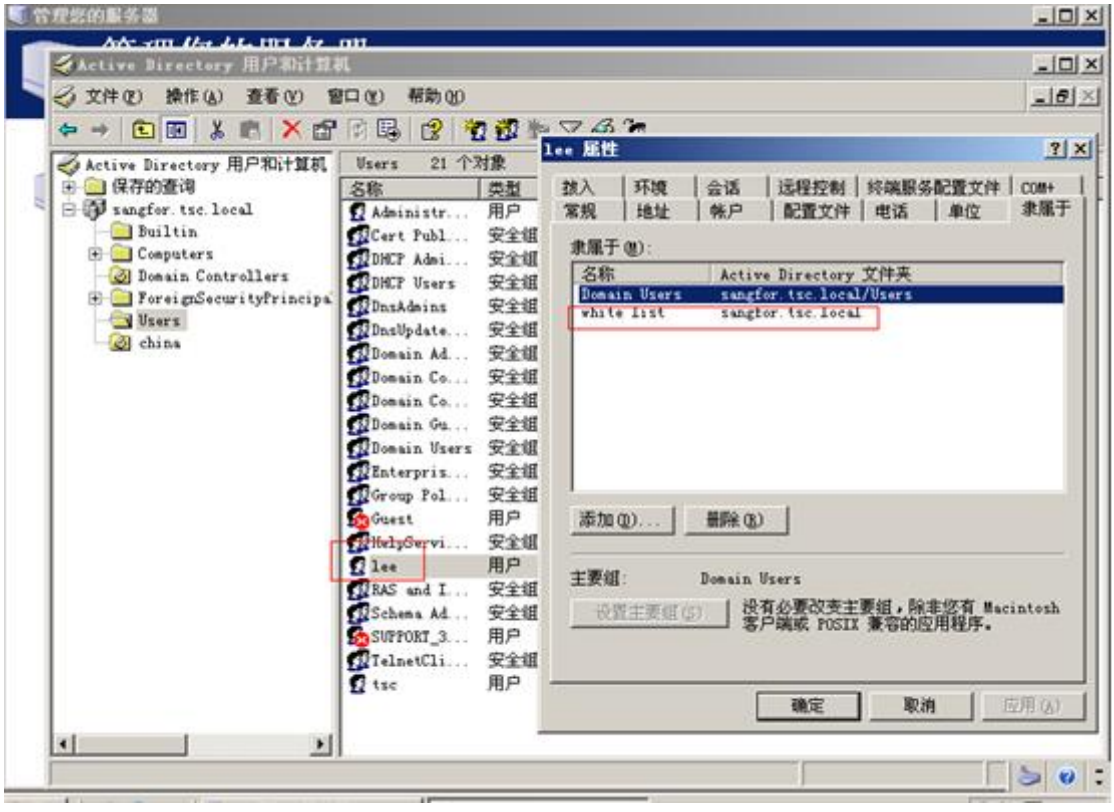

LDAP Sync Policy
Policy Name:
sangfor.tsc
Description:
Sync Mode:
Sync by OU
Enable Auto Sync
Time Interval:
24 hours
Sync Source (Remote)
LDAP Server:
sangfor.tsc
Synchronized Remote Target:
Select
CN=Users,DC=sangfor,DC=tsc,DC=local
Create local OU from root directory of remote target
Create local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

