VOLUME 6 NOMOR 1, APRIL 2017

ISSN 2089 - 1245

KILAT

JURNAL KAJIAN ILMU DAN TEKNOLOGI

ISSN 2089-1245

SEKOLAH TINGGI TEKNIK - PLN (STT-PLN)

KILAT	VOL.6	NO.1	HAL. 1 - 80	APRIL 2017	ISSN 2089 - 1245

IMPLEMENTASI PEMBATASAN AKSES PEMAKAI KOMPUTER MENGGUNAKAN GROUP POLICY OBJECT DI WINDOWS SERVER 2012 R2

Marliana Sari[1)]
1), Jurusan Teknik Komputer dan Manajemen Informatika Politeknik Negeri Medan
JL.Almamater No.1 Kampus USU, Medan 20155
Email :marliana.sari77@gmail.com[1)]

ABSTRACT

Network Security is a very important thing nowadays. Therefore organizations need to implement network security policies in their respective environments. One way to implement a network security policy is to limit user access by using the existing Active Directory GroupPolicy Object in Windows Server 2012 R2. By using Group Policy Object (GPO) in Windows Server 2012 R2, the administrator can apply the policy to the user or to the computer on the network.

Keywords: *Active Directory, Group Policy Object, GPO, Network Security*

ABSTRAK

Keamanan Jaringan adalah hal yang sangat penting saat ini.Oleh karena itu organisasi perlu untuk menerapkan kebijakan keamanan jaringan di lingkungan masing-masing. Salah satu cara untuk menerapkan kebijakan keamanan jaringan adalah membatasi akses user dengan menggunakan GroupPolicy Object yang ada Active Directory di Windows Server 2012 R2. Dengan menggunakan Group Policy Object (GPO) di Windows Server 2012 R2, maka administrator bisa menerapkan policy kepada user maupun kepada komputer yang ada di jaringan.

Kata kunci: *Active Directory,Group Policy Object, GPO, Keamanan Jaringan*

1. PENDAHULUAN

Penggunaan komputer di jaringan perlu diatur agar sesuai dengan tujuan perusahaan. Oleh karena itu maka kita perlu menerapkan kebijakan keamanan jaringan disini. Untuk mengelola sepuluh atau dua puluh komputer mungkin bukan masalah. Tapi bagaimana halnya jika Anda harus mengelola ratusan atau ribuan komputer atau user yang menggunakan komputer tersebut. Bayangkan betapa repotnya jika harus melakukan hal tersebut satu persatu. Untuk menginstall satu software saja Anda harus berkeliling dari satu komputer ke komputer lain. Untunglah hal itu sekarang bukan menjadi masalah lagi. Active Directory memiliki Group Policy yang akan membantu Anda untuk mengelola komputer maupun user di jaringan.

Di dalam paper ini Penulis akan memaparkan implementasi keamanan jaringan menggunakan Group Policy Object.Active Directory bertindak sebagai otoritas terpusat terhadap keamanan jaringan, melakukan verifikasi terhadap akses user, dan yang paling penting yaitu sebagai titik integrasi untuk membuat sistem bisa bekerja secara sinergis dalam mengkonsolidasi tugas-tugas manajemen.

Di jaringan ada banyak sumber daya yang perlu dikelola dengan baik. Ada file server, printer, intranet, scanner, dan berbagai perangkat lainnya yang digunakan oleh user di jaringan. Semua sumber daya tersebut bisa diatur oleh Active Directory, siapa-siapa saja yang boleh menggunakannya dan kapan sumber daya tersebut boleh digunakan. Tidak hanya itu, siapa saja yang mengelola sumber daya tersebut juga bisa diatur. Misalnya siapa saja yang boleh mereset password seorang user juga bisa diberikan hak untuk melakukan hal tersebut. Ini membuat Active Directory bisa diandalkan untuk membantu pekerjaan Administrator[3]

Active Directory memiliki sisi logical dan sisi fisik yang dilihat. Pada sisi logical akan ditemui istilah-istilah objek, domain tree dan forest. Sedangkan pada sisi fisik akan ditemui istilah-istilah domain controller, site serta subnet. Dari sudut pandang logis, Active Directory merupakan sistem yang menyimpan sesuatu yang bisa digunakan untuk mewakili suatu hal di jaringan. Suatu hal tersebut misalnya user atau pemakai jaringan, suatu file dan folder sharing, printer, komputer atau suatu hirarki organizational unit[2].

2. LANDASAN TEORI

2.1 Windows Server 2008

Windows Server 2008 merupakan sistem operasi server terbaru dari Microsoft. Sebagai penerus dari Windows Server 2003, Windows Server 2008 membawa banyak fasilitas baru yang belum ada di Windows Server 2003. Beberapa fasilitas yang baru yang ada di Windows Server 2008 antara lain Server Manager, Windows PowerShell, Windows Depolyment Services (WDS), Internet Information Services (IIS) 7.0 serta Read Only Domain Controller (RODC).

Penulis melihat langsung perbedaan antara Windows Server 2003 dengan Windows Server 2008 saat melakukan instalasi Windows Server 2008. Saat instalasi Windows Server 2008 akan muncul sedikit sekali pertanyaan yang berhubungan dengan konfigurasi komputer, misalnya menentukan nama server dan konfigurasi lainnya. Konfigurasi justru dilakukan setelah instalasi sistem operasi Windows Server 2008 selesai. Hal ini membuat instalasi Windows Server 2008 lebih cepat dilakukan.

Server Manager merupakan fasilitas yang baru yang ada di Windows Server 2008. Adanya Server Manager akan memudahkan Administrator untuk mengkonfigurasi Windows Server 2008.

2.2 Active Directory

Active Directory (DNS) adalah sistem penamaan yang dianut di internet. Jika kita bertanya tentang suatu alamat web site atau mengirim e-mail, maka DNS Server yang akan menjawab ke mana harus menuju.

