SANGFOR

IAM

Databases SSO Configuration Guide

Version 12.0.18

Perubahan Catatan

Tanggal	Deskripsi Perubahan
27 Dec , 2019	Version 12.0.18 Bahasa document release.

Daftar Isi

Bab 1 Pengenalan Fungsiapter

Database authentication IAM11.0 mengacu pada urutan informasi otentikasi yang disimpan dalam sistem basis data klien yang sudah ada. IAM11.0 mengonfigurasi pernyataan kueri SQL pada antarmuka IAM untuk secara aktif meminta daftar pengguna dan pengguna yang di otentikasi dalam sistem database. Dan di sinkronkan ke struktur organisasi IAM dan daftar Online user, sehingga ketika pengguna melewati Database Authentication, yaitu otentikasi pengguna IAM, pengguna diganti dari sistem Database Authentication, dan penggantian pada IAM juga otomatis selesai (Single Sign On / Diharapkan).

Jenis database yang didukung saat ini adalah oracle, ms sql server, db2 dan mysql.

Bab 2 Skenario Aplikasi

Ketika pengguna memiliki sistem otentikasi sendiri untuk otentikasi, latar belakang basis data adalah oracle, ms sql server, db2, dan mysql, dll. Dan ada tabel online user dalam database, IAM dapat digunakan bersama dengan database untuk masuk.

Bab 3 Kondisi yang Diperlukan

Untuk menentukan apakah klien dapat menggunakan metode Database Authentication, Anda dapat merujuk pada kondisi berikut:

1. Pengguna memiliki sistem database yang digunakan untuk mengelola informasi pengguna, seperti oracle, ms sql server, db2 atau mysql.
2. Online user dapat ditanyai dari database dengan memilih pernyataan, dan kumpulan hasil yang diekstrak berisi dua kolom: "nama pengguna" dan "alamat ip".
3. Jika Anda perlu menyinkronkan pengguna dan struktur organisasi, Anda dapat menggunakan pernyataan pilih untuk menanyakan semua pengguna dari database dan menanyakan grup pengguna (jika Anda tidak perlu menyinkronkan grup, Anda tidak perlu menanyakan grup pengguna mana).
4. Pelanggan diharuskan untuk menyediakan akun dalam database, yang dapat memiliki izin pilih pada tabel atau tampilan tabel data di atas.
5. IAM dapat berkomunikasi dengan server secara normal (IAM secara aktif terhubung ke port yang sesuai dari server database untuk memicu sinkronisasi, dan tidak mengharuskan data otentikasi pengguna ke server datab ase harus melewati IAM).