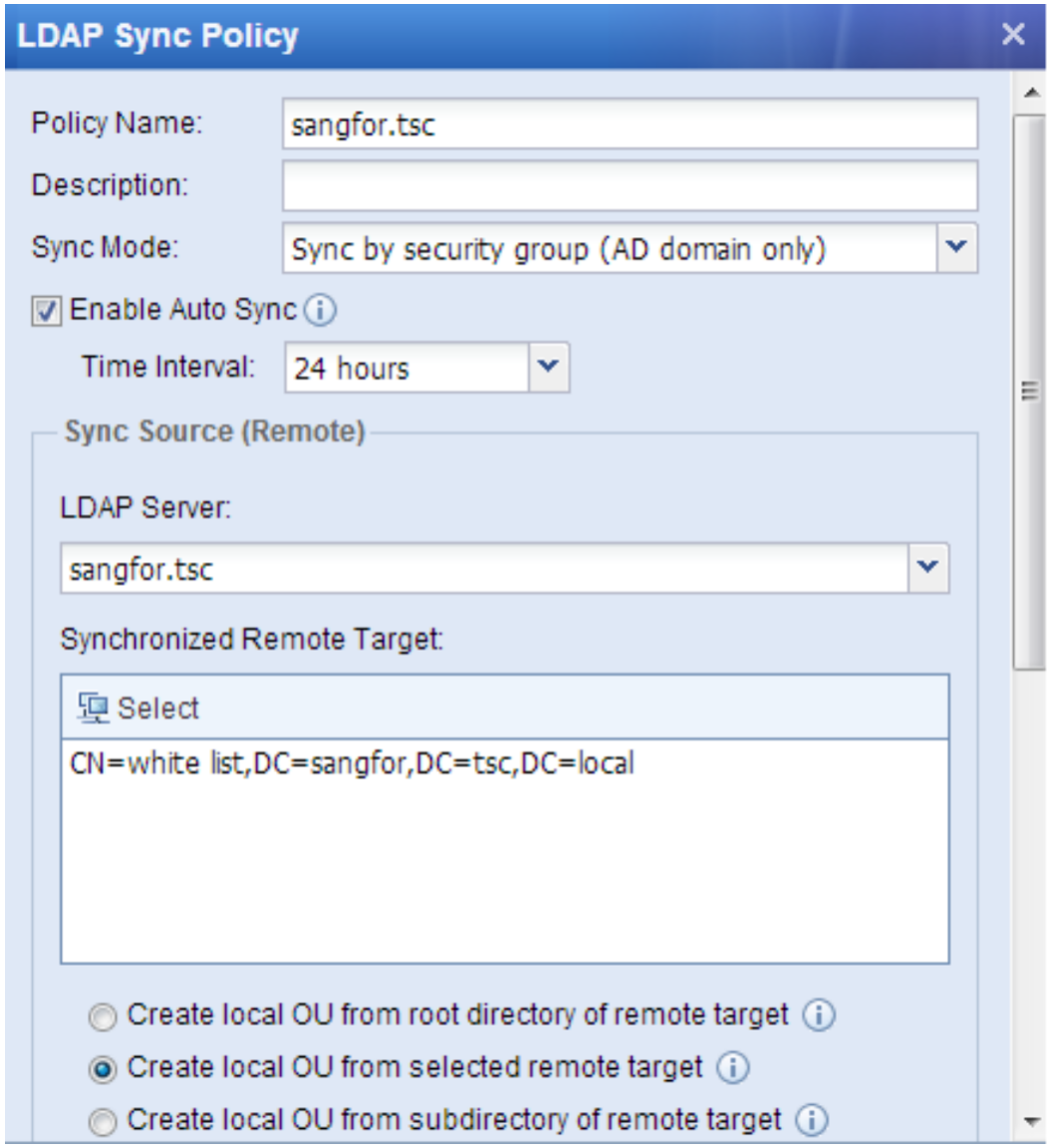

Sync Destination (Local)
Sync Method:
Synchronize LDAP OU and user to local
Synchronize LDAP user to local, OU ignored
Synchronize LDAP OU to local, user ignored
Sync Remote Target To:
/AD sync/
Synchronized accounts support multi-user login

