

Integrasi SQL Server 2000 dan Active Directory Service (ADS)

Bondhan Rio P

bondhan@skomtek.com

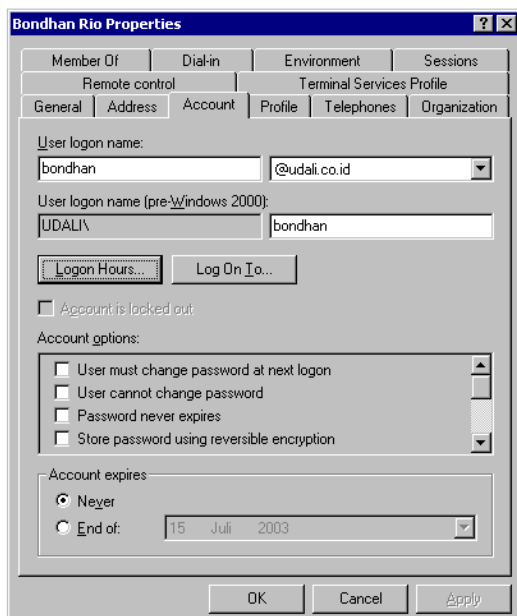
Lisensi Dokumen:

Copyright © 2003 IlmuKomputer.Com

Seluruh dokumen di IlmuKomputer.Com dapat digunakan, dimodifikasi dan disebarkan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang, kecuali mendapatkan ijin terlebih dahulu dari IlmuKomputer.Com.

Active Directory Service

Directory service merupakan sebuah service yang digunakan untuk menghubungkan semua resource yang ada pada jaringan dan berperan semacam sebuah buku telpon raksasa. Directory service pada NT 4 mempunyai peran penting dalam mengatur proses logon dan administrasi security secara terpusat.



dapat memiliki satu atau lebih controller ADS.

Pada generasi DS yang lebih lanjut, Microsoft memperkenalkan ADS yang disertakan bersama OS Windows 2000 server. ADS generasi kedua ini mempunyai kemampuan yang jauh lebih besar daripada pendahulunya. Selain itu Microsoft juga mempermudah administrasi dari ADS dengan menggunakan system hierarchical view dan multimaster.

Beberapa konsep yang berbeda antara DS pada NT 4 dan ADS pada W2KSRV adalah system domain controller yang diterapkannya. Pada NT. 4 kita mengenal dua jenis Domain Controller, yaitu PDC sebagai DC utama yang handle seluruh domain, dan BDC yang berguna sebagai replicate atau backup controller.

