

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- مشکل چیست؟

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 با نام‌های کاربری متفاوت 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. به لحاظ مدیریتی نیز در صورت قطع همکاری با یک کاربر، می‌بایست دسترسی او از سیستم‌های زیادی قطع شود.

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 اولین 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 (Single-Sign-On) گفته می‌شود و در بروشور محصول مربوطه، 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. در این سرویس Schema مشخصی جهت پوشش نیازهای سازمان/دانشگاه ایجاد می‌شود که تمام طبق RFC‌های الدپ نوشته و توسعه داده خواهد شد. 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 ۴ نود
- ✓ توزیع‌پذیری و گسترش‌پذیری و ضریب اطمینان از سرویس دهی
- ✓ پشتیبانی از SSL^۱، SASL و TLS
- ✓ پشتیبانی از IPv6



- ✓ پشتیبانی از ACL^۲
- ✓ پشتیبانی از قالب تبادل داده^۳ یا LDIF
- ✓ انعطاف پذیری در تعریف attribute ها و object class ها
- ✓ پشتیبانی از attribute های چند مقداره^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 شرکت نیز 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 ال دی پی 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

۲ Access Control List

۳ Data Interchange Format

۴ Multi-value



- ✓ امکان تعریف دامنه‌های مختلف و ساخت کاربر در دامنه مورد نظر
- ✓ امکان ایجاد نقش‌های جدید و مشخص نمودن سطوح دسترسی آن‌ها به LDAP
- ✓ امکان مشاهده تمام Schemaها و روابط همگام‌شده با ال‌دپ
- ✓ امکان نوشتن hint برای فیلدهای مد نظر و نمایش خودکار در فرم‌ها
- ✓ امکان اضافه نمودن کاربر از ال‌دپ 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

The screenshot shows the MBSCoPanel interface for managing LDAP Object Classes. The page title is "Object Classes" with a subtitle "List of all LDAP object classes". A sidebar on the left contains navigation options like "Dashboard", "Login History", "Server Status", "Settings", "MAIL", "Postfix", "Server Management", and "LDAP". The main content area features a table with columns: "OID", "Name", "Parent", "Type", "Required", and "Actions". The table lists various object classes such as "domain", "RFC822localPart", "dNSDomain", "domainRelatedObject", "friendlyCountry", "simpleSecurityObject", "pilotOrganization", "pilotDSA", "qualityLabelledData", and "pilotPerson". A pagination bar at the bottom indicates "Showing 1 to 10 of 113 entries".

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 می تواند 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 می توان 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 می شود و در LDAP ثبت خواهد شد.

ارتباط با سامانه مادر از طریق یک وب سرویس انجام می پذیرد (در اینجا سامانه پرسنلی) و یا می تواند 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 می بایست نسبت تکمیل ثبت نام خود اقدام نمایند.

لذا بصورت کلی قسمت ثبت نام دو قسمت خواهد داشت:

۱- ثبت نام کاربران جدید (دریافت هویت موقت و دائم)

۲- تکمیل ثبت نام کاربران قبلی

لازم به ذکر است که هزینه پیاده سازی 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 پیاده سازی هر فرآیند سربار و زمان کاری خودش را دارد و در هزینه پیاده سازی لحاظ خواهد شد. در ذیل تصاویری از قسمت ثبت نام آورده شده است.



سامانه مدیریت شناسه یکتا

صفحه اصلی
اعتبارسنجی هویت پرسنلی
پروفایل کاربری
بازنشانی رمز عبور
راهنما

اعتبارسنجی هویت پرسنلی

شماره پرسنلی

کد ملی

تاریخ تولد

< 1397 Aban >

Sa	Fr	Th	We	Tu	Mo	Su
4	3	2	1	30	29	28
11	10	9	8	7	6	5
18	17	16	15	14	13	12
25	24	23	22	21	20	19
2	1	30	29	28	27	26
9	8	7	6	5	4	3

October today

آیا شناسه کاربری سازمانی

شناسه کاربری سازمانی

رمز عبور

پاک کن
ارسال

کاربر گرامی

متنطور از شناسه کاربری سازمانی، نام کاربری فعلی شما است که برای ورود به پیندوز، سامانه‌های پرسنلی، اتوماسیون اداری و اینترنت استفاده می‌کند.

اگر شما چنین نام کاربری ندارید، می‌توانید تیک مربوطه را برداشته و ثبت نام خود را انجام دهید. اما در صورت داشتن این شناسه، شما آن را وارد کرده تا بعد از خدمات بهتری استفاده کنید.

مسئولیت عدم اعلام نام کاربری فعلی و عواقب آن به عهده شما خواهد بود.

در صورت هرگونه ابهام و یا مشکل با دفتر فناوری اطلاعات تماسی حاصل فرمایید.