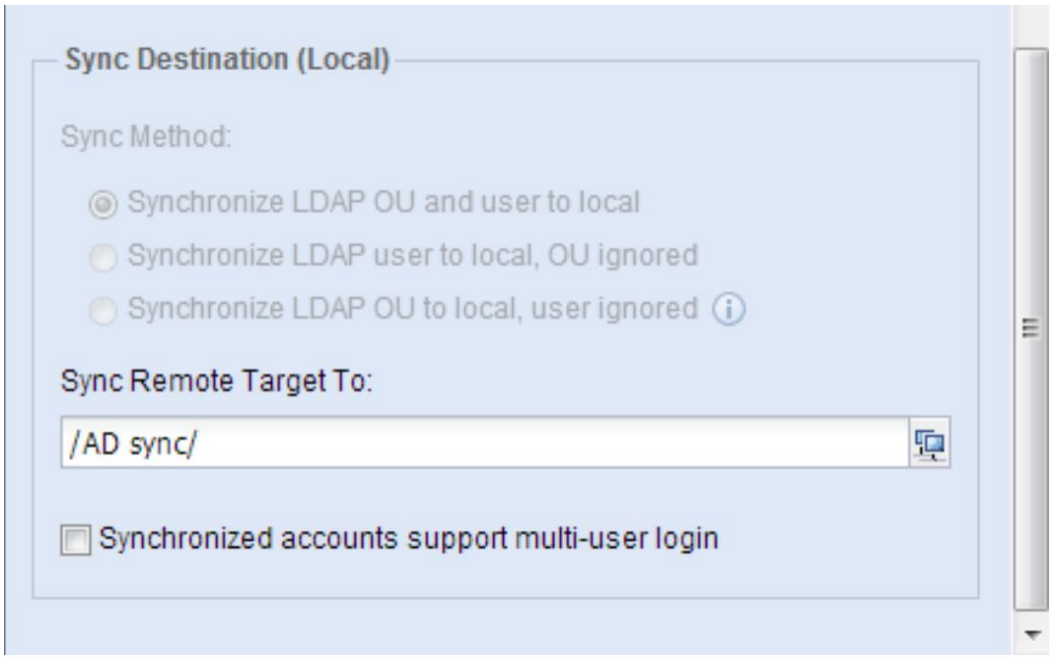
3.1.4 Results



Synchronize by Security Group (AD Domain Only):




