

سامانه اخذ و احراز هویت مرکزی



شرکت متن باز سامان

(سهامی خاص)



فهرست

- ۱- معرفی محصول ۳
- ۲- زیرساخت LDAP ۴
- ۳- پنل مدیریت ۵
- ۴- سامانه ثبت نام ۶
- ۵- سامانه بازیابی رمز عبور ۸
- ۶- پروفایل کاربری ۹
- ۷- سرویس ثبت تغییرات (همگام سازی) ۹



۱- معرفی محصول

با توسعه روز افزون صنعت IT و استفاده سازمان‌ها از جنبه‌های مختلف آن و همچنین نظر به گسترش نرم‌افزارهای درون سازمانی جهت کنار گذاشتن راه‌کارهای سنتی، کاربران، روزانه باید بر روی سیستم‌ها و سرویس‌های مختلفی، به صورت مجزا عمل ورود را انجام دهند. در مواردی که از سیستم‌های احراز هویت مرکزی استفاده می‌شود، دغدغه کمتر است، چرا که کاربر تنها یک نام کاربری دارد و همه‌جا از آن برای ورود استفاده می‌کند. اما در سیستم‌هایی که هر کدام بانک اطلاعاتی مستقلی را جهت احراز هویت دارند، مشکل از این نیز فراتر می‌رود و کاربر اصولاً مجبور است برای هر سامانه نام کاربری و رمز عبور متفاوتی را در ذهن خود نگه دارد. نگهداری این نام‌های کاربری و کلمات عبور ساده نیست و باعث سردرگمی کاربران و پایین آمدن سطح امنیت می‌شود و این خود انگیزه استفاده از ابزارهای نوین فناوری اطلاعات را در کاربران کاهش می‌دهد.

بنابر توضیحات بالا، سازمان‌های امروزی تمایل به استفاده از راه‌کارهایی دارند که مبتنی بر یک سیستم یکپارچه احراز هویت مرکزی بوده، که در اینجا براساس OpenIdap پیاده‌سازی شده‌است و همچنین در کنار آن سامانه‌ای جهت ورود کاربران قرار گیرد تا هر کاربر پس از یکبار ورود، به سیستم‌های دیگر نیز دسترسی داشته باشد و در زمان خروج نیز بتواند ارتباط خود را از تمام سیستم‌ها به یکباره قطع کند، که اصطلاحاً به آن سرویس یکبار ورود یا SSO گفته می‌شود و در برشور آن محصول، به تفصیل توضیح داده شده‌است.

زیر سامانه‌های این محصول به شرح زیر است:

- زیرساخت LDAP
- پنل مدیریت
- سامانه ثبت نام
- سامانه بازیابی رمز عبور
- پروفایل کاربری
- سرویس ثبت تغییرات (همگام‌سازی)



۲- زیرساخت LDAP

LDAP یک سرویس تحت شبکه برای ذخیره، آرایش مناسب و جانمایی منابع سازمانی نظیر کاربران، کامپیوترها، سرویس‌ها و سایر ادوات می‌باشد. پایگاه داده این سیستم از نوع RDBMS نبوده و اصطلاحاً Flat است و همین امر باعث می‌شود تا یک سرویس الدپ بتواند به صدها هزار درخواست در لحظه پاسخ دهد (write کم و read بالا). همانطور که مشخص است عمل نوشتن روی این سیستم اصولاً به ندرت اتفاق می‌افتد و عمل خواندن بارها و بارها تکرار می‌شود. این پروتکل بسیار سبک بوده و کتابخانه‌های آن در زبان‌های مختلف بصورت کامل پیاده‌سازی شده‌است. اکثر سیستم‌های الدپ قابلیت Master-Master replication یا نوشتن همزمان و تبادل داده را بر روی چندین گره دارا هستند. در نسخه‌های قدیمی‌تر آن تنها یک گره امکان نوشتن را ارائه می‌نمود.

شرکت متن باز سامان از سرویس OpenLDAP جهت پیاده‌سازی سیستم‌های احراز هویت مرکزی استفاده می‌کند. این سیستم علاوه بر محبوبیت بسیار زیاد و کارایی فوق‌العاده می‌تواند تا ۴ گره بصورت همزمان برای نوشتن و تعداد نامحدودی گره برای عمل خواندن به عنوان slave را پشتیبانی نماید. این سیستم‌ها بصورت کلاستر شده و پشت لود بالانس راه‌اندازی می‌شوند تا در مباحث گسترش‌پذیری و دسترسی‌پذیری منعطف باشند.