Di jaringan memiliki banyak sumber daya yang perlu dikelola dengan baik. Ada file server, printer, intranet, scanner, dan berbagai perangkat lainnya yang digunakan oleh user di jaringan. Semua sumber daya tersebut bisa diatur oleh Active Directory, siapa-siapa saja yang boleh menggunakannya dan kapan sumber daya tersebut boleh digunakan. Tidak hanya itu, siapa saja yang mengelola sumber daya tersebut juga bisa diatur. Misalnya siapa saja yang boleh mereset password seorang user juga bisa diberikan hak untuk melakukan hal tersebut. Ini membuat Active Directory bisa diandalkan untuk membantu pekerjaan sebagai seorang Administrator. Selain itu hal yang berkenaan dengan optimalisasi lalu lintas jaringan juga bisa diatur oleh Active Directory.

2.3 Group Policy Object

Group Policy merupakan kumpulan berbagai setting yang mengatur perilaku komputer atau user di jaringan yang tergabung dengan Active Directory. Berbagai setting yang bisa diatur oleh Group Policy ini antara lain adalah Windows Settings, Software Settings dan Administrative Template. Penulis menggunakan Software setting untuk melakukan instalasi software yang di tujukan kepada user atau komputer. Dengan menggunakan software setting maka instalasi software cukup dilakukan secara terpusat, cukup sekali saja membuat suatu paket dan paket itu akan di berikan kepada user atau komputer yang tergabung dalam Active Directory. Proses instalasi akan berjalan secara otomatis tanpa disadari oleh user yang bersangkutan. Selanjutnya software tersebut bisa langsung dipakai.

Berbagai setting yang berkaitan dengan keamanan atau security bisa di atur menggunakan Windows Settings. Selain itu Windows Setting juga bisa mengatur script yang dijalankan saat startUp atau Shutdown. Settings security yang bisa di atur antara lain adalah Account Policies, Local Policies, Event Log, Systems Services, IP Security Policies dan sebagainya.

2.4 Keamanan Jaringan

Keamanan jaringan adalah suatu cara atau suatu system yang digunakan untuk memberikan proteksi atau perlindungan pada suatu jaringan agar terhindar dari berbagai ancaman luar yang mampu merusak jaringan.

1. Elemen pembentukan keaman jaringan

Ada dua elemen utama pembentuk keamanan jaringan :

a. Tembok pengamanan (baik secara fisik maupun maya), yaitu suatu cara untuk memberikan proteksi atau perlindugan pada jarigan, baik secara fisik (kenyataan) maupun maya (menggunakan software)
b. Rencana pengamanan, yaitu suatu rancagan yang nantinya akan di implementasiakan uantuk melindugi jaringan agar terhindar dari berbagai ancaman dalam jaringan.

2. Alasan keaman jaringan sangat penting

Alasan keaman jaringan sangat penting karena:

1. Privacy / Confidentiality
   a. Defenisi : menjaga informasi dari orang yang tidak berhak mengakses.
   b. Privacy : lebih kearah data-data yang sifatnya privat , Contoh : e-mail seorang pemakai (user) tidak boleh dibaca oleh administrator.
   c. Confidentiality : berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk keperluan tertentu tersebut.
   d. Contoh : data-data yang sifatnya pribadi (seperti nama, tempat tanggal lahir, social security number, agama, status perkawinan, penyakit yang pernah diderita, nomor kartu kredit, dan sebagainya) harus dapat diproteksi dalam penggunaan dan penyebarannya.
   e. Bentuk Serangan : usaha penyadapan (dengan program sniffer).
   f. Usaha-usaha yang dapat dilakukan untuk meningkatkan privacy dan confidentiality adalah dengan menggunakan teknologi kriptografi.

2. Integrity
   a. Defenisi : informasi tidak boleh diubah tanpa seijin pemilik informasi.
   b. Contoh : e-mail di intercept di tengah jalan, diubah isinya, kemudian diteruskan ke alamat yang dituju.
   c. Bentuk serangan : Adanya virus, trojan horse, atau pemakai lain yang mengubah informasi tanpa ijin, “man in the middle attack” dimana seseorang menempatkan diri di tengah pembicaraan dan menyamar sebagai orang lain

.

3. Authentication
   a. Defenisi : metoda untuk menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud.

   b. Dukungan :
      · Adanya Tools membuktikan keaslian dokumen, dapat dilakukan dengan

teknologi watermarking(untuk menjaga “intellectual property”, yaitu dengan menandai dokumen atau hasil karya dengan “tanda tangan” pembuat) dan digital signature.

- Access control, yaitu berkaitan dengan pembatasan orang yang dapat mengakses informasi. User harus menggunakan password, biometric (ciri-ciri khas orang), dan sejenisnya.

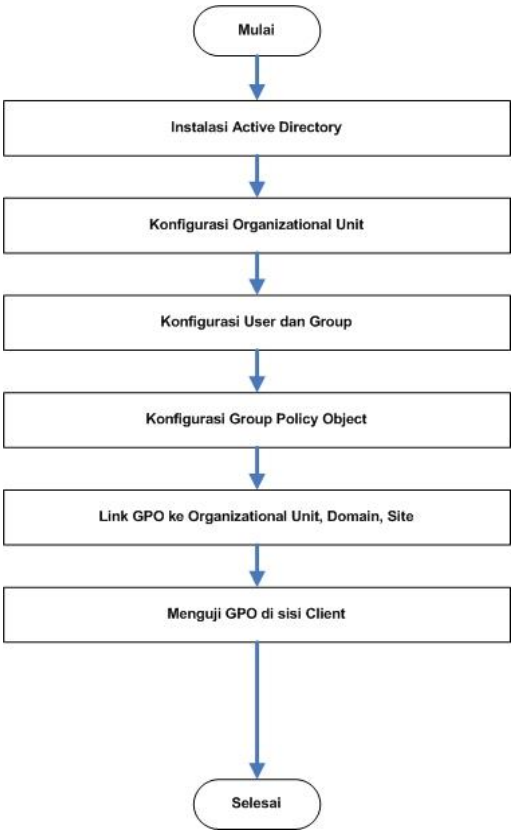
4. Availability
   a. Defenisi : berhubungan dengan ketersediaan informasi ketika dibutuhkan.
   b. Contoh hambatan :
      - “denial of service attack” (DoS attack), dimana server dikirimi permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai down, hang, crash.
      - mailbomb, dimana seorang pemakai dikirimi e-mail bertubi-tubi (katakan ribuan e-mail) dengan ukuran yang besar sehingga sang pemakai tidak dapat membuka e-mailnya atau kesulitan mengakses e-mailnya.