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

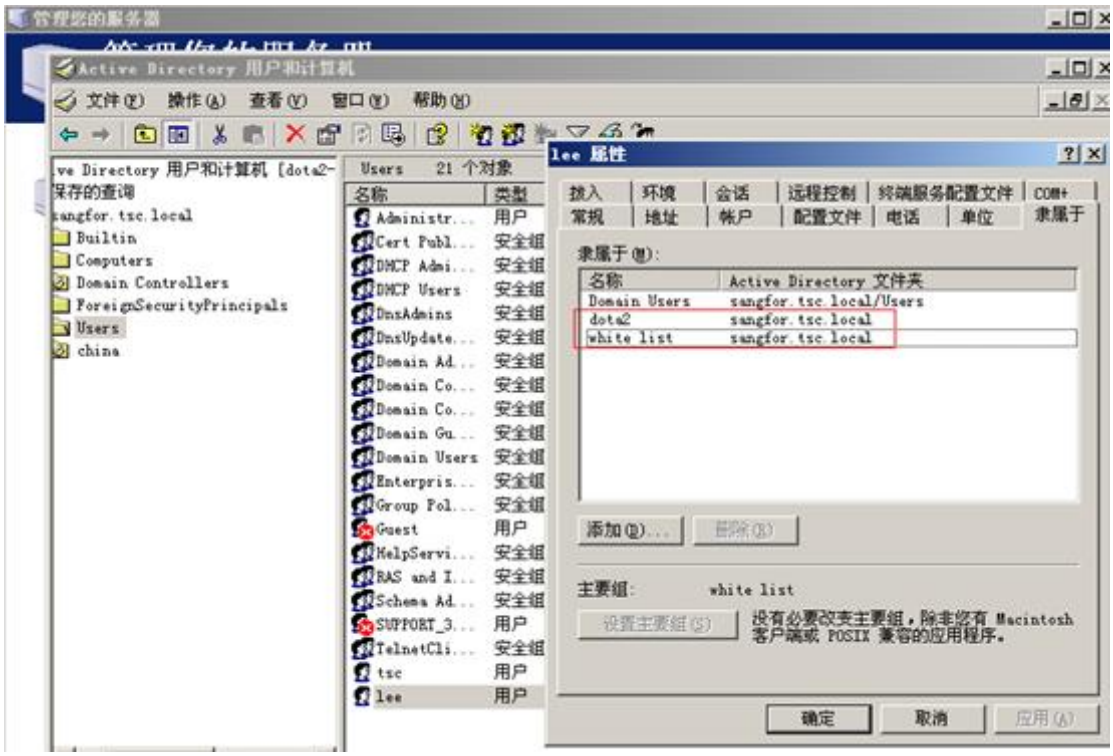
Result as picture shown

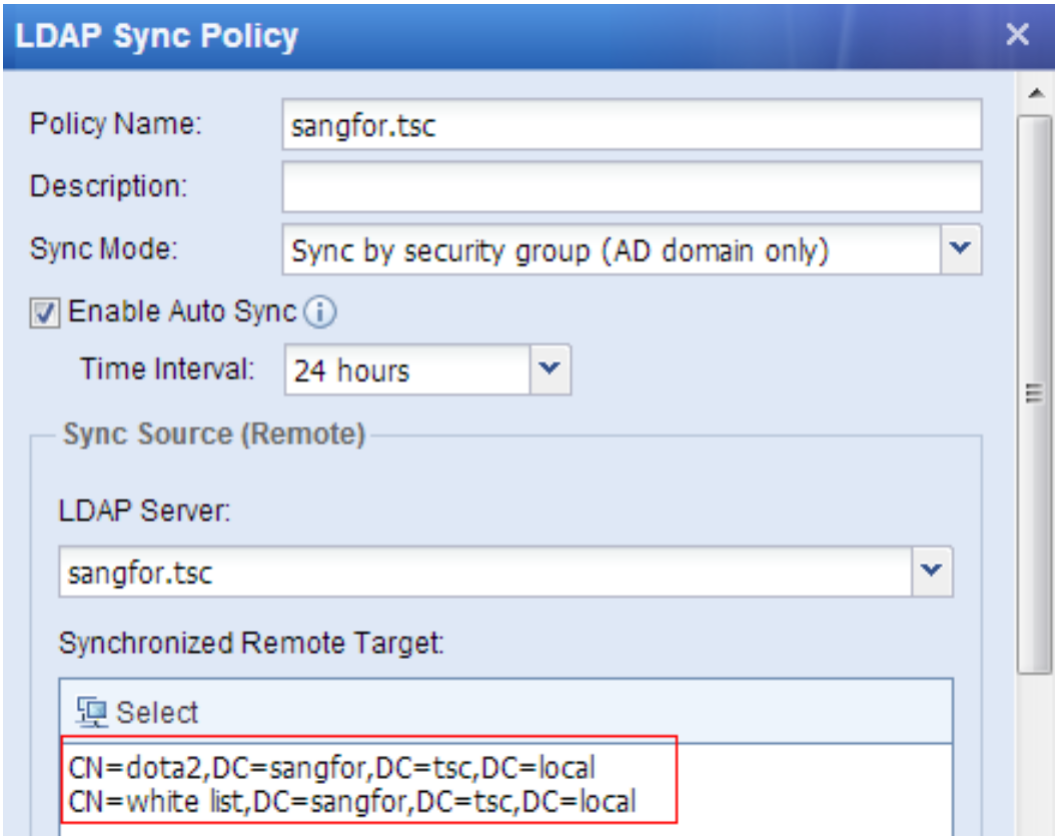
Noted: As below picture shown,if lee is belong to two security group "dota2" and "white list",how about the sync result?