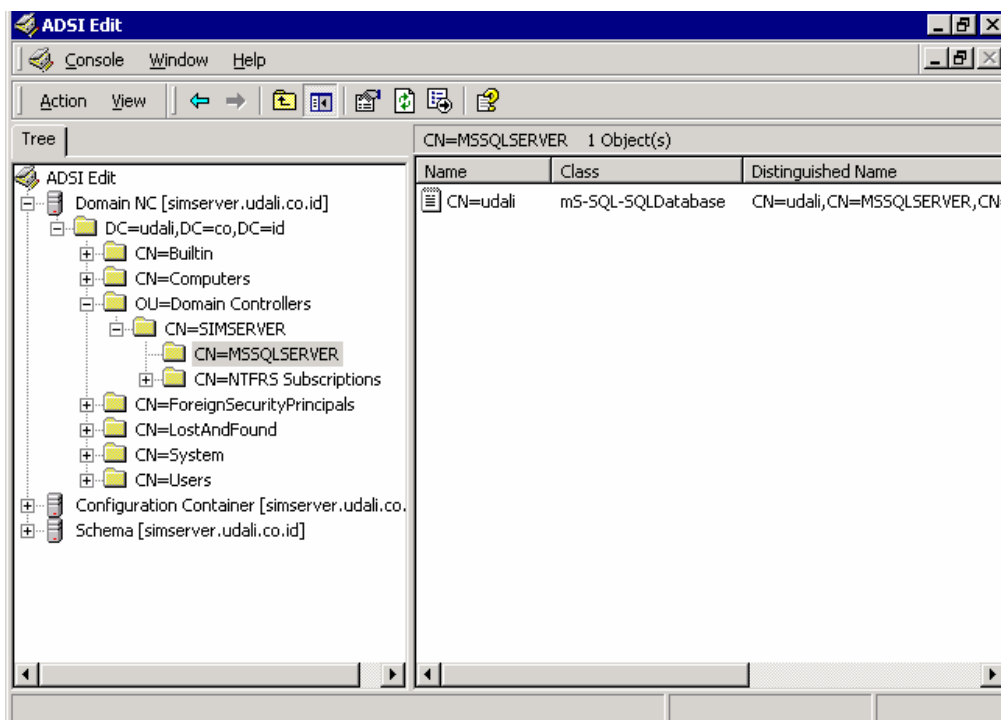
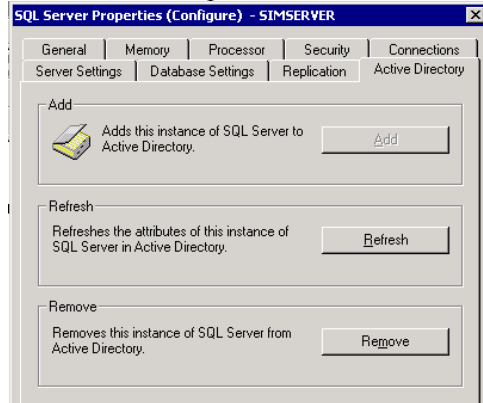
Pada ADS tidak lagi mengenal PDC dan BDC, akan tetapi semua controller mempunyai kemampuan yang sama. Hanya saja pembagian domain dibagi menjadi domain, forest, trees. Masing-masing group

SQL Server 2000 & Active Directory

SQL Server 2000 mempunyai kemampuan untuk dapat mendukung ADS pada Windows 2000. Dengan adanya integrasi SQL Server kepada ADS, maka penempatan server database, publikasi ataupun servis analisa dapat dilakukan dengan bebas. Tidak harus berada pada satu DMZ. Koneksi tidak lagi bergantung pada IP Address ataupun namebios. Dengan begitu keberadaan server akan lebih transparan, sehingga juga akan lebih menyulitkan gangguan keamanan terhadap data.

Dengan menggunakan sebuah aplikasi yang telah mendukung Active Directory Service Interfaces (ADSI), maka sebuah aplikasi akan langsung dapat menemukan dan terhubung dengan SQL Server dan memanfaatkan semua fasilitas dari DBMS. Seperti halnya publikasi dan database, dengan catatan bahwa kesemuanya telah didaftarkan pada ADS.

Pada ADS anda dapat mendaftarkan server, database dan publikasi. Pada contoh berikut pada SQL Server terdapat sebuah database yang bernama "udali", setelah diregistrasikan pada ADS maka dikenali sebagai object dengan class **MS-SQL-SQLDatabase**. Sedangkan SQL Server-nya sendiri dicatat dengan nama "MSSQLSERVER" dan dikenali sebagai object dengan class **MS-SQL-SQLServer**



Transparansi yang di berikan oleh ADS terhadap SQL Server 2000 memungkinkan database untuk dipindahkan antar server atau site tanpa mengganggu aplikasi ataupun service yang pada saat yang sama sedang memanfaatkannya.



Untuk melakukan koneksi database client menggunakan provider “OLE DB Provider for Microsoft Directory Service”.