5. Access Control
   a. Defenisi : cara pengaturan akses kepada informasi. berhubungan dengan masalah
   b. authentication dan juga privacy
   c. Metode : menggunakan kombinasi userid/password atau dengan menggunakan mekanisme lain.
6. Non-repudiation
   a. Defenisi : Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Dukungan bagi electronic commerce.

3. Syarat keaman jaringan
   a. Prevention (pencegahan).
      Kebanyakan dari ancaman akan dapat ditepis dengan mudah, walaupun keadaan yang benarbenar 100% aman belum tentu dapat dicapai. Akses yang tidak diinginkan kedalam jaringan komputer dapat dicegah dengan memilih dan melakukan konfigurasi layanan (services) yang berjalan dengan hati-hati.
   b. Observation (observasi).
      Ketika sebuah jaringan komputer sedang berjalan, dan sebuah akses yang tidak diinginkandicegah, maka proses perawatan dilakukan. Perawatan jaringan komputer harus termasuk melihat isi log yang tidak normal yang dapat merujuk ke masalah keamanan yang tidak terpantau. System IDS dapat digunakan sebagai bagian dari proses observasi tetapi menggunakan IDS seharusnya tidak merujuk kepada ketidak-pedulian pada informasi log yang disediakan.
   c. Response (respon).

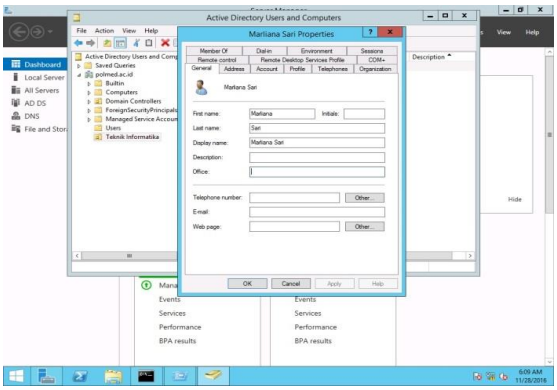
Bila sesuatu yang tidak diinginkan terjadi dan keamanan suatu system telah berhasil disusupi,maka personil perawatan harus segera mengambil tindakan. Tergantung pada proses produktifitas dan masalah yang menyangkut dengan keamanan maka tindakan yang tepat harus segera dilaksanakan. Bila sebuah proses sangat vital pengaruhnya kepada fungsi system dan apabila di-shutdown akan menyebabkan lebih banyak kerugian daripada membiarkan system yang telah berhasil disusupi tetap dibiarkan berjalan, maka harus dipertimbangkan untuk direncakan perawatan pada saat yang tepat . Ini merupakan masalah yang sulit dikarenakan tidak seorangpun akan segera tahu apa yang menjadi celah begitu system telah berhasil disusupi dari luar.

3. METODOLOGI PENELITIAN



Gambar 1. Alur Diagram Penelitian

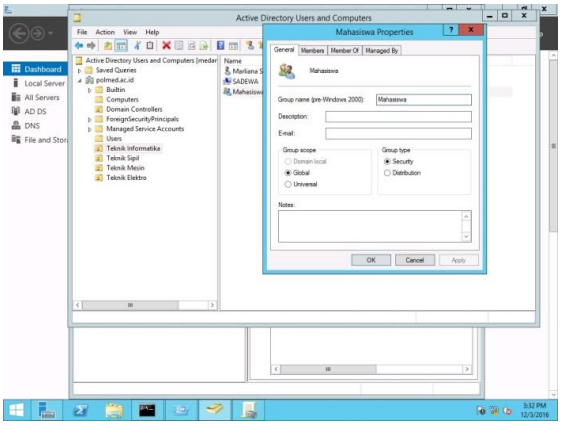
4. HASIL DAN ANALISA



Gambar 2. Objek User di Active Directory

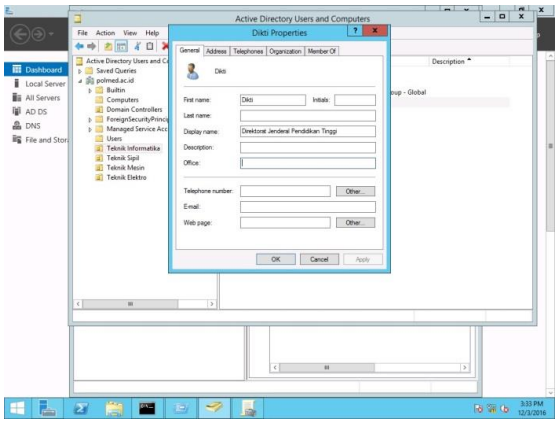
Active Directory Domain Services menyediakan database terdistribusi yang menyimpan dan mengelola informasi tentang sumber daya jaringan dan data yang spesifik dari aplikasi tertentu. Server yang menjalankan ADDS disebut domain controller. Administrator dapat menggunakan ADDS untuk mengatur elemen-elemen jaringan seperti user, komputer dan perangkat lainnya ke dalam struktur yang memiliki hirarki. Struktur hirarki yang dimaksud berisi Active Directory forest, dan Organizational unit (OU) di dalam domain. Objek merupakan hal yang paling mendasar dari Active Directory. Objek ini biasanya dibuat berdasarkan kelas tertentu. Setiap objek akan memiliki kumpulan atribut tertentu. Contoh objek di Active Directory antara lain adalah user, group, computer, contact, printer dan lain sebagainya[1].

Objek User merupakan objek yang mewakili user yang terdapat pada jaringan Active Directory. Setiap user mewakili sebuah nama yang digunakan untuk login ke jaringan, khususnya pada Active Directory. Pada saat user tersebut login, user tersebut harus memasukkan nama user dan password. Setelah berhasil diotentikasi oleh Active Directory maka user tersebut bisa bekerja di jaringan. User yang bersangkutan bisa mengakses file dan folder yang ada di server atau komputer lain, bisa menggunakan printer untuk mencetak serta bisa menggunakan e-mail dan Internet sesuai dengan hak yang sudah diberikan.



