SANGFOR

# IAM

## Databases SSO Configuration Guide

**Version 12.0.18**

# Change Log

| Date | Change Description |
| --- | --- |
| 27 Dec, 2019 | Version 12.0.18 document release. |
| | |

# CONTENT

# Chapter 1 Function Introduction

IAM11.0 database authentication refers to the sequence of authentication information stored in a client's existing database system. IAM11.0 configures SQL query statements on the interface to actively query the user list and authenticated users in the database system. , And synchronize to the IAM's organizational structure and online user list, so that when the user passes the database authentication, that is, the user authentication of the IAM, the user is replaced from the database authentication system, and the replacement on the IAM is also automatically completed. Single sign-on / expected)

Currently supported database types are oracle, ms sql server, db2 and mysql.

# Chapter 2 Application Scenario

When the user has his own authentication system for authentication, the background database is oracle, ms sql server, db2, and mysql, etc., and there is an online user table in the database, IAM can be used in conjunction with the database for single sign-on.

# Chapter 3 Necessary Conditions

1. To determine whether the client can use the database authentication method, you can refer to the following conditions:

2. Users have a database system used to manage user information, such as oracle, ms sql server, db2 or mysql.

3. An online user can be queried from the database with a select statement, and the extracted result set contains two columns: "user name" and "ip address".

4. If you need to synchronize users and organizational structure, you can use a select statement to query all users from the database and query the groups to which the users belong (if you do not need to synchronize groups, you do not need to query the groups to which users belong).

5. The customer is required to provide an account in a database, which can have select permission on the above data table tables or views.

6. IAM can communicate with the server normally (the IAM actively connects to the corresponding port of the database server to trigger synchronization, and does not require that the user's authentication data to the database server must pass through the IAM).