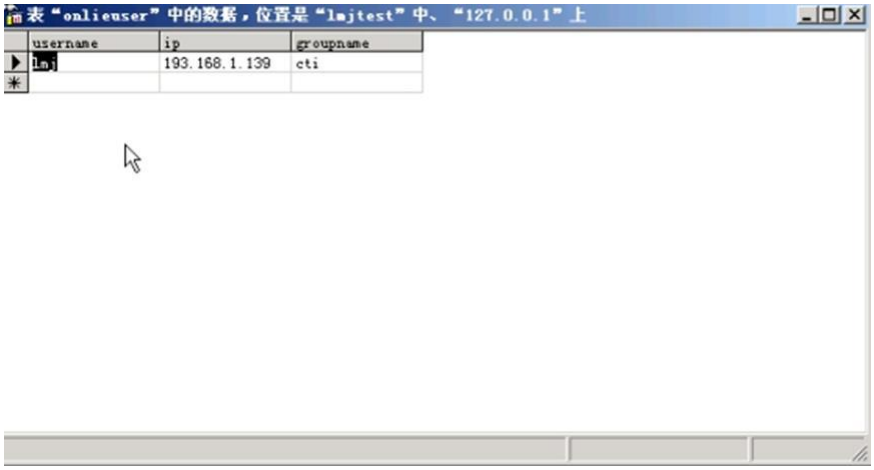
Bab 4 Ide Konfigurasi

4.1 Sebelum Persiapan Konfigurasi

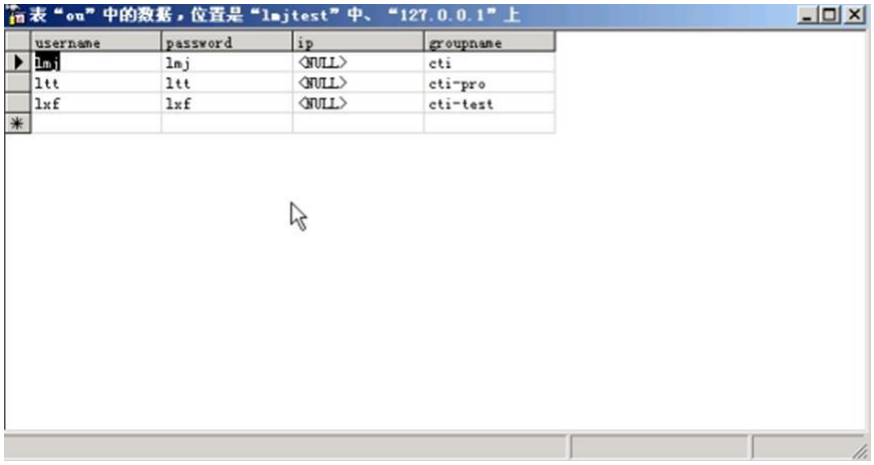
Sebelum mengonfigurasi, lihat bagian "Persyaratan" di atas untuk mendapatkan beberapa informasi dari pelanggan, seperti jenis basis data, kode server basis data, struktur tabel data, nama kolom kunci, dll. Dan minta pelanggan untuk memberikan akun basis data.

Pelanggan ini umumnya memahami database itu sendiri dan dapat menyediakannya secara langsung. Jika kita perlu menemukannya sendiri, kita bisa merujuk pada contoh berikut.

Bab ini mensimulasikan lingkungan klien. Asumsikan bahwa alamat IP server database klien adalah 193.168.1.124, tipe database adalah MS SQL, dan database untuk mengelola informasi pengguna bernama lmjtest. Diketahui bahwa informasi Online user pelanggan disimpan dalam tabel Online user, dan informasi struktur organisasi disimpan. Pada tabel ou, struktur kedua tabel tersebut adalah sebagai berikut:



Struktur tabel ou untuk menyimpan informasi struktur organisasi:

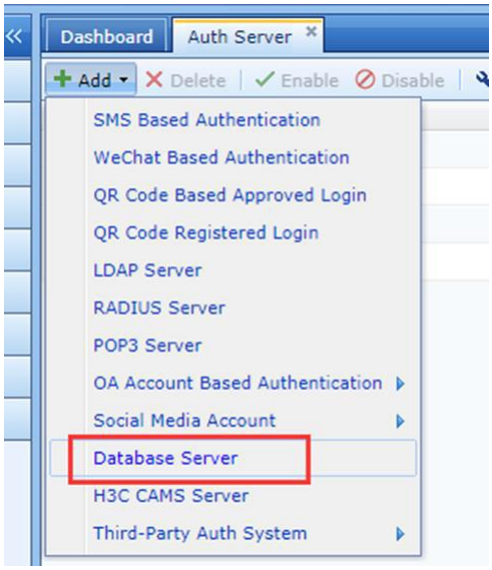


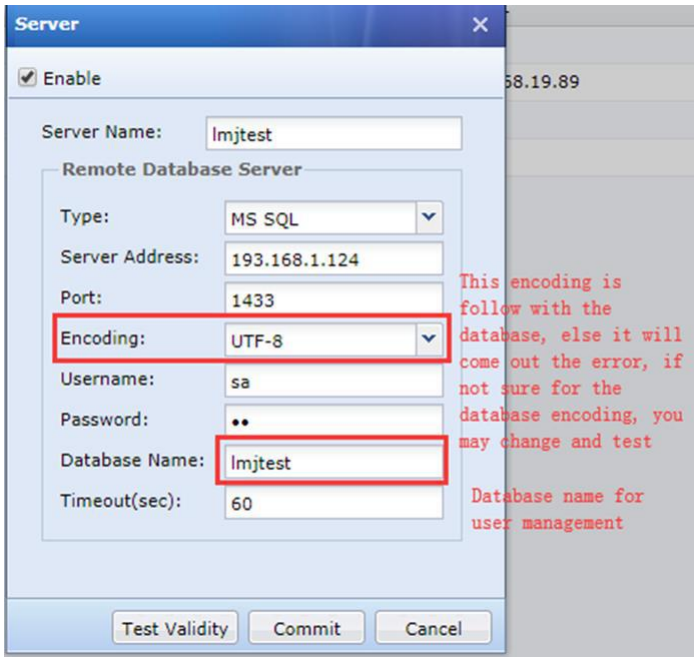
Dapatkan akun database. Dalam contoh ini, akun sa digunakan secara langsung. Faktanya, hanya pengguna yang memiliki izin kueri pada tabel data yang dapat digunakan. (Jika MS SQL perlu mengaktifkan otentikasi campuran).