Gambar 3. Objek Group

Objek group merupakan objek yang mewakili kumpulan user yang ada di Active Directory. User-user yang memiliki hak akses yang sama terhadap suatu file atau folder dikelompokkan pada group sama. Dengan cara seperti itu maka pengelolaan sumber daya jaringan akan menjadi lebih mudah. Cukup memberikan ijin akses pada group, maka semua anggota group tersebut akan mendapat hak akses yang sama. Misalkan ada user lain yang ingin mendapatkan hak akses terhadap file atau folder yang sama, maka cukup masukkan user tersebut ke group yang sama. Atau jika ada user yang sudah tidak boleh mengakses file atau folder tersebut, maka user tersebut dikeluarkan dari keanggotaan group tersebut.

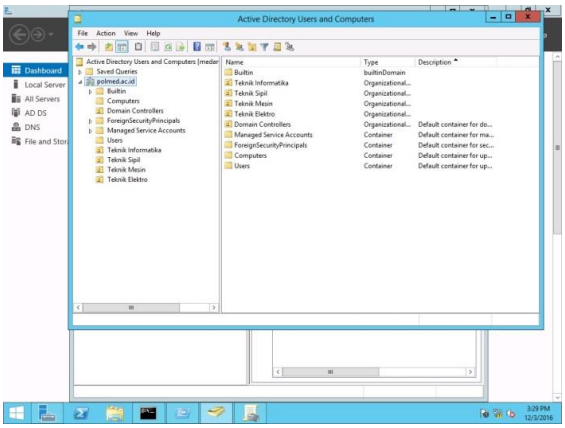


Gambar 4. Objek Contact

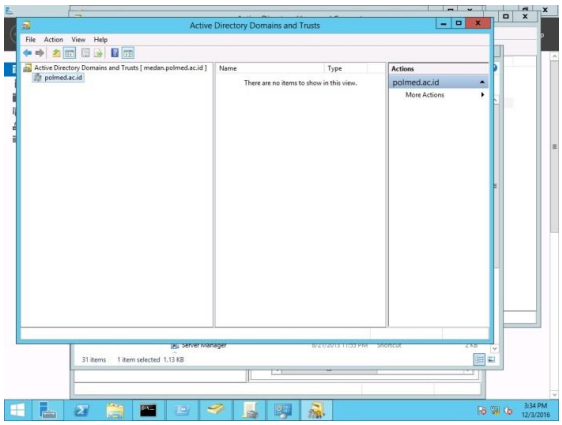
Komputer merupakan objek yang terdaftar pada Active Directory mewakili komputer yang digunakan oleh user. Selain sebagai workstation, komputer yang terdaftar pada Active Directory ada juga yang berfungsi sebagai server. Server yang dimaksud di sini adalah member server atau server yang bukan sebagai domain controller. Komputer tersebut terdaftar pada Active Directory setelah komputer tersebut bergabung dengan domain atau lebih dikenal dengan istilah join domain. Setiap komputer yang tergabung pada Active Directory memiliki atribut sistem operasi yang diinstall, apakah Windows 7 Professional atau Windows Server 2012 atau Windows 2000.

Active Directory memungkinkan suatu objek yang tidak boleh login ke jaringan tapi tetap terdaftar sebagai objek yang mudah ditemukan pada Active Directory. Objek ini dikenal dengan istilah contact. Dengan adanya contact, maka objek tersebut bisa dikirimkan e-mail dan sebagainya.

Printer merupakan objek yang terdaftar pada Active Directory untuk mewakili objek print device yang ada secara fisik. Printer tersebut disharing dan bisa digunakan untuk mencetak oleh semua user Active Directory yang sudah diberikan ijin akses, baik melalui group atau langsung user yang bersangkutan.



Gambar 5. Organizational Unit



Gambar 6. Domain

Organizational Unit adalah container pada Active Directory yang digunakan untuk mengelola object di Active Directory. OU merupakan suatu container, artinya di dalam OU kita bisa membuat atau meletakkan objek-objek yang terdapat pada domain, misalnya user, group, computer, contact, printer dan sebagainya. Di dalam perguruan tinggi struktur OU bisa diimplementasikan menggunakan struktur fakultas, seperti yang terlihat pada gambar 4 di atas.

Pada Gambar 4 di atas terdapat OU Teknik Informatika, Teknik Mesin, Teknik Elektro, Teknik Sipil dan lainnya. Semua struktur OU tersebut mewakili struktur organisasi perguruan tinggi. Di dalam suatu OU bisa terdapat OU, artinya struktur OU tidak dibatasi. Tetapi perlu diperhatikan agar jangan terlalu dalam struktur yang dibuat karena bisa membingungkan dan juga menurunkan unjuk kerja sistem.

Adanya Organizational Unit (OU) memudahkan pengelolaan dari Active Directory. Dengan cara ini maka pengelolaan Active Directory bisa didelegasikan kepada satu orang atau lebih. Selain itu pengelolaan juga bisa diberikan kepada sebuah group. Tugas pengelolaan Active Directory pada Organizational Unit ini bisa merupakan suatu tugas spesific misalkan melakukan penambahan user, mereset password, mengunci user atau membuka user yang terkunci.

Domain merupakan batas security dan administrasi directory service pada Windows Server 2012. Sistem penamaan yang digunakan pada Active Directory adalah Domain Name System atau DNS. Contoh nama domain Active Directory yang menggunakan sistem DNS adalah polmed.ac.id. Di dalam domain terdapat objek dan organizational unit. Selain itu juga domain merupakan batas implementasi policy misalnya group policy. Replikasi objek dari satu server domain controller ke domain controller lain juga dibatasi oleh domain.

Setiap domain paling tidak harus memiliki satu buah server domain controller. Selain berfungsi sebagai domain controller, server domain ini juga berfungsi sebagai domain name systems (DNS) server. Untuk menjaga keberadaan domain Active Directory sebaiknya setiap domain memiliki minimal dua buah domain controller. Tujuannya agar jika satu domain controller mengalami masalah maka jaringan tetap bisa berjalan, karena peran server telah diambil alih oleh domain controller yang lain. Setiap domain akan memiliki administrator masing-masing sehingga semua aktifitas pada domain yang bersangkutan diatur oleh administrator tersebut.