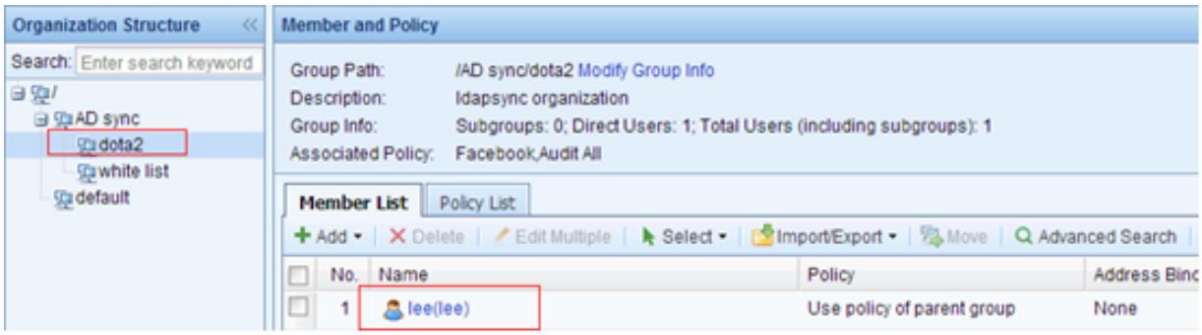
Result:

Attention:If customer want IAM to support Multi-Security group sync ,Please send theappvension and /etc/hwinfo to CTI and ask for customize patch.

IAM can not sync users that only belong to Security group named "Domain Users"



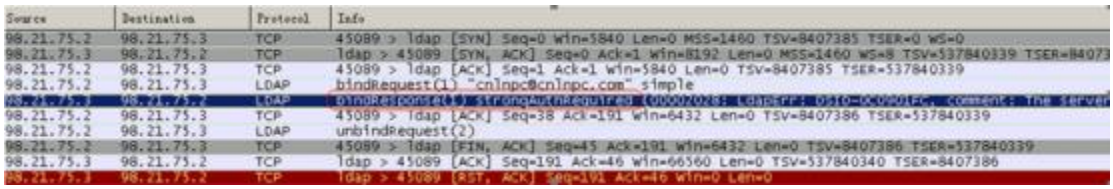




Chapter 4 Troubleshooting

1. Make sure you can telnet server tcp 389 port OK.
2. Use LDAP browser to confirm the attribute.
3. IAM can only support sync 65535 number of users and max OU import depth is 16.

4. IAM can not support StrongAuthRequired,you can confirm it by tcpdump packets.



1. Tcpdump -i eth0 host iam ip and ldap server ip and port 389 -s0 -w /tmp/ldap.cap
2. /etc/init.d/syncusrd stop
3. Click sync now,wait a while until sync failed
4. Send the ldap.cap and /var/log/ldpsync.log to CTI
5. /etc/init.d/syncusrd start
6. When IAM synchronizes the LDAP OU to the root group, it will auto delete these users who is not domian user.

Default setting is root group

Solution:

Create a group for AD in group/user and sync the remote target to a group instead of root group "/"

7. Error Code

Error Code	Error	Description
0	LDAP_SUCCESS	Indicates the requested client operation completed successfully.
1	LDAP_OPERATIONS_ERROR	Indicates an internal error. The server is unable to respond with a more specific error and is also unable to properly respond to a request. It does not indicate that the client has sent an erroneous message. In NDS 8.3x through NDS 7.xx, this was the default error for NDS errors that did not map to an LDAP error code. To conform to the new LDAP drafts, NDS 8.5 uses 80 (0x50) for such errors.

2	LDAP_PROTOCOL_ERROR	Indicates that the server has received an invalid or malformed request from the client.
3	LDAP_TIMELIMIT_EXCEEDED	Indicates that the operation's time limit specified by either the client or the server has been exceeded. On search operations, incomplete results are returned.
4	LDAP_SIZELIMIT_EXCEEDED	Indicates that in a search operation, the size limit specified by the client or the server has been exceeded. Incomplete results are returned.
5	LDAP_COMPARE_FALSE	Does not indicate an error condition. Indicates that the results of a compare operation are false.
6	LDAP_COMPARE_TRUE	Does not indicate an error condition. Indicates that the results of a compare operation are true.
7	LDAP_AUTH_METHOD_NOT_SUPPORTED	Indicates that during a bind operation the client requested an authentication method not supported by the LDAP server.
8	LDAP_STRONG_AUTH_REQUIRED	Indicates one of the following: In bind requests, the LDAP server accepts only strong authentication. In a client request, the client requested an operation such as delete that requires strong authentication. In an unsolicited notice of disconnection, the LDAP server discovers the security protecting the communication between the client and server has unexpectedly failed or been compromised.
9		Reserved.
10	LDAP_REFERRAL	Does not indicate an error condition. In LDAPv3, indicates that the server does not hold the target entry of the request, but that the servers in the referral field may.
11	LDAP_ADMINLIMIT_EXCEEDED	Indicates that an LDAP server limit set by an administrative authority has been exceeded.