Dapatkan pengkodean database. Jenis database yang berbeda mendapatkan pengkodean database yang berbeda. Misalnya, mysql bisa mendapatkan jenis pengkodean database dengan memasukkan perintah status.

4.2 Mengonfigurasi Single Sign On untuk Database Authentication (Sinkronisasi Pengguna Online)

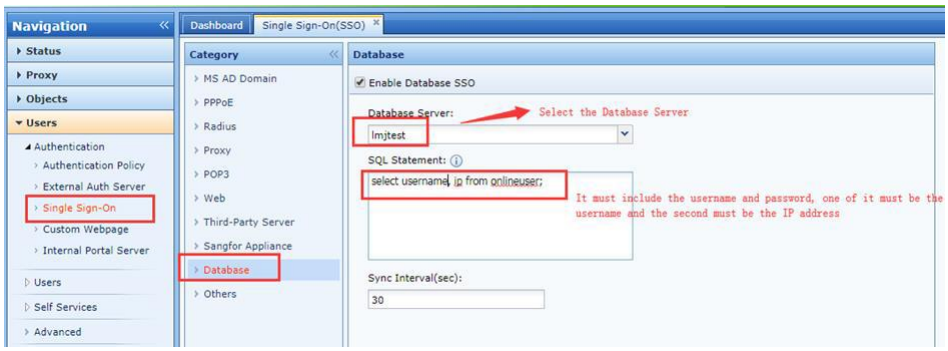
Tentukan server otentikasi eksternal, "User and Policy Management" - "User Authentication" - "External Authentication Server", tambahkan jenis database server otentikasi eksternal dan konfigurasikan, berikan perhatian khusus pada konfigurasi "database encoding" dan pengkodean yang digunakan oleh database adalah konsisten. "Timeout" mungkin perlu disesuaikan dengan jumlah pengguna. Standarnya adalah 60-an, sebagai berikut:



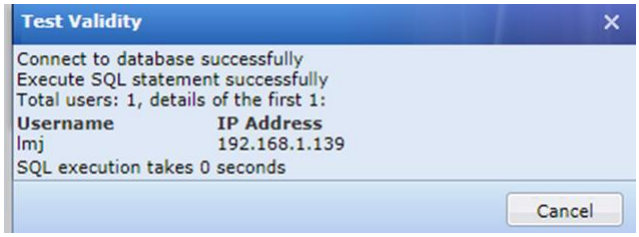


4.2.1 Aktifkan Single Sign on untuk Database Otentikasi

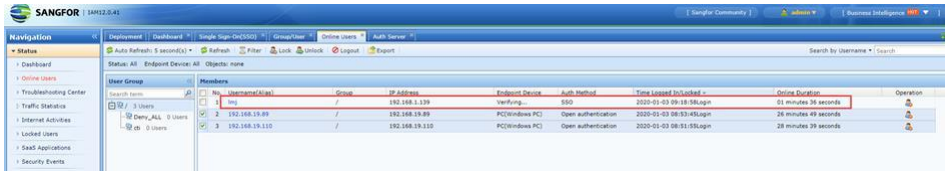
Pilih "Single Sign On" - "Database" - pilih "Enable Database SSO" dan pilih server otentikasi eksternal lmjtest yang baru saja ditentukan.



Klik "Test validity" untuk melihat hasil eksekusi pernyataan SQL, dan klik "Submit" untuk menyelesaikan konfigurasi.



Saat ini, IAM akan segera menyinkronkan daftar Online user secara otomatis. Konfigurasi Single Sign On database selesai pada langkah ini. Saat ini, daftar Online user dapat dilihat. Pengguna lmj sudah ada dalam daftar online user IAM. Metode otentikasi adalah Single Sign On:



Catatan:

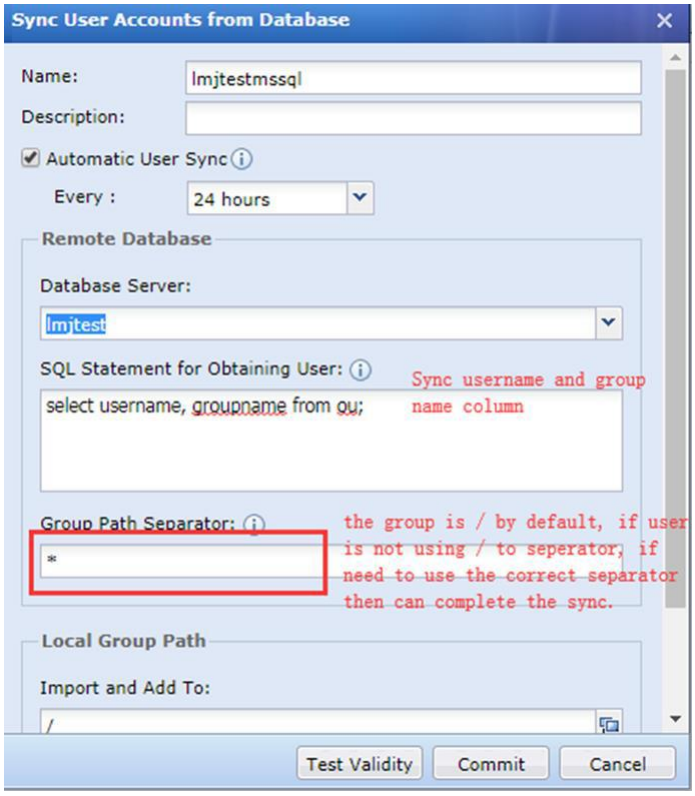
1. IAM hanya mendukung dua kolom nama pengguna dan alamat ip untuk user online, dan dalam kumpulan hasil yang diekstrak, kolom pertama adalah username dan kolom kedua adalah ip. Jika pernyataan sql pada gambar di atas adalah pilih ip, bentuk nama Online useruser, Dengan cara ini, validitas pengujian berhasil, tetapi sinkronisasi daftar Online user tidak berhasil.
2. Batas atas daftar Online user yang diperoleh IAM dari database adalah 20w. Jika jumlah pengguna melebihi 20w, meskipun batas 200000 tidak ditambahkan setelah pernyataan sql, IAM hanya menyinkronkan hasil 20w pertama ke daftar Online user.
3. Interval yang disarankan untuk mendapatkan daftar pengguna terotentikasi adalah 30 detik. Jika intervalnya terlalu kecil, kinerja IAM akan terpengaruh. Jika intervalnya terlalu besar, pengalaman pengguna akan terpengaruh. (Jika pengguna telah diautentikasi oleh sistem database pelanggan, tetapi IAM belum disinkronkan, kotak otentikasi dapat muncul atau menjadi pengguna sementara sesuai dengan pengaturan yang berbeda dari kebijakan otentikasi pengguna.)

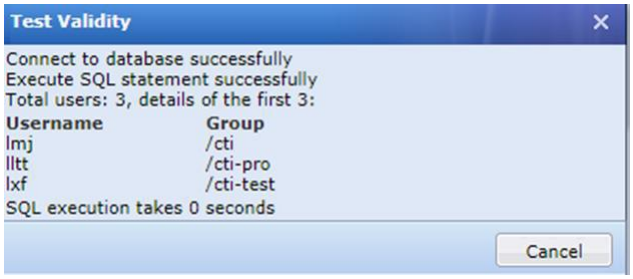
4.3 Mengonfigurasi Sinkronisasi Pengguna Otomatis (Struktur Organisasi Sinkronisasi)

4.3.1 Sinkronisasi Struktur Organisasi

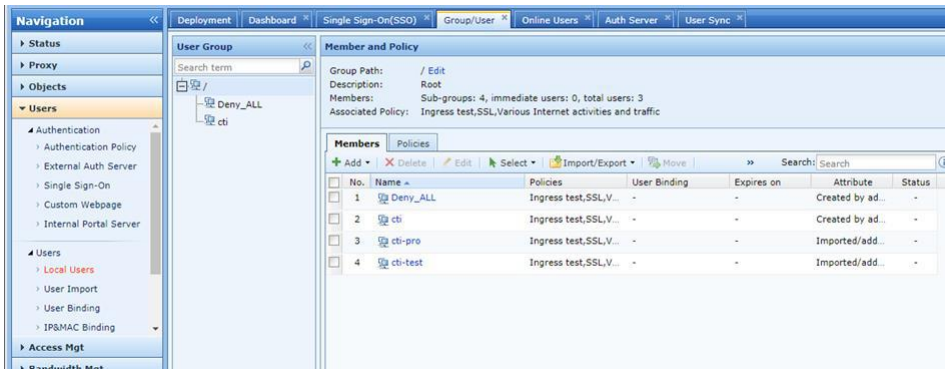
Tambahkan “Sync User account from Database” di “User import”, isi pernyataan sql pengguna dan pemisah jalur grup, pemisah jalur grup mengacu pada data pelanggan. Jika ada beberapa grup dalam tabel, simbol apa yang digunakan untuk memisahkan grup dan subgrup, seperti pada contoh di atas, mereka dipisahkan dengan tanda hubung:

Klik "Test Validity" untuk mendaftar informasi yang tersedia:



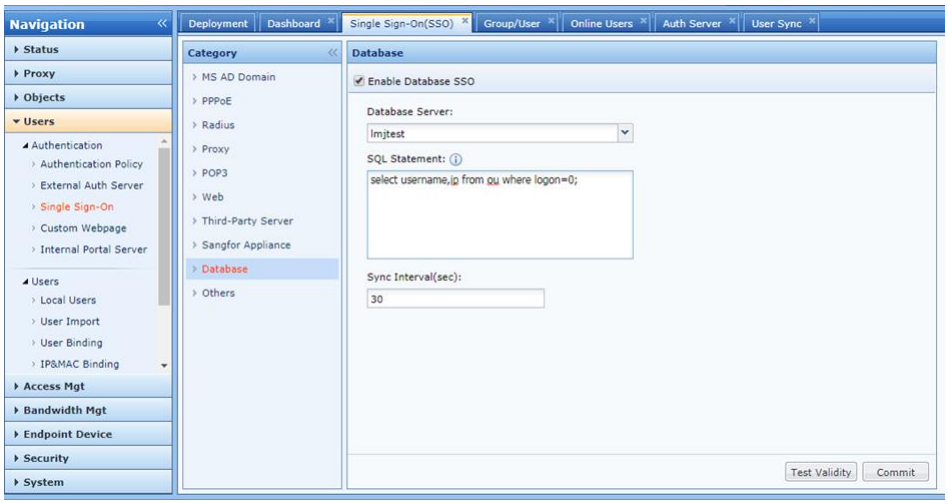


Ini akan mencantumkan SQL execution time, kali ini dapat digunakan sebagai referensi untuk menentukan waktu tunggu server otentikasi eksternal (waktu tunggu biasanya disarankan agar sedikit lebih besar dari nilai ini, seperti 10 detik), setelah sinkronisasi, Anda dapat melihat informasi struktur organisasi sebagai berikut:



Di atas adalah kasus di mana struktur organisasi pelanggan dan Online user disimpan dalam dua tabel. Jika informasi dari keduanya ada di tabel yang sama, selama ada pernyataan pilih, itu didukung. Misalnya: struktur tabel pelanggan ou adalah field logon digunakan untuk mengidentifikasi apakah pengguna sedang online. Jika logon = 0, pengguna sedang online, dan kemudian tidak perlu menyediakan tabel satu pengguna untuk mengimplementasikan fungsi mengekstrak Online user, seperti yang ditunjukkan pada gambar di bawah ini:

Dalam kasus ini, pernyataan SQL dari departemen otentikasi pengguna dapat diisi sebagai berikut:



Bab 5 Pencegahan

1. Dokumen ini hanya mencantumkan konfigurasi database Single Sign On. Konfigurasi lain sama dengan metode otentikasi lainnya. Misalnya, kebijakan otentikasi perlu dikonfigurasi sesuai dengan kebutuhan pelanggan.
2. Anda hanya dapat menyinkronkan Online user tanpa menyinkronkan struktur organisasi. Jika pengguna tidak berada dalam struktur organisasi, ikuti proses otentikasi pengguna baru, tetapi hanya dapat ditambahkan ke grup tertentu, yang tidak dapat mencerminkan struktur organisasi. Jika sinkronisasi dikonfigurasi nanti, selama atribut pengguna tidak diubah menjadi pengguna yang dibuat sendiri, mereka masih dapat disinkronkan ke struktur yang sesuai.
3. Daftar Online user hanya mendukung dua kolom alamat "username" dan "ip". Jika pengguna memiliki lebih banyak atribut, seperti mengidentifikasi apakah pengguna dinonaktifkan, dll. Sinkronisasi saat ini tidak didukung. Pengguna yang disinkronkan secara default diaktifkan dan tidak pernah kedaluwarsa.
4. Proses keluar dari pengguna dari IAM mirip dengan proses masuk. Ketika tidak ada pengguna hasil query, IAM menghapus pengguna dari daftar Online user. Proses ini transparan bagi pengguna.
5. Konfigurasi lain yang terkait dengan Database authentication dapat dipahami secara harfiah, tanpa menjelaskannya satu per satu, Anda dapat merujuk ke manual pengguna nanti.
6. Metode implementasi ini adalah bahwa IAM secara berkala mendapatkan Online user dari server basis data, bukan server IAM yang menunjukkan persepsi waktu nyata setiap pengguna yang diautentikasi oleh server basis data, sehingga akan ada sedikit penundaan dalam otentikasi IAM.