Domain di dalam Active Directory memiliki struktur hirarki atau berjenjang. Ada yang disebut parent domain dan child domain. Contoh parent domain misalnya polmed.ac.id sedangkan contoh child domain misalnya teknik.polmed.ac.id hirarki parent dan child domain ini dikenal dengan istilah domain tree yang bersifat contigous namespace. Domain tree pada Active Directory ini dibentuk oleh konsep yang namanya trust. Trust adalah hubungan antara satu domain dengan domain lain dimana satu domain bisa mengakses sumber daya yang ada di domain lain. Berdasarkan arahnya trust bisa dibedakan menjadi dua, yaitu trust satu arah atau one way trust dan trust dua arah atau two way trust.

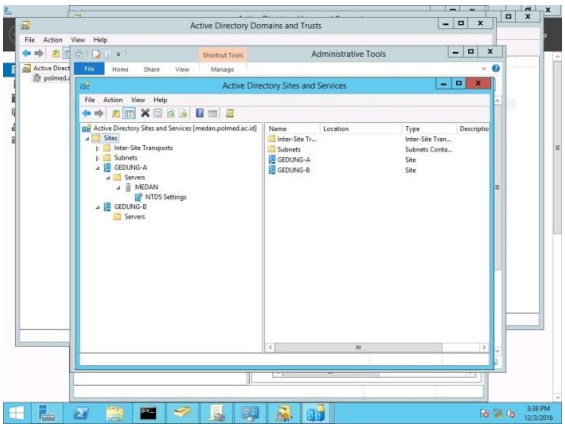
Trust satu arah adalah hanya salah satu domain bisa mengakses domain yang lain. Misalkan domain A dan domain B. Trust satu arah ini contohnya hanya user domain A yang bisa mengakses file atau folder yang ada di domain B, sedangkan user domain B tidak bisa mengakses file atau folder yang ada di domain A. Dalam hal ini domain A disebut dengan Trusted Domain, sedangkan domain B disebut Trusting Domain. Trust dua arah atau two way trust memungkinkan domain A mengakses domain B dan sebaliknya juga demikian.

Selain itu ada jenis trust lain yaitu transitive dan intransitive trust. Misalkan domain A trust domain B dan domain B trust domain C maka domain A trust domain C. Sistem seperti ini dengan trust yang transitive. Sedangkan jika bukan bersifat demikian maka ini disebut dengan intransitive trust. Selain itu ada jenis trust yang lain yaitu external trust, shortcut trust dan forest trust.

Forest merupakan kumpulan domain dari satu atau beberapa buah domain tree yang memiliki skema yang sama. Kumpulan tree tersebut tidak

harus memiliki nama domain yang seragam, misalkan satu domain tree memiliki nama mataram.com sedangkan yang lain download.net. Forest merupakan level tertinggi yang ada di dalam struktur logika Active Directory. Domain yang pertama kali dibuat di forest disebut dengan forest root domain.

Domain Controller adalah server yang diinstall Windows Server 2012 dan diinstall Active Directory. Server ini bisa dilihat secara fisik berupa hardware. Setiap domain controller akan menjalankan fungsi penyimpan serta replikasi. Satu server domain controller hanya bisa menjalankan fungsi untuk satu domain. Agar fungsi kelangsungan hidup domain selalu terjaga maka paling tidak Anda harus memiliki beberapa domain controller, agar jika satu domain controller mengalami masalah maka domain controller yang lain bisa menggantikan. Domain controller yang ada di Active Directory memiliki satu atau beberapa peran antara lain Flexible Single Master Operation (FSMO), Global Catalog dan DNS Server.



Gambar 7. Site

Site mewakili kumpulan domain controller yang berada di dalam satu lokasi. Umumnya lokasi ini merupakan jaringan yang memiliki kecepatan tinggi seperti Local Area Network (LAN). Local Area Network ini paling tidak memiliki kecepatan 100 Mbps atau Fast Ethernet. Ada juga LAN yang memiliki kecepatan 1 Gbps atau yang dikenal dengan Gigabit Ethernet. Tidak tertutup juga kemungkinan site adalah lokasi lain yang dipisahkan oleh Wide Area Network (WAN) yang berkecepatan tinggi misalnya menggunakan fiber optic atau gelombang radio. Pada saat pertama kali diinstall, Active Directory akan membuat site yang bernama Default First Site Name Site. Server domain controller yang diinstall akan diletakkan di Default First Site Name Site ini.

Subnet merupakan sub jaringan di dalam konsep TCP/IP. Komputer yang berada di dalam satu subnet dapat berkomunikasi satu sama lain secara langsung tanpa melalui router. Masing-masing subnet bisa dibedakan berdasarkan subnet mask yang digunakan. Nantinya subnet ini akan diasosiasikan dengan site. Satu site bisa terdiri dari satu subnet, atau beberapa subnet diasosiasikan dengan satu site.

Operation master adalah suatu peran tertentu dalam suatu forest atau domain yang dimiliki oleh sebuah domain controller. Peran ini ada yang berada di level domain dan ada yang di level forest. Untuk level forest hanya ada satu domain controller yang memegang peran tersebut di semua domain yang ada di forest tersebut. Operation master yang berada di level domain akan dipegang oleh salah satu domain controller yang ada di domain tersebut dan ada di semua domain pada forest tersebut.Ada dua operation master yang berada di level forest, yaitu Schema Master dan Domain Naming Master. Sedangkan Operation Master yang ada di level domain ada tiga yaitu:PDC emulator, RID Master dan Infrastructure Master.

Pada saat instalasi Active Directory di server domain controller yang pertama kali di forest root domain, semua peran tersebut akan dipegang oleh satu domain controller saja. Setelah Anda selesai menginstall domain controller tambahan maka peran tersebut bisa dipindahkan ke domain controller yang baru. Jika Anda membuat domain tree baru di dalam forest atau menginstall child domain, maka domain controller tersebut akan mengambil tiga peran yang ada di level domain. Masing-masing peran memiliki tugas tertentu, dimana jika peran tersebut tidak ada maka suatu pekerjaan tidak dapat dilakukan. Misalnya jika domain naming master tidak ada kita tidak bisa menambahkan domain baru.

