

Implementasi *Single Sign-On* Berbasis *Active Directory* Sebagai Basis Data dan Layanan Direktori

Implementation of Active Directory Single Sign-On as Database and Directory Service

Salman Farizy

Dosen STMIK Eresha/Pranata Indonesia

Email : sfarizy06@hotmail.com

Abstrak --- Sudah banyak kejadian serangan keamanan sistem informasi baik itu dari dalam organisasi kita sendiri ataupun dari luar organisasi, terjadi karena perubahan teknologi yang begitu pesat dan cepatnya, internet yang begitu meluas dan terbuka membuat banyak kasus yang terjadi saat ini, serangan para hacker di 'trigger' atau dipicu karena masih banyaknya perusahaan belum 100% menyadari betapa sangat pentingnya keamanan sistem informasi yang harus diterapkan dan dijalankan atau kemungkinan lain akan terjadi pihak IT department seperti Infrastruktur, administrator jaringan, database, system engineer, technical support dan lain sebagainya agak kurang memperhatikan betapa sangat pentingnya keamanan sistem informasi yang dikelola di organisasi tersebut. sehingga membuat celah para 'hacker' untuk menyerang sistem dan akhirnya akan merugikan baik dari sisi operasional maupun finansial.

Salah satu alternatif pemecahan masalah atau satu solusi yang ditawarkan yaitu dengan menggunakan SSO (Single Sign On) dalam sebuah lingkungan jaringan, dimana menyimpan credential yang terdapat pada server pusat atau dalam sebuah direktori selain itu juga sistem ini juga harus memiliki suatu kemampuan replikasi pada penyimpanan credential dan punya metode dari penyimpanan tersebut melalui 'cache'.

Dengan melakukan log in dan memasukan password, user cukup sekali saja melakukan proses autentikasi untuk mendapatkan " Access rights" atau hak akses terhadap semua layanan yang terdapat di dalam lingkup jaringan dan lingkup Active Directory (AD).

Kata Kunci : *Single Sign on, Domain Controller, Active Directory* .

Abstract --- There have been many incidents of information system security attacks both from within our own organization and from outside the organization, occurred because of rapid and rapid technological changes, the internet that is so widespread and open makes many cases happen today, the attacks of hackers are 'triggered' or triggered because there are still many companies not yet 100% aware of the importance of information system security that must be implemented and carried out or other possibilities will occur IT departments such as Infrastructure, network administrators, databases, system engineers, technical support and so on pay less attention to how very the importance of information system security managed in the organization. so that it creates a gap for 'hackers' to attack the system and ultimately will be detrimental both in terms of operational and financial.

One alternative problem solving or one solution offered is to use SSO (Single Sign On) in a network environment, where storing credentials contained on a central server or in a directory otherwise this system must also have a replication capability on credential storage and have a method of storing it via 'cache'.

By logging in and entering passwords, the user can just once do the authentication process to get "Access rights" or access rights to all services contained in the network scope and scope of Active Directory (AD).

Keywords : *Single Sign on, Domain Controller, Active Directory*

1. PENDAHULUAN

Sudah banyak didengar dan dialami akhir – akhir ini kejadian serangan keamanan sistem informasi (KSI) baik itu dari dalam organisasi kita sendiri ataupun sesuatu yang dari luar organisasi, terjadi karena perkembangan teknologi yang begitu cepatnya, internet yang begitu meluas dan terbuka membuat banyak kasus yang terjadi saat ini, serangan para *hacker* di ‘trigger’ atau dipicu karena masih banyaknya perusahaan belum 100% menyadari betapa pentingnya keamanan sistem informasi yang harus diterapkan dan dijalankan atau kemungkinan lain bisa juga terjadi pihak IT department seperti Infrastruktur, administrator jaringan, database, system engineer, technical support dan lain sebagainya agak kurang memperhatikan betapa sangat pentingnya keamanan sistem informasi yang dikelola di organisasi tersebut. sehingga membuat celah para ‘hacker’ untuk menyerang sistem dan akhirnya akan merugikan baik dari sisi operasional maupun finansial.

Alternative yang coba ditawarkan adalah dengan menerapkan atau menggunakan SSO (Single Sign On) dalam sebuah lingkungan jaringan yang menyimpan credential yang terdapat pada server pusat atau dalam sebuah direktori.

Sistem ini juga harus memiliki suatu kemampuan replikasi pada penyimpanan credential dan punya metode dari penyimpanan tersebut melalui ‘cache’.

Dengan melakukan log in dan memasukan password, user cukup sekali saja melakukan proses autentikasi untuk mendapatkan “ Access rights” atau hak akses terhadap semua layanan yang terdapat di dalam lingkup jaringan dan lingkup Active Directory (AD).