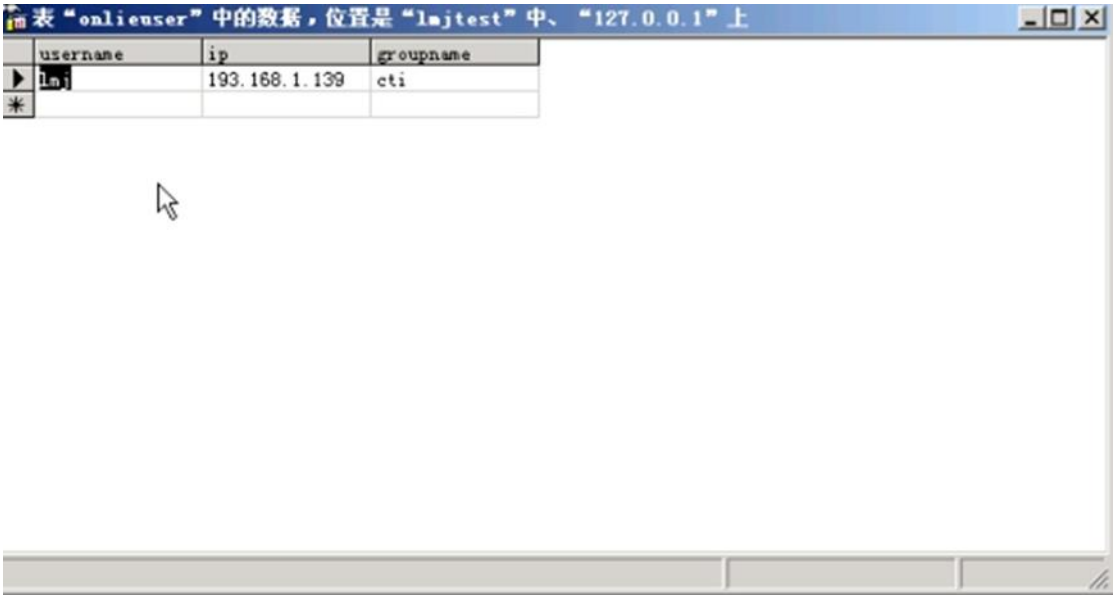
# Chapter 4 Configuration Ideas

## 4.1 Before the Configuration Preparation

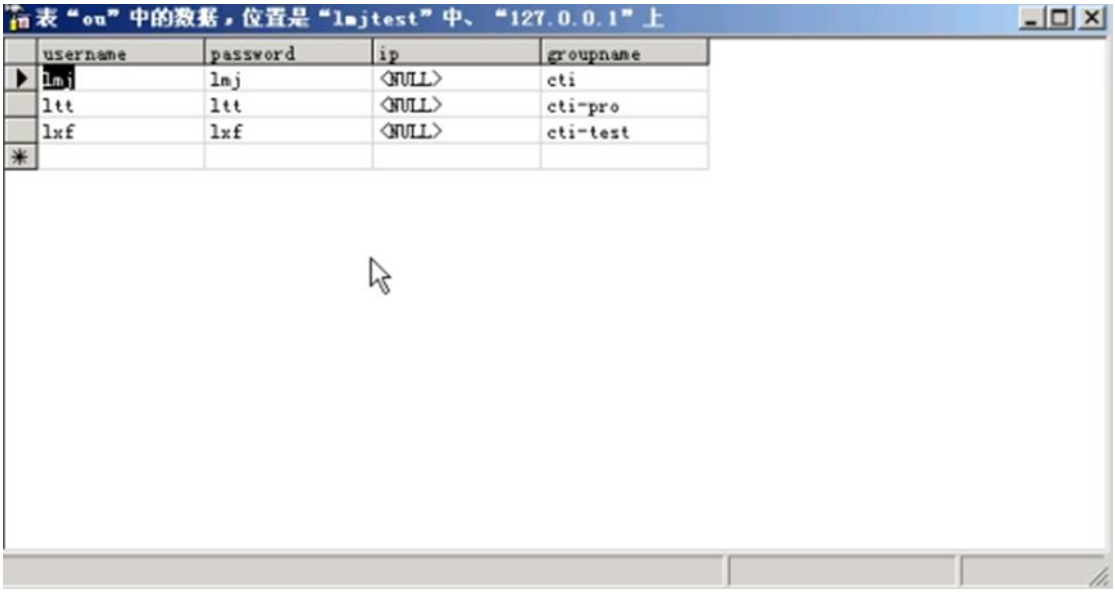
Before configuring, please refer to the "Requirements" section above to obtain some information from the customer, such as database type, database server code, data table structure, key column names, etc., and ask the customer to provide a database account.

These customers generally understand the database themselves and can provide it directly. If we need to find it ourselves, we can refer to the following examples.

This chapter simulates a client environment. Assume that the client database server IP address is 193.168.1.124, the database type is MS SQL, and the database for managing user information is named lmjtest. It is learned that the customer's online user information is stored in the table onlineuser, and the organizational structure information is stored. In table ou, the structure of the two tables is as follows:




Ou table structure for storing organizational structure information:

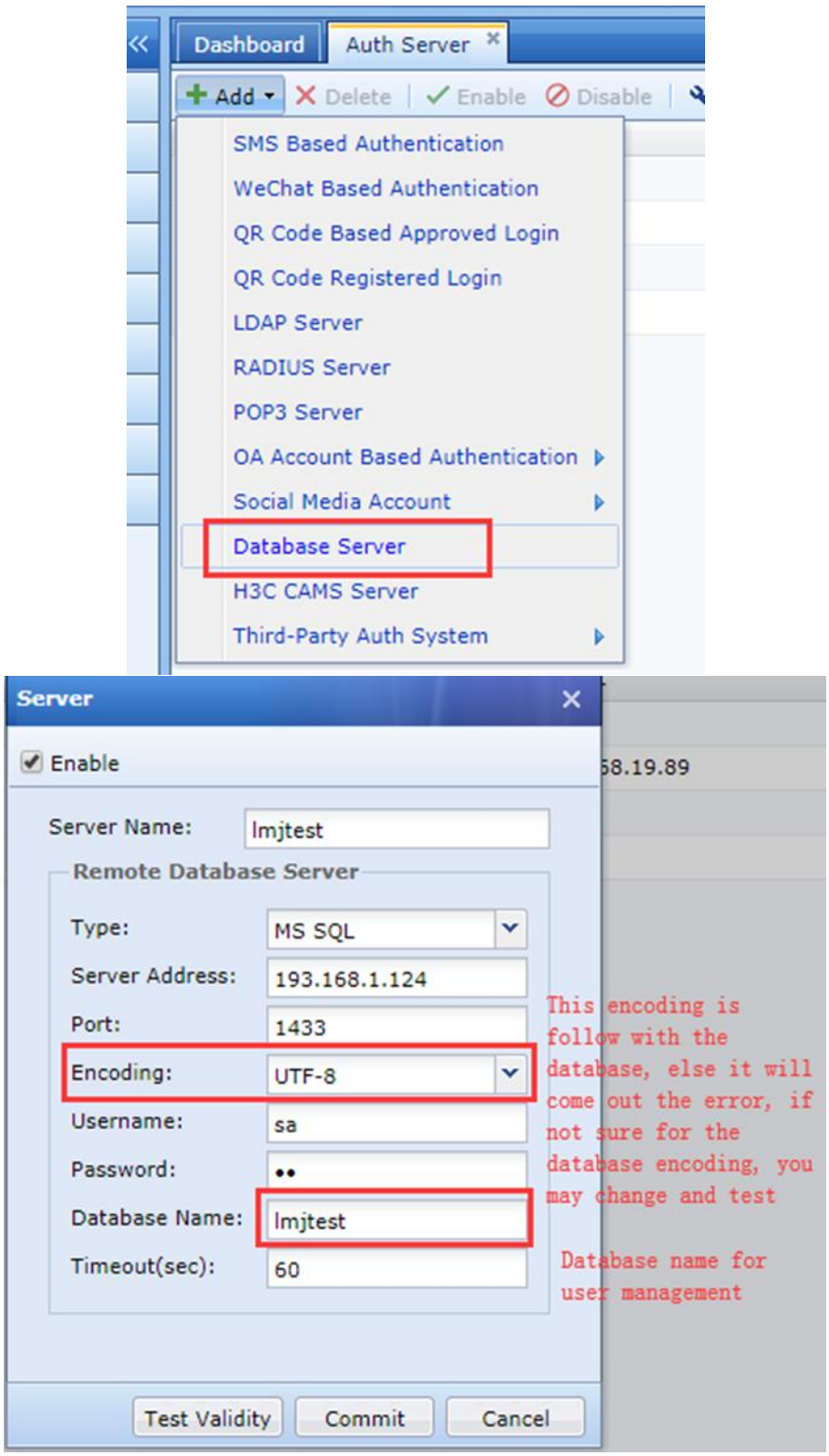



Obtain a database account. In this example, the sa account is used directly. In fact, only users who have query permissions on the data table can be used. (If MS SQL needs to enable mixed authentication)

Get the database encoding. Different database types get different database encodings. For example, mysql can obtain the database encoding type by entering the status command.

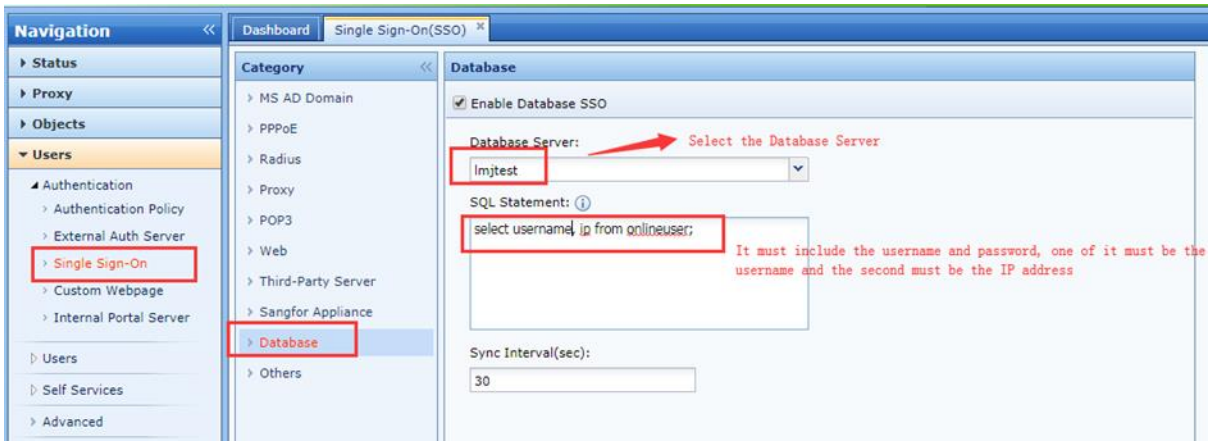
## 4.2 Configuring Single Sign-On for Database Authentication (Synchronizing Online Users)

Define an external authentication server, "User and Policy Management"-"User Authentication"-"External Authentication Server", add a database type external authentication server and configure it, pay special attention to the configuration of "database encoding" and the encoding used by the database is consistent. The "timeout" may need to be adjusted according to the number of users. The default is 60s, as follows:

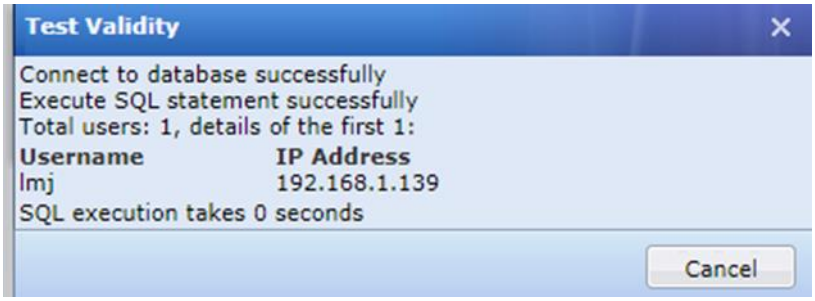



## 4.2.1 Enable Single Sign-on for Database Authentication

select "Single sign-on"-"Database"-select "Enable Database SSO" and select the external authentication server lmjtest just defined.




Click "Test validity" to see the execution result of the SQL statement, and click "Submit" to complete the configuration.




At this time, the IAM will automatically synchronize the online user list immediately. The database single sign-on configuration is completed at this step. At this time, the online user list is viewed. The user lmj is already in the IAM online user list. The authentication method is single sign-on:


**Note:**

1. IAM only supports two columns of username and ip address for online users, and in the extracted result set, the first column is the user name and the second column is ip. If the sql statement in the figure above is select ip, username form onlineuser, In this way, the validity of the test is successful, but the synchronization of the online user list is unsuccessful.

2. The upper limit of the online user list that IAM obtains from the database is 20w. If the number of users exceeds 20w, even if limit 200000 is not added after the sql statement, IAM only synchronizes the first 20w results to the online user list.

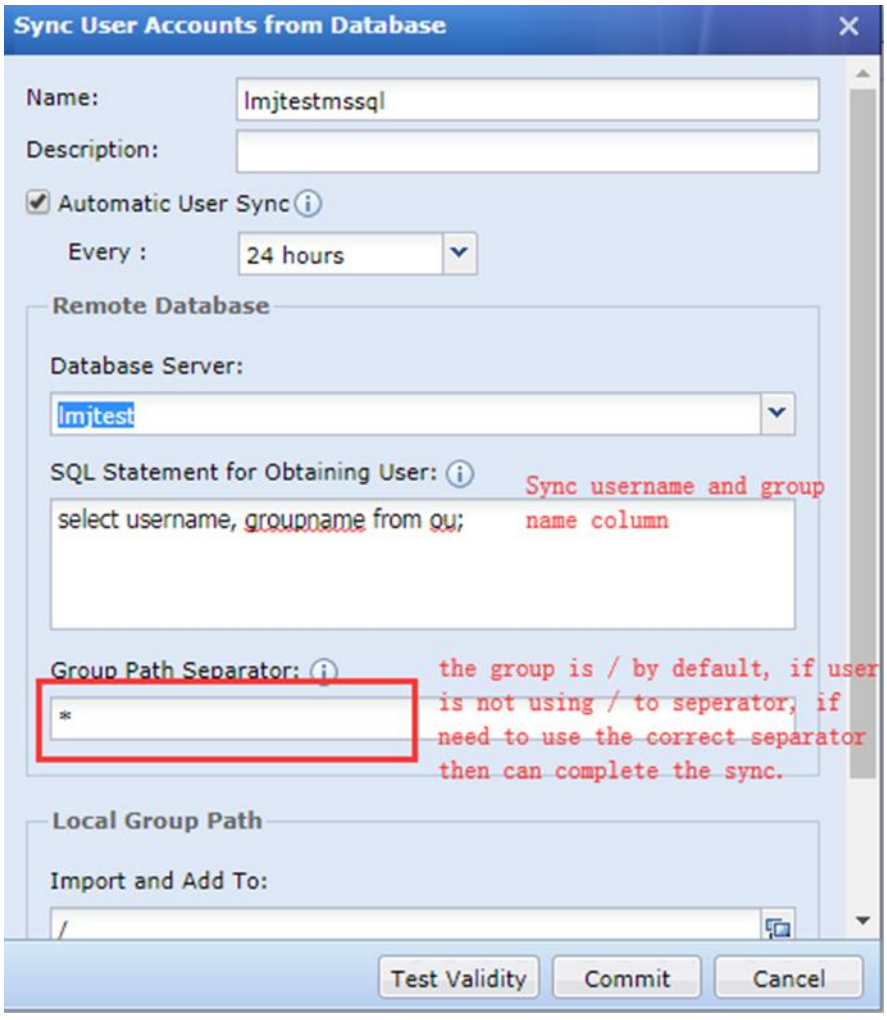
3. The recommended interval for obtaining the list of authenticated users is 30s. If the interval is too small, IAM performance will be affected. If the interval is too large, the user experience will be affected. (If the user has been authenticated by the customer database system, but the IAM has not been synchronized, the authentication box may pop up or become a temporary user according to different settings of the user authentication policy.)