Schema Master merupakan peran yang dipegang oleh salah satu domain controller yang ada di forest. Domain controller yang memegang peran schema master akan sangat berperan terhadap penambahan atau penonaktifan skema yang ada di Active Directory. Skema itu sendiri terdiri dari dua bagian yaitu kelas dan atribut. Kelas merupakan pengelompokan jenis objek yang ada di Active Directory. Contoh kelas misalnya users, computers dan printers. Sedangkan atribut adalah keterangan atau informasi yang terdapat pada objek yang bersangkutan. Contohnya adalah user memiliki atribut nama depan, nama belakang, nama login dan sebagainya. Jika ada perubahan pada schema maka kita harus merubahnya di schema master. Misalnya kita mau melakukan instalasi Exchange Server, dimana harus menambahkan atribut baru yaitu e-mail address, perubahan tersebut dilakukan di schema master Active Directory.

Seperti Schema Master, Domain Naming Master merupakan peran yang dipegang oleh salah satu domain controller yang ada di forest. Domain controller yang memegang peran domain naming master akan sangat berperan terhadap penambahan penghapusan suatu domain yang terdapat di forest Active Directory. Untuk menambahkan suatu tree baru di forest Active Directory, proses dcpromo pada waktu instalasi Active Directory di suatu server domain controller yang baru harus berhasil menghubungi domain naming master. Demikian juga halnya jika kita ingin menambahkan suatu child domain di bawah domain tree yang sudah ada, maka kita juga harus berhasil menghubungi domain naming master yang ada di forest.

PDC Emulator merupakan peran yang dipegang oleh salah satu domain controller yang ada di domain. Setiap domain yang ada di forest pasti memiliki domain controller yang berperan sebagai

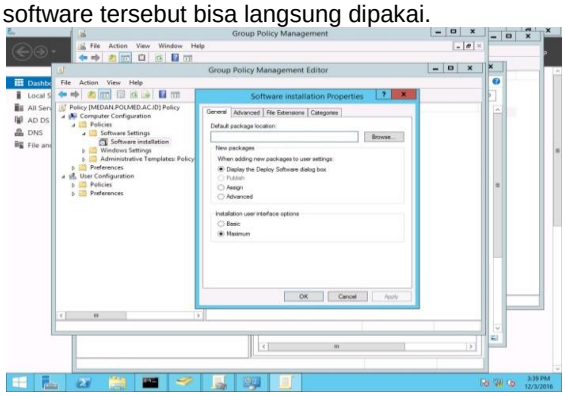
PDC Emulator. PDC Emulator ini akan berperan sebagai server PDC jika di jaringan Anda masih terdapat Windows NT 4.0 sebagai Backup Domain Controller. Selain itu juga berfungsi untuk penggantian password bagi Windows Client versi lama misalnya Windows 98 atau Windows ME. Fungsi lain PDC Emulator adalah sinkronisasi jam antar komputer di jaringan.

RID Master merupakan peran yang dipegang oleh salah satu domain controller yang ada di domain. Setiap domain yang ada di forest pasti memiliki domain controller yang berperan sebagai RID Master. Server domain controller dengan peran RID Master akan bertugas membagikan nomor unik kepada setiap objek yang dibuat di domain Active Directory. Nomor ini dikenal sebagai Security Identifier (SID).

Infrastructure Master merupakan peran yang dipegang oleh salah satu domain controller yang ada di domain. Setiap domain yang ada di forest pasti memiliki domain controller yang berperan sebagai Infrastructure Master. Server domain controller dengan peran Infrastructure Master akan mengatur keanggotaan group dari suatu user. Dengan adanya hubungan trust pada Active Directory, maka user atau group di suatu domain bisa menjadi anggota group di domain yang lain. Pointer keanggotaan inilah yang dijaga oleh Infrastructure Master.

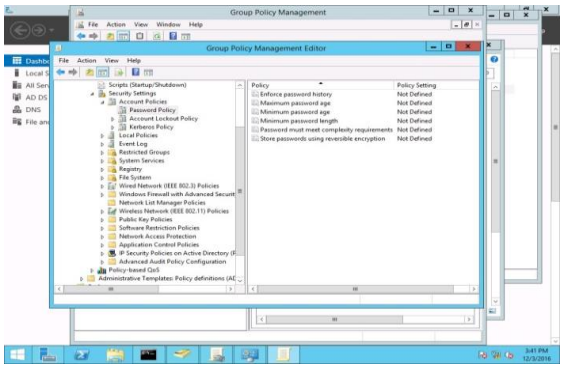
Global Catalog Server merupakan peran yang dipegang oleh salah satu atau beberapa server domain controller yang ada di domain. Setiap domain yang ada di forest pasti memiliki paling tidak satu domain controller yang berperan sebagai Global Catalog Server. Server domain controller dengan peran Global Catalog Server akan bertugas melakukan otentikasi terhadap nama user dan password yang diisi oleh user pada saat melakukan login ke jaringan.

Group Policy [4] merupakan kumpulan berbagai setting yang mengatur perilaku komputer atau user di jaringan yang tergabung dengan Active Directory. Berbagai setting yang bisa diatur oleh Group Policy ini antara lain adalah Windows Settings, Software Settings dan Administrative Template. Kita bisa menggunakan Software setting untuk melakukan instalasi software yang kita tujukan kepada user atau komputer. Dengan menggunakan software setting maka instalasi software cukup kita lakukan secara terpusat, cukup sekali saja membuat suatu paket dan paket itu akan kita berikan kepada user atau komputer yang tergabung dalam Active Directory. Proses instalasi akan berjalan secara otomatis tanpa disadari oleh user yang bersangkutan. Selanjutnya software tersebut bisa langsung dipakai.