12	LDAP_UNAVAILABLE_CRITICAL_EXTENSION	Indicates that the LDAP server was unable to satisfy a request because one or more critical extensions were not available. Either the server does not support the control or the control is not appropriate for the operation type.
13	LDAP_CONFIDENTIALITY_REQUIRED	Indicates that the session is not protected by a protocol such as Transport Layer Security (TLS), which provides session confidentiality.
14	LDAP_SASL_BIND_IN_PROGRESS	Does not indicate an error condition, but indicates that the server is ready for the next step in the process. The client must send the server the same SASL mechanism to continue the process.
15		Not used.
16	LDAP_NO_SUCH_ATTRIBUTE	Indicates that the attribute specified in the modify or compare operation does not exist in the entry.
17	LDAP_UNDEFINED_TYPE	Indicates that the attribute specified in the modify or add operation does not exist in the LDAP server's schema.
18	LDAP_INAPPROPRIATE_MATCHING	Indicates that the matching rule specified in the search filter does not match a rule defined for the attribute's syntax.
19	LDAP_CONSTRAINT_VIOLATION	Indicates that the attribute value specified in a modify, add, or modify DN operation violates constraints placed on the attribute. The constraint can be one of size or content (string only, no binary).
20	LDAP_TYPE_OR_VALUE_EXISTS	Indicates that the attribute value specified in a modify or add operation already exists as a value for that attribute.
21	LDAP_INVALID_SYNTAX	Indicates that the attribute value specified in an add, compare, or modify operation is an unrecognized or invalid syntax for the attribute.
22-31		Not used.
32	LDAP_NO_SUCH_OBJECT	Indicates the target object cannot be found. This code is not returned on following operations: Search operations that find the search base but cannot find

		any entries that match the search filter. Bind operations.
33	LDAP_ALIAS_PROBLEM	Indicates that an error occurred when an alias was dereferenced.
34	LDAP_INVALID_DN_SYNTAX	Indicates that the syntax of the DN is incorrect. (If the DN syntax is correct, but the LDAP server's structure rules do not permit the operation, the server returns LDAP_UNWILLING_TO_PERFORM.)
35	LDAP_IS_LEAF	Indicates that the specified operation cannot be performed on a leaf entry. (This code is not currently in the LDAP specifications, but is reserved for this constant.)
36	LDAP_ALIAS_DEREF_PROBLEM	Indicates that during a search operation, either the client does not have access rights to read the aliased object's name or dereferencing is not allowed.
37-47		Not used.
48	LDAP_INAPPROPRIATE_AUTH	Indicates that during a bind operation, the client is attempting to use an authentication method that the client cannot use correctly. For example, either of the following cause this error: The client returns simple credentials when strong credentials are required...OR...The client returns a DN and a password for a simple bind when the entry does not have a password defined.
49	LDAP_INVALID_CREDENTIALS	Indicates that during a bind operation one of the following occurred: The client passed either an incorrect DN or password, or the password is incorrect because it has expired, intruder detection has locked the account, or another similar reason. This is equivalent to AD error code 52e.
49	ERROR_TOO_MANY_CONTEXT_IDS	Corresponds to data code 568. Indicates that during a log-on attempt, the user's security context accumulated too many security IDs. This is an issue with the specific LDAP user object/account which should be investigated by the LDAP administrator.

