آشنایی با شبکه‌های Domain و سرویس

اکتیو دایرکتوری

تفاوت Domainهای NT و Server 2000

یکی دیگری از تفاوت‌های Domainهای مبتی بر سیستم‌عامل NT و Domainهای بعد از سیستم‌عامل ۲۰۰۰-۲۰۰۳-۲۰۰۸ و 2008 R2 در خصوص authentication یا تصدیق هویت می‌باشد.

شاید این سؤال برای شما پیش آید که زمانی‌که شما یک User Name وPassword را برای Login نمودن به شبکه برروی یک کامپیوتر عضو Domain وارد می‌نمایید Domain Controller از کجا متوجه می‌شود که این User Name وارد شده همان کاربری است که در DataBase آن تعریف شده است؟

در جواب باید نگاهی به این پروسه داشته باشید. زمانی‌که کاربر اطلاعات User Name و Pass را وارد می‌کند و Ok می‌نماید این اطلاعات به صورت Encrypt و رمز می‌شود و به DataBase موجود در ساختار Active Directory فرستاده می‌شود. در این حالت DataBase اطلاعات را دریافتی را با اطلاعات موجود و تعریف شده در Database خود مقایسه می‌کند در صورت تأیید اطلاعات مجدداً User Name وPass وارد شده به‌صورت رمز شده (Encrypt) به مرحله Login فرستاده می‌شود در این مرحله اطلاعات از رمز خارج می‌شود و در صورت درستی اطلاعات اجازه Login داده می‌شود.

در گذشته یعنی در سیستم‌عامل NT این وظیفه برعهده پروتکل NTLM که مخفف New Technology LAN Manager می‌باشد انجام می‌شد.

پروتکل NTLM دارای چندین مشکل اساسی بود:

هک‌شدن سریع این پروتکل

سرعت پایین

نویسنده: هادی مشکانی فراهانی

http://danesh-ac.ir

https://telegram.me/daneshacademy

https://www.instagram.com/daneshacademy

پروتکل NTLM تنها به Server اجازه شناسایی هویت کاربران را می‌دهد و کلاینت‌ها یا سرویس گیرنده قادر به شناسایی هویت سرور نمی‌باشند. همچنین با استفاده از این پروتکل سرورها قادر به شناسایی هویت یکدیگرنمی‌باشند.

اعتبارسنجی NTLM برای محیط‌های شبکه‌ای که سرور حقیقی و واقعی پنداشته می‌شود، طراحی گردیده است.

بر همین اساس شرکت مایکروسافت در domianهای مبتنی بر سیستم‌عامل‌های سروری 2000, 2003, 2008 و 2008 R2 از پروتکل فوق امن و secure به نام Kerberos استفاده کرد. این پروتکل توسط دانشگاه برکلی آمریکا معرفی شد. این پروتکل به‌عنوان یکی از پیچیده‌ترین و امن‌ترین پروتکل‌های دنیا محسوب می‌شود. این پروتکل در ساختار Active Directory سیستم‌عامل‌های سروری Microsoft وLinux مورد استفاده قرار گرفته است. این پروتکل در هر دو سیستم‌عامل‌های linux وMicrosoft به‌عنوان پروتکل authentication مورد استفاده قرار می‌گیرد.

امروز از پروتکل NTLM برای authentication در سطح شبکه‌های Workgroup مورد استفاده قرار می‌گیرد.

معرفی پروتکل LDAP

مایکروسافت ساختار سرویس Active Directory را براساس پروتکل LDAP بنا نموده است. پروتکل LDAP به دغدغه‌های کاربران برای پیدا کردن منابع و سرویس‌ها پایان داده است و بی‌تردید می‌توان به‌عنوان مهمترین خصوصیت‌های Domainهای مبتنی بر سیستم‌عامل ۲۰۰۰ دانست.

تعریف پروتکل LDAP

Lightweight Directory Access Protocol یا LADP مجموعه از پروتکل‌ها و متدها برای دسترسی به اطلاعات ساختارهایی همانند Active Directory می‌باشد. علاوه‌بر این تعریف دیگری که برای این پروتکل ارائه شده است به شرح زیر می‌باشد.

در حقیقت LDAP ابزاری برای مدیریت اطلاعات شبکه، حساب‌های کاربری، ماشین‌های میزبان شبکه و منابع درون شبکه است. با استفاده از این استاندارد می‌توان یک مدیریت متمرکز و واحد را به کل پیکره شبکه اعمال نمود.

نویسنده: هادی مشکانی فراهانی

پروتکل LDAP کار خود را بر پایه استاندارد x.500 بنا نهاده است. استاندارد x.500 تعیین می‌کند که افراد و Objectها در Directory به چه نحوی سازماندهی شوند. دایرکتوری‌های x.500 تحت یک ریشه عمومی در ساختار سلسله مراتبی Tree با سطوح مختلف برای هر عنوان اطلاعاتی همانند کشور، ناحیه، سازمان، یا افراد سازماندهی می‌شود. به‌عنوان طراحی برای پیاده‌سازی مستحکم و ساده‌تر X.500 پروتکل LDAP اصل کاربردی محسوب می‌شد که به‌عنوان ستون فقرات سرویس Directory Active مایکروسافت و سرویس ناول دایرکتوری ارائه شد.

بعد از مدتی به این نکته پی برده شد که پروتکل LDAP دارای خصوصیاتی است که می‌تواند جایگزینی برای NIS شود. پروتکل LDAP برای ارتباط معمول از پورت TCP 389 و برای انجام Encryption از پورت TCP 636 استفاده می‌کند. علاوه‌بر این پروتکل LDAP می‌تواند با برنامه‌های خارجی دیگر که دارای authentication می‌باشند همانند Linux وUnix در ارتباط باشد.

LDAP روش یا متد استانداری برای به روزرسانی و دسترسی به Directoryهایی همانند ساختار Active Directory ارائه می‌دهد. این پروتکل این اجازه را به شما می‌دهد که از اطلاعات یک Tree استفاده نمایید به طور نمونه مشاهده نمایید که در این ساختار چه نوع Objectهایی وجود دارد.

پروتکل LDAP در بسیاری مواقع سریع‌تر از X.500 عمل می‌کند که بر همین اساس به این پروتکل لقب X.500 Lite را داده‌اند. پروتکل x.500 یک مدل کلی برای سرویس‌های مرتبط با Directoryهایی در OSI است.

در ساختار Directory مبتنی‌بر LDAP هر Object با این مشخصه معرفی می‌شود که به این مشخه متفاوت DN گفته می‌شود. هر نام DN می‌تواند از چندین نام متفاوت مرتبط RDN تشکیل شده باشد.

نمونه‌ای از این مشخصه‌ها:

DC : Domain Controller

CN : Comman Name

OU : Organization Unit Name

O : Organization Name

C : Country Name

از نمونه Serverهایی که با LDAP را ه‌اندازی می‌شوند می‌توان به موارد زیر اشاره نمود.

نویسنده: هادی مشکانی فراهانی

http://danesh-ac.ir

https://telegram.me/daneshacademy

https://www.instagram.com/daneshacademy

Microsoft Active Directory

Novell 6.5 NetWaree Directory

Open LDAP(linux)

Sun Directory Server

Fedora Directory Server

نسخه های مختلف Srver 2003 در نوع معماری پردازنده که شامل X64 و x86 می‌شود سخت‌افزارهای متفاوتی را در هر Edition پشتیبانی می‌کنند که در جدول زیر نمایش داده شده است.

استفاده شده است.Kerberos v.5ز پروتکل