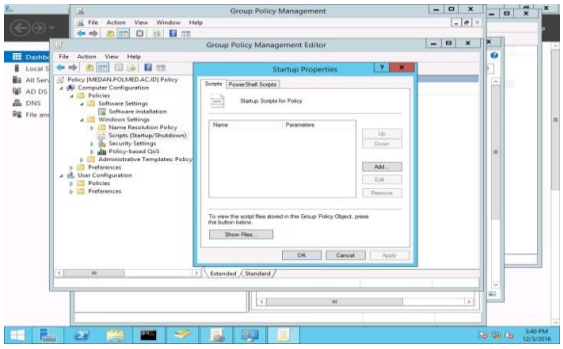
Gambar 8. GPO Software Installation

Berbagai setting yang berkaitan dengan keamanan atau security bisa kita atur menggunakan Windows Settings. Selain itu Windows Setting juga bisa mengatur script yang dijalankan saat startUp atau Shutdown. Settings security yang bisa kita atur antara lain adalah Account Policies, Local Policies, Event Log, Systems Services, IP Security Policies dan sebagainya.



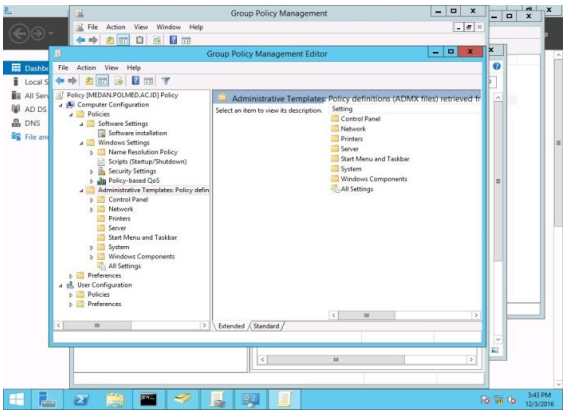
Gambar 9. GPO Security Settings

Administrative Template berisi berbagai setting yang mengatur perilaku sistem operasi antara lain Windows Component, Start Menu and Task Bar, Desktop, Control Panel, Shared Folders, Network, Printer, dan System. Menggunakan Administrative Template untuk mengkonfigurasikan Wallpaper yang sama bagi semua user di jaringan sangatlah mudah. Demikian juga jika ingin menghilangkan menu Run yang ada di tombol Start, juga bisa dengan mudah untuk dilakukan.



Gambar 10. GPO Scripts

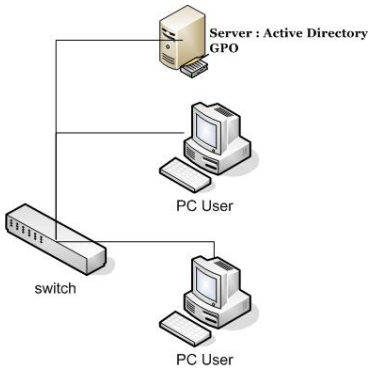
Group Policy Object juga bisa mengatur script yang akan dijalankan pada saat komputer startup atau pada saat seorang user login ke jaringan. Script yang dijalankan bisa berupa script biasa ataupun Windows Powershell scripts.



Gambar 11. GPO Administrative Templates

Walaupun namanya Group Policy, bukan berarti bahwa hal ini ditujukan untuk group yang ada di Active Directory, entah itu Security Group atau Distribution Group. Setting yang ada di Group Policy bisa diterapkan ke suatu domain, site, atau organizational unit (OU) bukan ke group.

Gambar 12 di bawah ini adalah skema jaringan yang akan diimplementasikan menggunakan Group Policy Object.

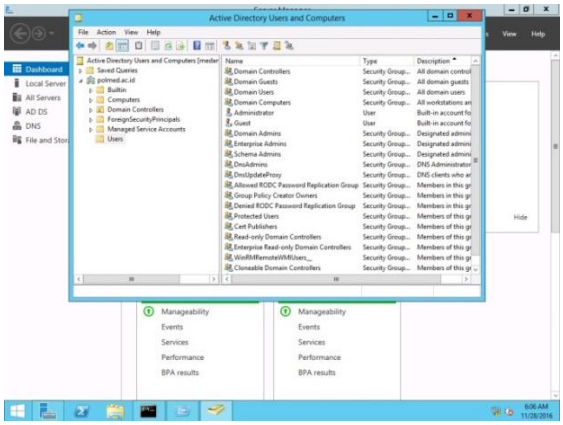


Gambar 12. Skema Group Policy Object

Pada gambar di atas kita mengimplementasikan Group Policy Object menggunakan satu buah server. Server pertama adalah server yang berfungsi sebagai server Active Directory dan file server root atau file server yang paling atas. Pada Active Directory kita akan membuat sebuah domain polmed.ac.id. Pada Domain ini tersimpan seluruh nama user dan group yang akan mengakses jaringan.

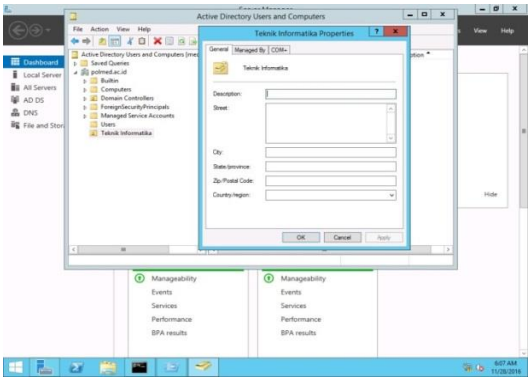
Gambar 11 di atas menampilkan alur diagram untuk mengimplementasikan Group Policy Object di Windows Server 2012 R2. Ada beberapa langkah yang digambarkan dalam diagram alir tersebut. Langkah pertama adalah melakukan instalasi Active Directory pada Windows Server 2012 R2. Untuk menginstall Active Directory kita harus mengkonfigurasikan TCP/IP Address beserta parameternya seperti IP Address, Subnet Mask dan Default Gateway. Selanjutnya kita harus mengkonfigurasikan DNS Suffix untuk domain DNS nya, misalnya polmed.ac.id. Setelah Active Directory terpasang langkah selanjutnya adalah membuat Organizational Unit yang akan digunakan sebagai Container untuk tempat user dan group yang dibuat di Active Directory. Setelah OU terbentuk, langkah selanjutnya adalah membuat user yang akan digunakan untuk login di PC. Setelah itu kita akan membuat Group Policy Object (GPO) di server Active Directory. Langkah selanjutnya adalah kita akan menghubungkan atau link GPO tersebut dengan Organizational yang tadi telah dibuat. Setelah itu langkah terakhir adalah menguji GPO tadi di sisi komputer Client. Setelah user tersebut login, cobalah untuk menampilkan tombol Run yang ada di menu Start.