قابلیت‌های این سرویس به شرح زیر است:

- ✓ احراز هویت مرکزی کاربر
- ✓ سفارشی‌سازی نمودن Schema بسته به نیاز سازمان
- ✓ پشتیبانی از نوشتن همزمان تا سقف ۴ نود
- ✓ توزیع‌پذیری و گسترش‌پذیری
- ✓ پشتیبانی از SSL^۱، SASL و TLS
- ✓ پشتیبانی از IPv6
- ✓ پشتیبانی از ACL^۲

Simple Authentication and Security Layer ۱

Access Control List ۲



- ✓ پشتیبانی از قالب تبادل داده^۳ یا LDIF
- ✓ انعطاف پذیری در تعریف attribute ها و object class ها
- ✓ پشتیبانی از attribute های چند مقدار^۴

۳- پنل مدیریت

شرکت متن باز سامان جهت تسهیل امور مربوط به مدیریت، حذف، اضافه و ویرایش کاربران و همچنین افزایش سرعت دسترسی به schema های توسعه داده شده، سامانه ای را تحت عنوان «سامانه مدیریت پست الکترونیک»، با زبان PHP بر روی فریم ورک Laravel، توسعه داده است که اطلاعات آن در سایت تحت همین عنوان قابل رویت می باشد. ویژگی های زیر بخش LDAP این سامانه به شرح زیر است.

- ✓ امکان ساخت، ویرایش مشخصه ها و حذف و جستجوی کاربران در LDAP
- ✓ تعیین سطوح دسترسی به مقادیر مختلف با استفاده از Role و Permission
- ✓ امکان تعریف دسترسی کاربر به همه سامانه ها
- ✓ مشاهده مشخصات کامل کاربران
- ✓ امکان انجام جستجوی ساده و پیشرفته
- ✓ امکان همگام سازی Schema الدپ توسط مدیر سیستم
- ✓ ایجاد فرم های مختلف بصورت خود کار بر پایه تعاریف Schema
- ✓ امکان تعیین مقدارهای پیش فرض برای فیلدهای مشخص
- ✓ امکان نمایش فیلدهای دلخواه در فرم های مختلف
- ✓ امکان پر شدن خود کار فرمها بر اساس اطلاعات وارده جهت سهولت و جلوگیری از خطای انسانی
- ✓ امکان تعریف و کنترل فیلدهای نمایش داده شده در قسمت جستجو
- ✓ امکان تعریف دامنه های مختلف و ساخت کاربر در دامنه مورد نظر

۳ Data Interchange Format

۴ Multi-value



- ✓ امکان ایجاد نقش‌های جدید و مشخص نمودن سطوح دسترسی آن‌ها به LDAP
- ✓ امکان مشاهده تمام Schemaها و روابط همگام‌شده با ال‌دی‌پی
- ✓ امکان نوشتن hint برای فیلدهای مد نظر و نمایش خودکار در فرم‌ها
- ✓ امکان اضافه نمودن کاربر از ال‌دی‌پی جهت ورود به پنل مدیریت و اعطای حق دسترسی
- ✓ امکان ایجاد هویت‌های مشخص (دانشجو، کارمند، استاد، مهمان و غیره) جهت سهولت و سرعت در ساخت کاربرها

OID	Name	Parent	Type	Required	Actions
0.9.2342.19200300.100.4.13	domain	top	STRUCTURAL	dc, objectClass	Details
0.9.2342.19200300.100.4.14	RFC822localPart	domain	STRUCTURAL	dc, objectClass	Details
0.9.2342.19200300.100.4.15	dNSDomain	domain	STRUCTURAL	dc, objectClass	Details
0.9.2342.19200300.100.4.17	domainRelatedObject	top	AUXILIARY	associatedDomain, objectClass	Details
0.9.2342.19200300.100.4.18	friendlyCountry	country	STRUCTURAL	co, objectClass, c	Details
0.9.2342.19200300.100.4.19	simpleSecurityObject	top	AUXILIARY	objectClass, userPassword	Details
0.9.2342.19200300.100.4.20	pilotOrganization	-	STRUCTURAL		Details
0.9.2342.19200300.100.4.21	pilotDSA	-	STRUCTURAL		Details
0.9.2342.19200300.100.4.22	qualityLabelledData	top	AUXILIARY	dSAQuality, objectClass	Details
0.9.2342.19200300.100.4.4	pilotPerson	person	STRUCTURAL	objectClass, cn, sn	Details

۴- سامانه ثبت نام

اولین قدم برای هویت یکپارچه در سازمان، تسهیل در دریافت نام کاربری هست. دریافت نام کاربری می‌تواند بر مبنای یک احراز هویت اولیه (ورود کد ملی و کد پرسنلی) بنا نهاده شود و یا اینکه



مثلاً تاریخ تولد را به عنوان تضمین کافی می‌توان به آن اضافه نمود. هویت نهایی در LDAP ساخته خواهد شد و پارامترهایی که مربوط به هویت یک کاربر هستند از یک سامانه مادر خوانده می‌شود و در LDAP ثبت خواهد شد.