50	LDAP_INSUFFICIENT_ACCESS	Indicates that the caller does not have sufficient rights to perform the requested operation.
51	LDAP_BUSY	Indicates that the LDAP server is too busy to process the client request at this time but if the client waits and resubmits the request, the server may be able to process it then.
52	LDAP_UNAVAILABLE	Indicates that the LDAP server cannot process the client's bind request, usually because it is shutting down.
52e	AD_INVALID CREDENTIALS	Indicates an Active Directory (AD) AcceptSecurityContexterror, which is returned when the username is valid but the combination of password and user credential is invalid.This is the AD equivalent of LDAP error code 49.
53	LDAP_UNWILLING_TO_PERFORM	Indicates that the LDAP server cannot process the request because of server-defined restrictions. This error is returned for the following reasons: The add entry request violates the server's structure rules...OR...The modify attribute request specifies attributes that users cannot modify...OR...Password restrictions prevent the action...OR...Connection restrictions prevent the action.
54	LDAP_LOOP_DETECT	Indicates that the client discovered an alias or referral loop, and is thus unable to complete this request.
55-63		Not used.
64	LDAP_NAMING_VIOLATION	Indicates that the add or modify DN operation violates the schema's structure rules. For example, The request places the entry subordinate to an alias. The request places the entry subordinate to a container that is forbidden by the containment rules. The RDN for the entry uses a forbidden attribute type.
65	LDAP_OBJECT_CLASS_VIOLATION	Indicates that the add, modify, or modify DN operation violates the object class

		rules for the entry. For example, the following types of request return this error: The add or modify operation tries to add an entry without a value for a required attribute. The add or modify operation tries to add an entry with a value for an attribute which the class definition does not contain. The modify operation tries to remove a required attribute without removing the auxiliary class that defines the attribute as required.
66	LDAP_NOT_ALLOWED_ON_NONLEAF	Indicates that the requested operation is permitted only on leaf entries. For example, the following types of requests return this error: The client requests a delete operation on a parent entry. The client request a modify DN operation on a parent entry.
67	LDAP_NOT_ALLOWED_ON_RDN	Indicates that the modify operation attempted to remove an attribute value that forms the entry's relative distinguished name.
68	LDAP_ALREADY_EXISTS	Indicates that the add operation attempted to add an entry that already exists, or that the modify operation attempted to rename an entry to the name of an entry that already exists.
69	LDAP_NO_OBJECT_CLASS_MODS	Indicates that the modify operation attempted to modify the structure rules of an object class.
70	LDAP_RESULTS_TOO_LARGE	Reserved for CLDAP.
71	LDAP_AFFECTS_MULTIPLE_DSAS	Indicates that the modify DN operation moves the entry from one LDAP server to another and requires more than one LDAP server.
72-79		Not used.
80	LDAP_OTHER	Indicates an unknown error condition. This is the default value for NDS error codes which do not map to other LDAP error codes.

525	USER NOT FOUND	Indicates an Active Directory (AD) AcceptSecurityContextdata error that is returned when the username is invalid.
530	NOT_PERMITTED_TO_LOGON_AT_THIS_TIME	Indicates an Active Directory (AD) AcceptSecurityContextdata error that is logon failure caused because the user is not permitted to log on at this time. Returns only when presented with a valid username and valid password credential.
531	RESTRICTED_TO_SPECIFIC_MACHINES	Indicates an Active Directory (AD) AcceptSecurityContextdata error that is logon failure caused because the user is not permitted to log on from this computer. Returns only when presented with a valid username and valid password credential.
532	PASSWORD_EXPIRED	Indicates an Active Directory (AD) AcceptSecurityContextdata error that is a logon failure. The specified account password has expired. Returns only when presented with valid username and password credential.
533	ACCOUNT_DISABLED	Indicates an Active Directory (AD) AcceptSecurityContextdata error that is a logon failure. The account is currently disabled. Returns only when presented with valid username and password credential.
701	ACCOUNT_EXPIRED	Indicates an Active Directory (AD) AcceptSecurityContextdata error that is a logon failure. The user's account has expired. Returns only when presented with valid username and password credential.
773	USER MUST RESET PASSWORD	Indicates an Active Directory (AD) AcceptSecurityContextdata error. The user's password must be changed before logging on the first time. Returns only when presented with valid user-name and password credential.

SANGFOR