تولید شده در شرکت متن باز سامان

اعتبار سنجی اولیه

صفحه اصلی
دریافت شناسه کاربری
پروفایل کاربری
بازنشانی رمز عبور
راهنما

دریافت شناسه کاربری

شماره دانشجویی

شناسه هویتی

کد ملی

مقدار

تاریخ تولد

کد امنیتی

پاک کن
ارسال



قوانین تعیین رمز عبور:

- رمز عبور نباید از A کاراکتر کمتر باشد.
- حداقل شامل یک حرف کوچک انگلیسی باشد.
- حداقل شامل یک حرف بزرگ انگلیسی باشد.
- حداقل شامل یک عدد باشد.

درخواست شناسه کاربری

شناسه کاربری درخواستی

رمز عبور

تکرار رمز عبور

شماره همراه

ایمیل شخصی شما (از این آدرس در صورت لزوم استفاده خواهد شد)

تکرار ایمیل

پاک کن
درخواست

کاربر گرامی

شناسه کاربری درخواستی می‌بایست منطبق با نوشتار نام و نام خانوادگی شما به انگلیسی باشد. نام‌های کاربری نامناسب و نامرتب تأیید نخواهد شد. بعنوان نمونه شخصی با نام **علی احمدی** می‌تواند یکی از نام‌های کاربری زیر را درخواست دهد:

a.ahmadi

ali.ahmadi

al.ahmadi

در صورتی که نام خانوادگی شما چند بخشی است می‌توانید از یکی از بخش‌های آن که بیشتر به آن شناخته می‌شوید استفاده کنید. در صورت هرگونه ابهام و یا نیاز به کمک، با کارشناسان دفتر فناوری تماس حاصل فرمایید.

ورود سایر اطلاعات

درخواست شناسه موقت

کد فعال سازی به 0902xxxxx26 ارسال شد

کد تایید

ارسال مجدد؟

پاک کن
درخواست

تعیین اصالت شماره همراه

پایان

درخواست حساب کاربری شما با موفقیت ثبت شد

تایید یا عدم تایید حساب کاربری شما از طریق پیامک و ایمیل به اطلاع شما خواهد رسید. در صورت تایید می‌توانید از حساب کاربری خود استفاده کنید.

نام کاربری مورد درخواست شما: **di**

در صورت طولانی شدن تایید یا عدم تایید می‌توانید با دفتر فناوری تماس حاصل فرمایید.

سامانه احراز هویت مرکزی



درخواست کاربران توسط مدیرانی که مجوز دارند قابل تأیید یا رد هست که در هر دو صورت به اطلاع کاربر رسانده می‌شود:

User Requests All user requests in the database. Admin > User Requests > List

10 records per page Search:

National ID	First Name	Last Name	Email	User Type	Department	Actions
0047	سعید	ابو	hes. ac.ir	3	دفتر بنی اطلاعات	Reject Approve Delete

National ID First Name Last Name Email User Type Department Actions

Showing 1 to 1 of 1 entries Previous 1 Next

همچنین عملیاتی که مدیران بر روی کاربران مختلف انجام می‌دهند، ثبت شده و قابل مشاهده خواهد بود که مثلاً درخواست‌ها توسط چه کسی تأیید و یا رد شده است. هر دو این قسمت‌ها در پنل مدیریت یکپارچه شرکت متن باز سامان ایجاد شده است.

Activity Logs All activity logs in the database. Admin > Activity Logs > List

FILTERS Date range National ID or Email Remove filters

10 records per page Search:

Log Date	Event
	User request with national ID 0083 for email address metal. ac.ir was approved by Sha. udeh
	User request with national ID 121 for email address moh. c.ir was approved by superadmin

Log Date Event

Showing 1 to 2 of 2 entries Previous 1 Next



۵- سامانه بازیابی رمز عبور

سامانه بازیابی رمز عبور، به منظور بازیابی گذرواژه به ۳ روش زیر طراحی شده است:

- از طریق سوال امنیتی
- از طریق آدرس ایمیل دوم
- از طریق شماره تلفن همراه

Attribute های مربوط به هر کدام از روشهای 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 روشهای 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 رمز عبور جدید، منتقل می شود.

رمز عبور

روش ارسال کد فعال سازی

ارسال کد تایید با موبایل

ارسال کد تایید با ایمیل

نام کاربری

ارسال کد بازنشانی



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 شرکت متن باز سامان، اطلاعات کاربران را به صورت هوشمند به قسمتهای مختلف تقسیم کرده و بر روی برگه‌های^۵ مختلف نمایش می‌دهد. کاربر می‌تواند از طریق این قسمت رمز عبور خود را نیز تغییر دهد.

تصویر صفحه بعد نمای کلی پروفایل کاربری را نمایش می‌دهد.



تغییر رمز عبور

رمز عبور قدیمی

رمز عبور جدید

تکرار رمز عبور

Please fill out this field.

پنل مدیریت

کاربر فایل

اطلاعات پرسنلی

اطلاعات سیستمی کاربر

کاربر

تغییر رمز عبور

سعید علی

خروج

تاریخ تولد:

محل تولد

نام پدر

تهران

هدایت اله

۷- سرویس ثبت تغییرات (همگام سازی)

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.