Active directory itu sebenarnya suatu database yang menyimpan informasi seperti nama, alamat, nomor telephone dan lain sebagainya yang terindex sehingga memudahkan proses jika akan dilakukan pencarian.

2. PEMBAHASAN

Active Directory (AD) adalah implementasi LDAP directory services yang digunakan dalam lingkungan Microsoft.

AD sendiri sebenarnya merupakan suatu database terdistribusi yang dapat mereplikasi ke semua Domain Controller (DC) pada suatu jaringan. Isi dari database tersebut menyimpan informasi berupa :

- + User.
- + Computer.
- + Group.
- + Policy.
- + Aplikasi.
- + Printer
- + Object directory lain.

Secara garis besar ada beberapa fungsi dari AD adalah :

- + Pengelolaan network resources dapat dikontrol secara terpusat oleh administrator, hanya user atau pengguna yang mempunyai hak akses atau ‘access right’ yang dapat mengakses network resources tersebut. Selain itu Administrator juga dapat mendelegasikan wewenang kepada pengguna lain.
- + Mengoptimalkan penggunaan network traffic dan mengamankan objek dalam suatu struktur logical, misalnya saja pada saat user log in ke jaringan akan di arahkan atau diotentikasikan oleh DC yang terdekat, selain itu replikasi antar DC dapat diatur penggunaannya pada saat penggunaan bandwidth dalam posisi iddle atau rendah dengan membuat schedule antar DC .
- + Active directory terdiri dari komponen – komponen yang membentuk struktur logical dan physical.
- + Implementasi atau penerapan AD dapat dilakukan untuk skala kecil maupun enterprise.

A. Pengertian Active Directory (Ad) Secara Logical.

Apa saja komponen yang dimiliki oleh AD secara logical ?

- + Schema/Object.

Komponen AD yang mendefinisikan dan menginformasikan class object dan attribut object, dimana class object mendefinisikan objek baru yang bisa kita buat pada AD misalnya saja computer class dan user class, sedangkan didalam attribut objek itu sendiri berisi suatu Informasi apa saja yang dapat disimpan pada setiap class objek, seperti pada user class terdapat display name, email address, dll.

B. Organizational Unit (OU)

OU adalah salah satu dari group khusus yang memungkinkan untuk mengelompokkan user & device, seperti :

- + Mendelegasikan hak akses atas group tersebut kesatu orang yang diberikan wewenang atau tanggung jawab, ambil contoh akan dibuat OU untuk sales departemen., lalu manager atau yang diberi hak akses untuk mengelola departemen tersebut diberikan hak administrasi dan, kegunaannya jika suatu ketika saat ada salah seorang staff dari dept. meminta penggantian password / user tsb sendiri misalnya saja lupa password maka manager tersebut atau yang diberi kuasa dapat melakukannya, tetapi cakupannya hanya mempunyai hak atas dept. itu saja dan tidak untuk departemen yang lain.

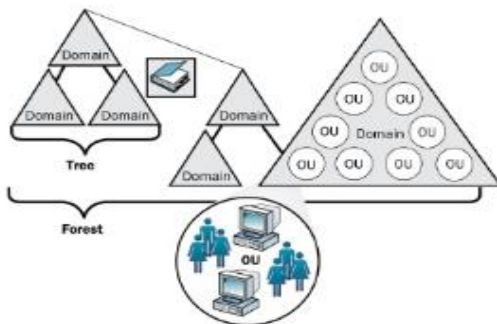
OU biasanya digunakan untuk tujuan diantaranya mengadministrasi seperti pendelegasian dan juga untuk memudahkan pencarian objek. OU merupakan pilihan yang cukup bagus bagi beberapa kantor dengan lokasi yang berbeda atau yang berjenis remote.

Contoh :

PT. Example memiliki 10 branch office. Administrator yang mengelola seluruh sistem tersebut berada di kantor pusat (Head Office). Dengan OU, suatu ketika jika terjadi satu atau beberapa masalah serta kebutuhan di kantor cabang, administrator tidak perlu datang secara khusus untuk memperbaikinya, cukup user account yang diberi mandat / wewenang oleh seorang administrator sebagai sub administrator di OU tersebut yang melakukannya.

C. Domain

Domain adalah sekumpulan objek seperti user, komputer, group, printer, aplikasi dan network resource lainnya, biasanya digunakan untuk mengelompokkan dan memanager AD objek dalam satu organisasi, dapat juga untuk memberikan policy tertentu pada satu OU yang didalamnya bisa terdapat objek-objek yang lain, pada 1 Domain pasti ada minimal 1 Domain Controller yang terinstall, dalam satu DC hanya bisa ada satu Domain.