Contoh connection string yang adalah sebagai berikut

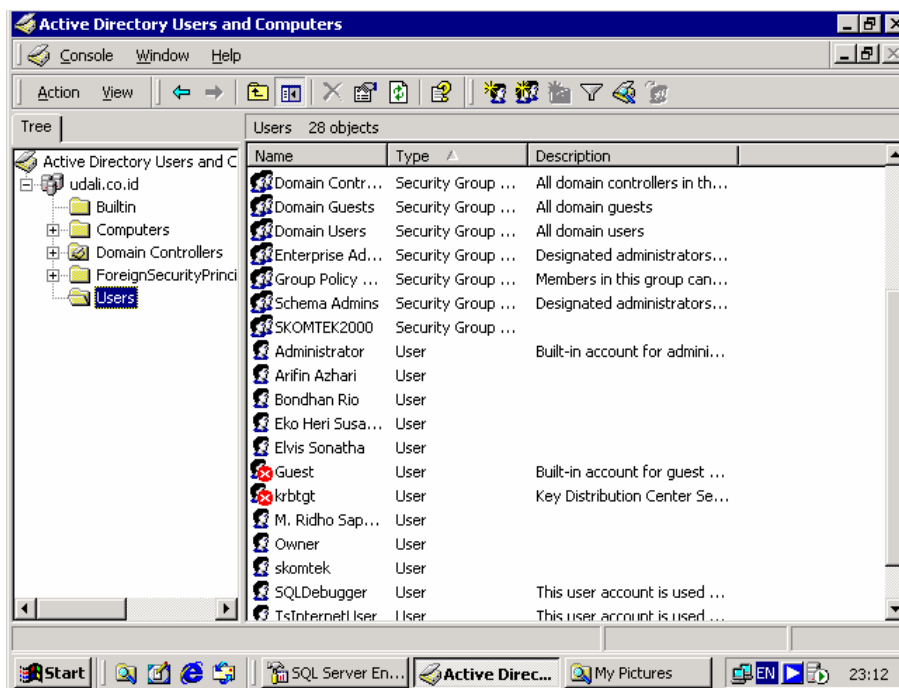
```
“Provider=ADsDSOObject;Encrypt Password=False;Integrated Security=SSPI;
Mode=ReadWrite; Bind Flags=0; ADSI Flag=-2147483648”
```

Beberapa schema ADS yang dipergunakan oleh SQL Server 2000 adalah sebagai berikut.

1. **MS-SQL-SQLServer**, Untuk mengidentifikasi object SQL Server.
2. **MS-SQL-SQLPublication**, Untuk mengidentifikasi publikasi dari SQL Server replication.
3. **MS-SQL-SQLDatabase**, Identifikasi database pada SQL Server database.
4. **MS-SQL-OLAPServer**, Identifikasi SQL Server Analysis Server.

Active Directory Users and Computers

Pada saat kita mengkonfigurasi sebuah SQL Server untuk mempunyai beberapa account yang terpisah, maka kita dapat melakukannya di SQL Server Enterprise Manager. Akan tetapi jika kita mengkonfigurasi SQL Server untuk berintegrasi dengan keamanan Windows 2000, maka user account akan kita buat pada konsol Active Directory Users and Computers.



Cara kedua lebih efisien dan efektif untuk dilakukan. Selain kita tidak perlu mengulang pekerjaan, keamanan dan hak akses dapat diatur dengan lebih mudah.

Konfigurasi SQL Server 2000

Untuk dapat mempergunakan fasilitas keamanan dari ADS secara keseluruhan SQL Server 2000 harus dikonfigurasi terlebih dahulu untuk dapat menerima delegasi. Untuk dapat menggunakan keamanan account dari delegasi, SQL Server harus memiliki Service Principal Name (SPN) yang diberikan oleh administrator domain pada Windows 2000. Kemudian SPN akan dihubungkan dengan service account yang ada pada SQL Server.

SPN ini juga berfungsi untuk membuktikan bahwa SQL Server telah diverifikasi bahwa dia aktif pada sebuah dan pada socket komunikasi tertentu.

Setup SPN dapat dilakukan dengan cara :

```
setspn -A MSSQLSvc/Host:port serviceaccount|sqlaccount
```

Contohnya seperti berikut :

```
setspn -A MSSQLSvc/simserver.udali.co.id sa
```

Selain itu kita juga harus mengatur TCP/IP untuk memakai use security account delegation. Untuk hal ini kita tidak dapat mempergunakan named pipes karena SPN mempergunakan socket TCP/IP khusus. Untuk mengatur port yang kita akan kita pergunakan :

```
setspn -A MSSQLSvc/simserver.udali.co.id:1122 bondhan
```