ارتباط با سامانه مادر از طریق یک وب‌سرویس انجام می‌پذیرد (در اینجا سامانه پرسنلی) و یا می‌تواند از طریق یک view در دیتابیس انجام شود. البته با توجه به اینکه مشخصات کاربران فعلی نیز در سامانه LDAP وجود ندارد کاربران فعلی نیز در یک بازه زمانی مشخصی می‌بایست نسبت تکمیل ثبت نام خود اقدام نمایند.

لذا بصورت کلی قسمت ثبت نام دو قسمت خواهد داشت:

۱- ثبت نام کاربران جدید

۲- تکمیل ثبت نام کاربران قبلی

لازم به ذکر است که هزینه پیاده‌سازی سیستم ثبت نام بسته به انواع کاربر متفاوت خواهد بود. مثلاً اگر سازمان برای کاربران رسمی، مهمان، مشاور و غیره دارای فرآیندهای مختلف باشد بدیهی هست که پیاده‌سازی هر فرآیند سربار و زمان کاری خودش را دارد و در هزینه پیاده‌سازی لحاظ خواهد شد.

دریافت شناسه کاربری

شماره دانشجویی

شناسه هویتی

مقدار

تاریخ تولد

کد امنیتی



ارسال پاک کن



۵- سامانه بازیابی رمز عبور

سامانه بازیابی رمز عبور، به منظور بازیابی گذرواژه به ۲ روش زیر طراحی شده است:

- از طریق سوال امنیتی
- از طریق آدرس ایمیل دوم

Attribute های مربوط به هر کدام از دو روش فوق در LDAP تعبیه شده است و کاربر در هنگام ثبت نام موظف است حداقل یکی از آنها را جهت بازیابی، مقداردهی نماید. در طی فرآیند بازیابی، از کاربر خواسته می شود تا یکی از روش های فوق را انتخاب کند. در صورت انتخاب مورد اول، سوال امنیتی انتخاب شده در هنگام ثبت نام از او پرسیده می شود و جواب ثبت شده با مقدار موجود در LDAP مقایسه شده و صفحه ای مانند تصویر شماره ۵ نمایش داده می شود. در صورت انتخاب طریق دوم، ایمیلی به آدرس ایمیل دوم کاربر ارسال می شود و در نهایت دوباره کاربر به صفحه مذکور جهت انتخاب پسورد جدید، منتقل می شود.



۶- پروفایل کاربری

قسمت پروفایل کاربری جهت ورود کاربران و مشاهده پروفایل خودشان هست. همچنین براساس نیاز سازمان این امکان وجود دارد که بعضی فیلدها نشان داده نشوند و همچنین امکان مدیریت فیلدهایی که کاربران قادر به تغییر آنها هستند، از سمت پنل مدیریت وجود دارد. این سیستم بر اساس اطلاعات Schema همگام شده در پنل مدیریت اطلاعات کاربران را به صورت هوشمند به قسمت‌های مختلف تقسیم کرده و بر روی برگه‌های مختلف نمایش می‌دهد. کاربر می‌تواند از طریق این قسمت رمز عبور خود را نیز تغییر دهد.

۷- سرویس ثبت تغییرات (همگام‌سازی)

با توجه به اینکه اطلاعات افراد پرسنل، شاغل و غیره در سازمان ممکن است تغییر یابد سامانه‌ای جهت همگام‌سازی این اطلاعات راه‌اندازی خواهد شد که به صورت مرتب به سرور مادر متصل شده (این امکان هست که در صورت نیاز سرور مادر بتواند از طریق وب‌سرویس اطلاعات کاربران را بروز کند) و اطلاعات کاربرانی که تغییر کرده است را بروز می‌کند و بر حسب آن تغییرات لازم را اعمال می‌کند (مثلاً غیر فعال کردن یک کاربر). البته بدیهی هست که این روش از حالتی که سامانه مادر در هنگام تغییر اطلاعات، آن را به وب سرویس الدپ (که توسط شرکت ارائه خواهد شد) اعلام کند، کندتر خواهد بود.