Gambar 1. Active Directory Logical Component

D. Domain Tree

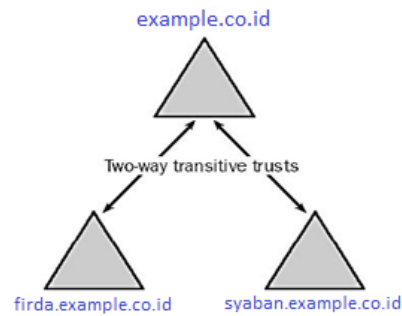
Susunan Hirarki dari domain - domain dalam satu forest, yang penulisan namanya contiguous dengan parentnya.

Contoh:

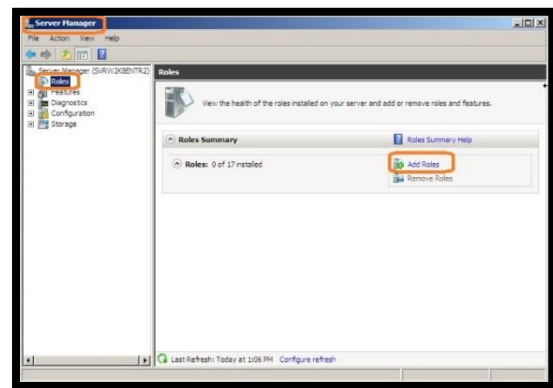
- parentnya → example.co.id
- childnya → firda.example.co.id.
- childnya → syaban.example.co.id.

Domain sendiri dapat memiliki beberapa sub domain yang dapat dibagi lagi berdasarkan kebutuhan masing – masing organisasi, yang mana

hubungan antara domain dan sub domain bersifat *Two-way Trust* maksudnya memungkinkan user account pada domain root dapat mengakses sub domain dan sebaliknya.



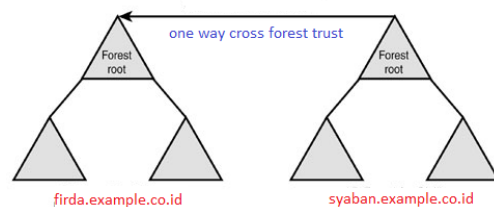
Dengan demikian, user account yang ada pada organisasi atau perusahaan example.co.id dapat mengakses firda.example.co.id, dan sebaliknya. Tree sendiri adalah kumpulan dari domain dan sub domain nya. Kumpulan ini disebut Tree karena bentuk hubungannya yang seperti pohon, yang ditunjukkan pada gambar dibawah.



Gambar 2. Domain Tree

E. Forest

Merupakan salahsatu keseluruhan dari AD, termasuk didalamnya domain, juga domain tree, schema, objek maupun OU. Hubungan antara dua Tree dalam satu Forest biasanya mempunyai sifat *One way Trust*.



Gambar 3. Forest

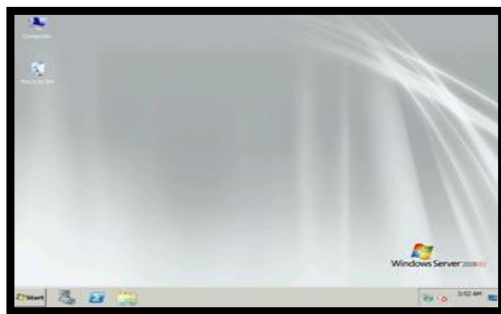
Relasi *One way Trust* bagi seorang user account yang mengakses salah satu Tree dpt juga mengakses Tree lainnya, namun tidak berlaku sebaliknya. Ilustrasi pada gambar ini dapat dilihat dari contoh berikut.

3. IMPLEMENTASI

Untuk bisa menggunakan atau menerapkan AD, hal yang pertama adalah dengan instalasi Windows Server 2008R2 terlebih dahulu sesuai dengan spesifikasi dan skenario ini yang ada sebelumnya, setelah selesai dan silahkan login sebagai administrator :