Langkah pertama dalam implementasi GPO ini adalah melakukan instalasi Active Directory. Hasil instalasi Active Directory ditunjukkan pada gambar 13 di bawah ini.



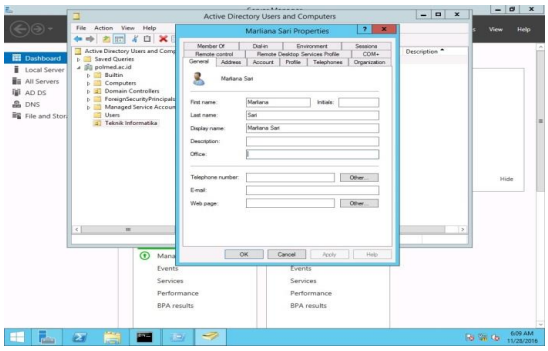
Gambar 13. Active Directory

Langkah kedua adalah membuat Organizational Unit. Hasil pembuatan Organizational Unit ini dapat dilihat pada gambar 4 di bawah ini:



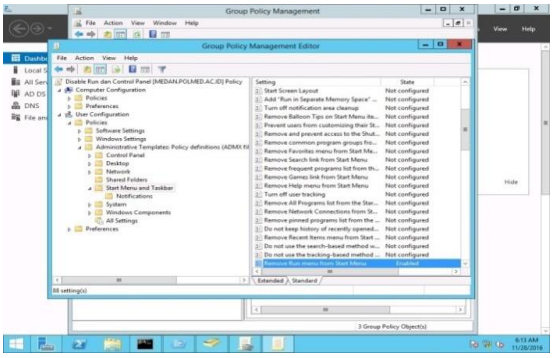
Gambar 14. Organizational Unit

Langkah ketiga adalah mengkonfigurasikan user yang akan digunakan sebagai pemakai untuk login di jaringan. Hasil konfigurasi user tersebut dapat dilihat pada gambar 15 di bawah ini. Pada gambar tersebut kita membuat sebuah user dengan nama Marliana Sari yang diletakkan di dalam OU Teknik Informatika.



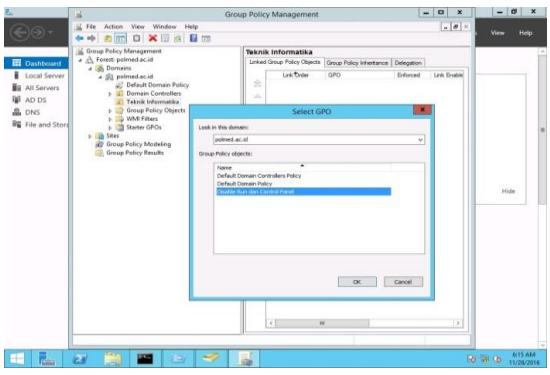
Gambar 15. Active Directory Users

Langkah keempat adalah membuat Group Policy Object yang akan diterapkan pada user maupun komputer. Hasil pembuatan Group Policy Object tersebut ditunjukkan pada gambar 16 di bawah ini. Pada gambar tersebut dibuat policy untuk membatasi akses user terhadap Start menu and Task Bar. Salah satu policy yang diatur adalah Remove Run menu from Start menu. Status semula item policy tersebut adalah Not configured. Agar policy tersebut diberlakukan kepada user maka status policy tersebut diubah menjadi Enabled.



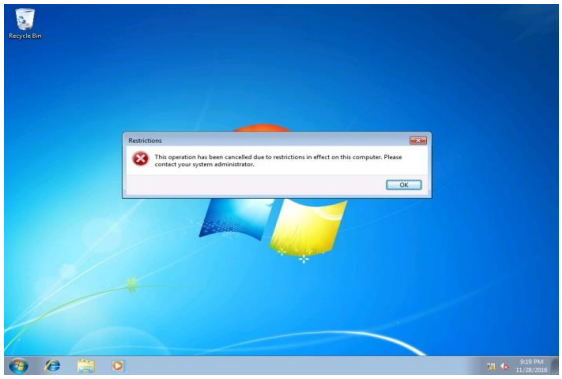
Gambar 16. Group Policy Object

Langkah kelima adalah menghubungkan Group Policy Object kepada Organizational Unit, Domain atau Site seperti yang ditunjukkan pada gambar 17 di bawah ini. Group Policy Object yang telah dibuat tersebut dihubungkan dengan OU Teknik Informatika, sehingga semua user yang ada di OU Teknik Informatika tersebut akan menerima pembatasan sesuai dengan yang sudah diatur di dalam GPO tersebut.



Gambar 17. Linked GPO

Langkah keenam adalah kita menguji GPO tersebut pada komputer client seperti yang ditunjukkan pada gambar 18 di bawah ini.Pertama kali user akan login menggunakan nama login yang dibuat



Gambar 18. Hasil Pengujian GPO

Hasil pengujian di atas menunjukkan bahwa client tidak bisa menjalankan Run sesuai dengan setting yang sudah di atur dalam GPO.

5. KESIMPULAN DAN SARAN

Dari pembahasan di atas dapat disimpulkan hal-hal sebagai berikut:

1. Group Policy Object (GPO) memberikan kemudahan bagi adminstrator untuk mengelola policy bagi user dan komputer.
2. Group Policy akan meningkatkan keamanan di jaringan karena bisa membatasi user agar tidak mengakses setting di komputer yang tidak diijinkan.

Adapun saran dari hasil penelitian ini sebagai berikut:

1. Penelitian ini belum mengaudit aksi yang dilakukan oleh user di jaringan.

DAFTAR PUSTAKA

[1] Andik Susilo, 2012. Panduan Praktis Microsoft Windows Server 2012. Elex Media Komputindo, Jakarta.

[2] Wahana Komputer, 2013. Konsep dan Implementasi Jaringan Menggunakan Windows Server 2012. Andi Offset. Jogjakarta.

[3] Tutang, 2015. Microsoft Windows Server 2012 R2. Datakom. Jakarta.

[4] Nanang Sadikin, 2008. Active Directory Windows Server 2008. Mataram Ciptakarsa. Jakarta.