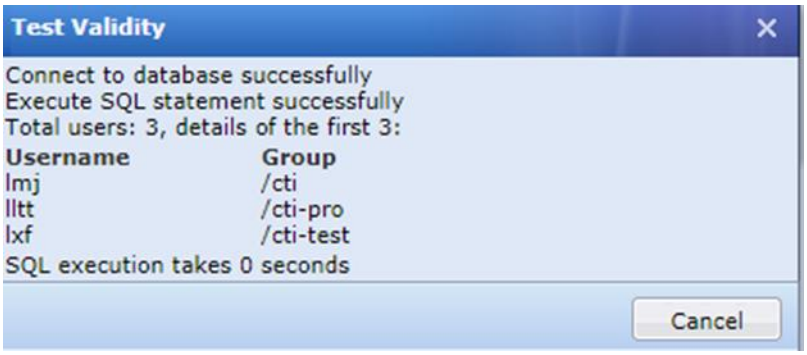
# 4.3 Configuring Automatic User Synchronization (Synchronization Organization Structure)

## 4.3.1 Synchronize the Organizational Structure

Add a "Sync User account from Database" in "User import", fill in the user's sql statement and group path separator, the group path separator refers to the customer's data If there are multiple groups in the table, what symbol is used to separate groups and subgroups, as in the above example, they are separated by dashes:

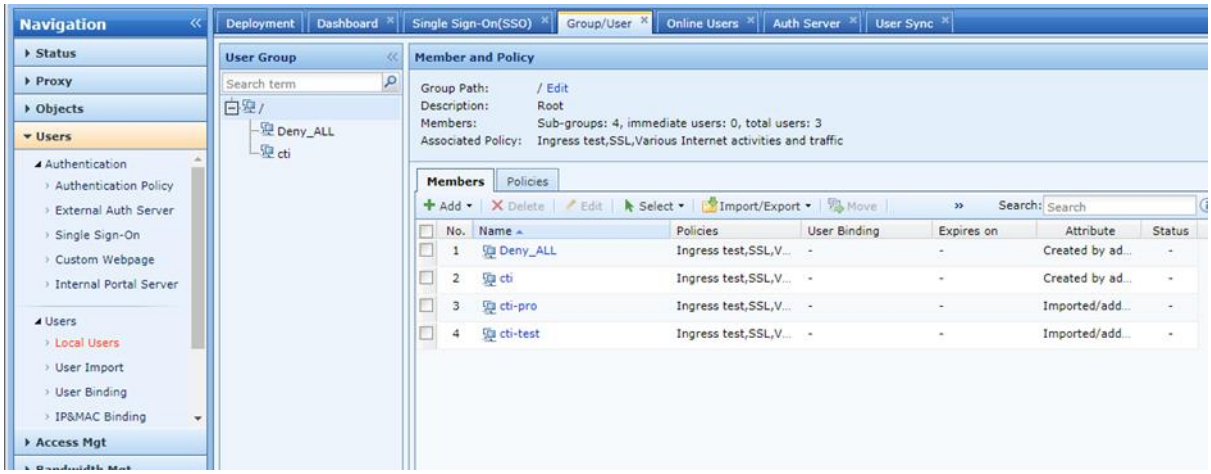
Click "Test Validity" to list the available information:



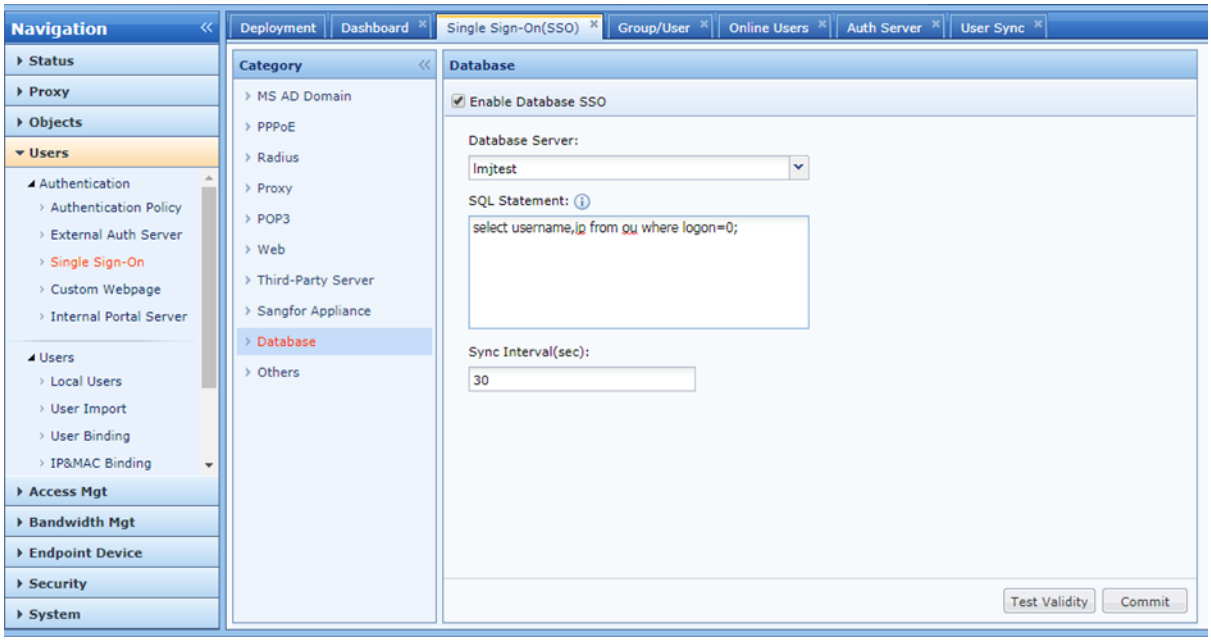

This will list the SQL execution time, this time can be used as a reference to define the timeout time of

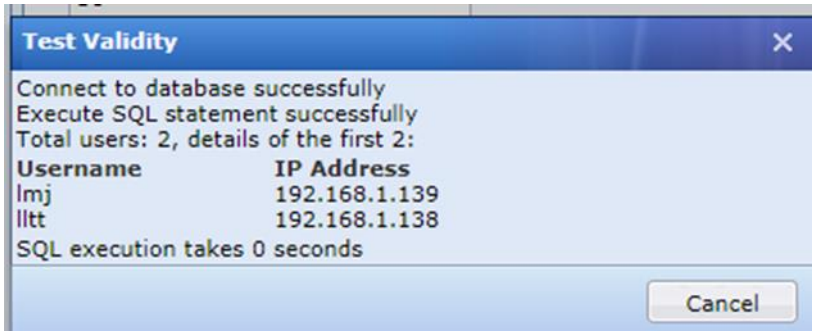
the external authentication server (timeout time is generally recommended to be slightly larger than this value, such as 10s), after the synchronization, you can see the organizational structure information as follows:




The above is the case where a customer's organizational structure and online users are stored in two tables. If the information of the two is in the same table, as long as there is a select statement, it is supported. For example: the structure of the customer's ou table is A logon field is used to identify whether the user is online. If logon = 0, the user is online, and then there is no need to provide the onlieuser table to implement the function of extracting online users, as shown in the figure below:


In this case, the SQL statement of the user authentication department can be filled as follows:






# Chapter 5 Precaution

1. This document only lists the configuration of the database single sign-on. Other configurations are the same as other authentication methods. For example, the authentication policy needs to be configured according to customer requirements.

2. You can only synchronize online users without synchronizing the organizational structure. If the user is not in the organizational structure, follow the new user authentication process, but it can only be added to the specified group, which cannot reflect the organizational structure. If synchronization is configured later, as long as the user attributes are not changed to self-built users, they can still be synchronized to the corresponding structure.

3. The online user list only supports two columns of "user name" and "ip" address. If the user has more attributes, such as identifying whether the user is disabled, etc., synchronization is currently not supported. Users synced by default are enabled and never expire.

4. The process of logging out of the user from the IAM is similar to the process of logging in. When there is no user in the result returned by the select statement, the IAM removes the user from the online user list. This process is transparent to the user. I will not go into details.

5. Other configurations related to database authentication can be understood literally, without explaining them one by one, you can refer to the user manual later.

6. This implementation method is that the IAM periodically obtains online users from the database server, instead of the IAM server real-time perception of each user authenticated by the database server, so there will be a little delay in IAM authentication.

SANGFOR