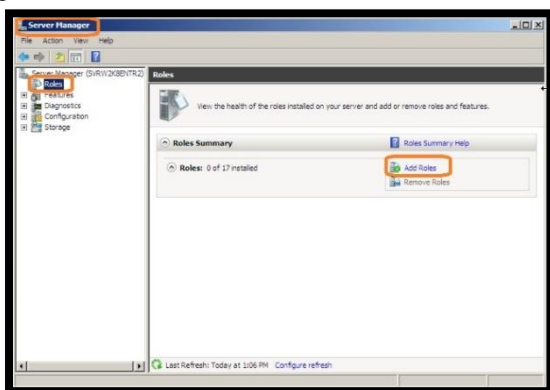


Gambar 4. Menu user logon Untuk tampilan windows server 2008R2



Gambar 5. Tampilan Windows Server

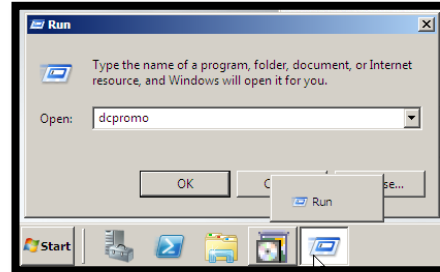
Berikutnya pada taskbar paling bawah click *server manager*, dan pilih “*add role*” untuk instalasi *Active Directory Domain Services* seperti gambar berikut :



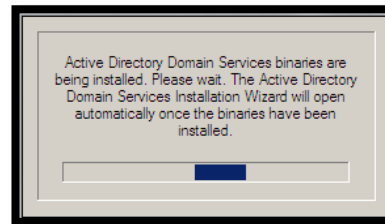
Gambar 6. Server Manager

Pada kotak dialog *Add Roles Wizard* akan ditampilkan konfigurasi yang harus dilakukan sebelum melanjutkan proses instalasi, yaitu mempunyai user name yang berstatus *Administrator* untuk dapat login pada Windows Server tersebut, melakukan konfigurasi dasar seperti TCP/IPv4, update windows, firewall dan

test koneksi pada Windows Server yang digunakan, jangan lupa sebelum proses dilakukan komputer client atau user paling tidak sudah tersambung pada jaringan tersebut untuk memuluskan proses installasi AD, langkah berikutnya adalah, klik tombol *next* untuk melakukan proses selanjutnya pada kotak dialog *Add Roles Wizard*. Selanjutnya klik tombol *start* → *run*. Setelah tampil menu run ketik “*dcpromo*” dan klik tombol *ok*.

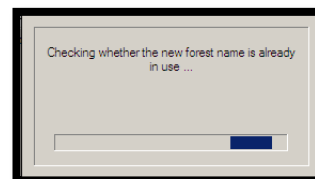
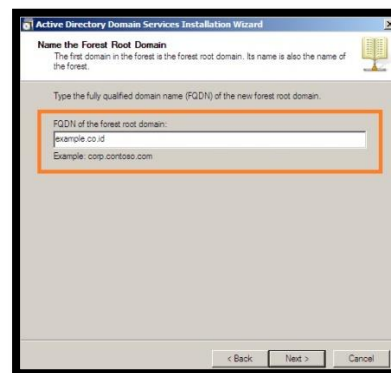


Gambar 7. Instalasi Active Directory maka muncul menu proses instalasi AD.



Gambar 8. Instalasi AD

Proses installasi sedang berlangsung tunggu sampai beres, lalu isi nama domain pada organisasi tersebut yang akan digunakan pada *FQDN* (Full Qualified Domain Name) sebagai catatan dan masukan, gunakan domain organisasi yang sebelumnya sudah didaftarkan pada Internet Service Provider.



Gambar 9. FQDN

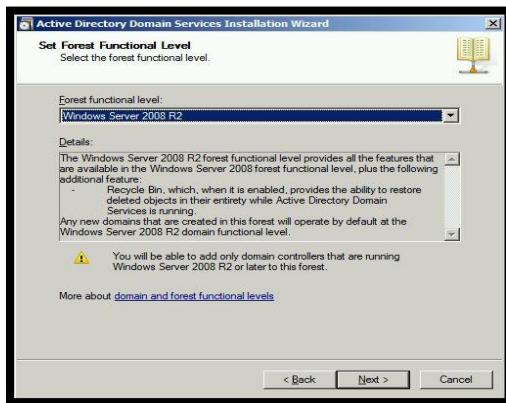
Window selanjutnya akan ditampilkan *Domain NetBIOS* dimana mempunyai fungsi untuk

mendukung sistem operasi sebelumnya seperti versi Windows 2000, Windows 98 dan Windows Melenium, yang akan dihubungkan dengan Windows Server 2008R2, lalu tekan tab *next* untuk melanjutkan proses wizard selanjutnya.



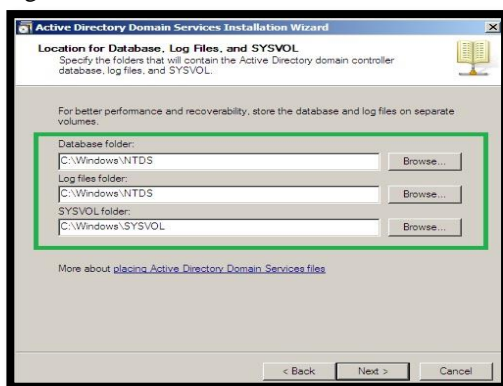
Gambar 10. Domain NetBIOS Name

Menu *Set Forest Functional Level* akan tampil, ada beberapa opsi windows yang dapat berjalan atau kompatibel dengan Windows Server yang digunakan, 'press' next tab dan pilih *Windows Server 2008R2*.



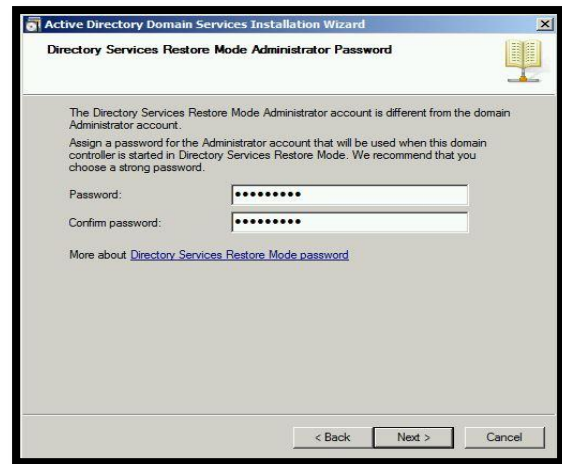
Gambar 11. Forest Functional level

Tentukan lokasi untuk penyimpanan file DB (Database), Logfiles, dan SYSVOL. Tekan tombol *Browse* dan cari folder yang akan digunakan, akhiri dengan klik tab *next*.



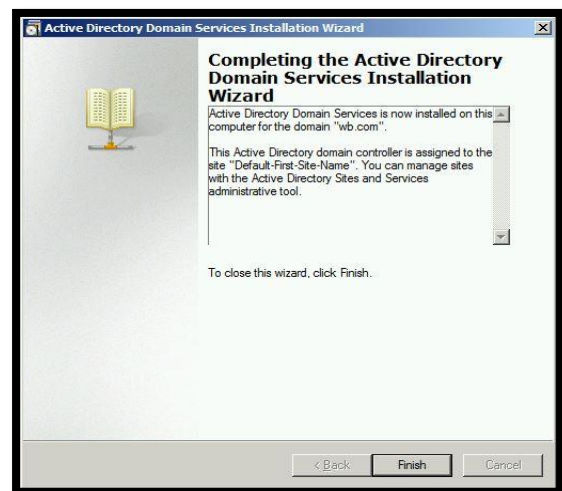
Gambar 12. Lokasi Penyimpanan Database, Log File & Sysvol

Create password untuk *Directory Services Restore Mode Administrator Password*, boleh berbeda dengan Administrator yang sebelumnya, lalu klik tombol *next*.



Gambar 13. Restore Mode Administrator

Setelah beberapa saat akan muncul notifikasi bahwa AD sudah terinstall, klik tab *finish* untuk mengakhirinya.



Gambar 14. Complete Installasion



Gambar 15. Restart Active Directory



Gambar 16. Login Administrator

Masukan domain dan user administrator, serta password pada tampilan awal setelah komputer restart.

3. KESIMPULAN

- a) AD sangat diperlukan dalam infrastruktur untuk menyimpan semua konfigurasi, baik itu user, group, aplikasi, policy dan masih banyak yang lainnya secara terpusat.
- b) Keamanan Sistem Informasi dapat terjaga dan terpantau, dari penyalahgunaan dari user yang tidak bertanggung jawab.
- c) AD membantu dan memudahkan dalam mengelola Organizational Unit (OU) dalam organisasi atau perusahaan .
- d) Administrator mudah untuk menambahkan atau mengurangi server, tanpa mengganggu user karena user hanya mengakses satu nama.

DAFTAR PUSTAKA

- [1] <http://sfarizy10.blogspot.co.id/2011/11/kenali-lebih-deket-lagi-ama-nyang.html>
- [2] <http://sfarizy10.blogspot.co.id/2012/08/iseng2-sambil-nunggu-ngabuburit-kite.html>
- [3] Allen, R., L.E. Hunter., and B.J. Dinerman., Windows Server 2003 Networking Recipe, Apress, New York, 2006.
- [4] Allen, R., Active Directory Cookbook for Windows Server 2003 & Windows 2000, O'Reilly Media, California, 2002.