شرکت متن باز سامان

تولید و توسعه سیستم‌عامل لینوکس و نرم‌افزارهای متن باز سفارشی

طرح سامانه احراز هویت مرکزی و یک‌بار ورود

نسخه ۱,۰

دی ۱۳۹۵

فهرست

مقدمه ۲
LDAP ۳
زیر ساخت سیستم LDAP ۳
ملزومات راه‌اندازی سرویسها ۳
سیستم مدیریت متمرکز LDAP ۴
واسط کاربری ۴
مشاهده وقایع ۴
مدیریت کاربران ۵
SSO ۶
مزایا ۶
معایب ۶
انواع سرویسهای SSO ۶
سامانه انتخابی ۷
ویژگیهای سامانه ۷
مدلهای اجرا و پیاده‌سازی ۷
معماری طرح ۹
برخی از پروژه‌های انجام شده ۱۰
پرسشنامه فنی مرتبط با سامانه احراز هویت مرکزی ۱۱
فرم پرسشنامه ۱۱

مقدمه

در راستای توسعه روز افزون صنعت IT و استفاده سازمانها از جنبه‌های مختلف این صنعت و نظر به گسترش نرم‌افزارهای درون سازمانی جهت کنار گذاشته شدن روشهای سنتی، کاربران مجبور هستند، روی هر سیستم 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. اما در سیستمهایی که هر کدام بانک اطلاعاتی خودشان را جهت احراز هویت به کار می‌گیرند، مشکل از این نیز فراتر می‌رود و کاربر اصولا مجبور است که برای هر سامانه نام کاربری و رمز متفاوتی را در ذهن خود نگه‌دارد. نگهداری این نام‌های کاربری و کلمات عبور ساده نیست و باعث سردرگمی کاربرانی می‌شود که آنچنان هم مایل به استفاده از سیستم‌های امروزی نیستند.

لذا سازمانهای امروزی اصولا تمایل پیدا کرده‌اند تا از راه‌حلهایی استفاده کنند که مبتنی بر یک سیستم یکپارچه احراز هویت مرکزی بوده و همچنین در کنار آن سامانه‌ای جهت ورود کاربران قرار گیرد که هر کاربر پس از یکبار ورود به سیستم‌های دیگر نیز دسترسی داشته باشد و در زمان خروج نیز از تمام سیستم‌ها بتواند ارتباط خود را به یکباره قطع کند.

شرکت متن باز سامان با توجه به سابقه خود در طراحی و پیاده‌سازی و توسعه سیستم‌های احراز هویت مرکزی (LDAP) و سامانه‌های یکبار ورود (SSO) طرح پیش رو را جهت بررسی اولیه آن سازمان محترم ارائه کرده است تا با سهولت بیشتری طی مراحل بعدی را آماده سازد.

LDAP یک پروتکل نرم‌افزاری برای ذخیره و آرایش مناسب و جانمایی مربوط به منابع سازمانی شامل کاربران، کامپیوتران، سرویس‌ها و سایر ادوات می‌باشد. پایگاه داده این نوع سیستم‌ها از نوع RDBMS نبوده و همین امر باعث می‌شود تا یک سرویس الدپ بتواند به صدها هزار درخواست در لحظه پاسخگو باشد. همانطور که مشخص است عمل نوشتن روی این سیستم اصولا به ندرت اتفاق می‌افتد و عمل خواندن بارها و بارها تکرار می‌شود.

این پروتکل بسیار سبک بوده و در زبانهای مختلف کتابخانه‌های آن بصورت کامل پیاده‌سازی شده است. اکثرا سیستمهای الدپ توان Master-Master replicationیا نوشتن همزمان و تبادل داده را بر روی چندین نود دارا هستند. در سرویسهای قدیمی آن تنها یک نود 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 فوق العاده می‌تواند تا ۴نود بصورت همزمان نوشتن را پشتیبانی نماید و به تعداد نامحدودی میتواند از نودهای slave که تنها برای خواندن اطلاعات هست استفاده کند. این سیستمها بصورت کلاستر شده و پشت لود بالانسر راه اندازی می‌شود تا در حد نیاز بتواند در مواقع لزوم گسترش یابد.

زیر ساخت سیستم LDAP

با توجه به ضرورت در دسترس بودن این سرویس، در تمامی زمانهایی که ممکن است یکی از سرویس‌دهنده‌ها دچار اختلال کاری از لحاظ نرم‌افزاری یا سخت‌افزاری شود، لذا استفاده از موارد زیر پیشنهاد می‌شود:

۱- استفاده از OpenLDAP نسخه ۲,۴ – در نسخه ۲,۴ امکان write همزمان بر روی چندین نود وجود دارد. در این نسخه چندین سیستم به عنوان Master تعریف شده و هر بروزرسانی در هرکدام انجام شود سرورهای دیگر نیز مطلع می‌شوند. این روش باعث می‌شود تا از single point of failure جلوگیری شود و عمل نوشتن در صورت در دسترس نبودن هر کدام از نودها در نودهای دیگر صورت گیرد.

۲- استفاده از سیستم‌های تقسیم بار - استتفاده از سیستمهای توزیع بار یا LoadBalancer باعث می‌شود تا زمانی که یک سیستم بخواهد با LDAP صحبت کند، تنها بسته‌های خود را به یک IP ارسال می‌کند. سیستم توزیع بار بر اساس الگوریتم تعیین شده، ترافیک دریافتی را به یکی از سرورهای پشت سر خود که در صحت و سلامت کامل به سر می‌برد ارسال می‌کند. اگر هر کدام از سرورهای LDAP دچار مشکل شوند دیگر ترافیکی به آن فرستاده نمی‌شود. مشکلات سیستم‌های LDAP یا قطعی بعضی از نودها از دید سرویسی که می‌خواهد با آن صحبت کند کاملا مخفی خواهد ماند.

ملزومات راه‌اندازی سرویسها

جهت راه‌اندازی نسخه ۲,۴ از نرم‌افزار OpenLDAP ملزومات زیر مورد نیاز هست:

۱- حداقل چهار سرور مجازی جهت راه‌اندازی سیستمهای LDAP (مشخصات سخت افزاری پس از دریافت RFP ارسال می‌شود)

۲- دو سرور مجازی جهت راه‌اندازی سیستمهای توزیع‌بار(مشخصات سخت افزاری پس از دریافت RFP ارسال می‌شود)

۳- import کردن اطلاعات قبلی در سیستم جدید (برای مواردی که سرویس الدپ در حال حاضر موجود باشد)

سیستم مدیریت متمرکز LDAP

با توجه به نیازمندیهای فعلی اکثر سازمانها، یک نرم‌افزار تحت وب برای رفع نیازهای مدیریت اطلاعات کاربران و پیگیری و رفع اشکال کاربران سیستم‌های مبتنی بر پایه زیرساخت LDAP پیشنهاد می‌شوند.

مشخصات این سامانه مدیریت تحت وب طبق بندهای ذیل است.

واسط کاربری

این نرم‌افزار مدیریتی بصورت تحت وب اجرا خواهد شد. این واسط کاربری همچنین می‌تواند بستری مناسب برای دیگر ابزارهای مورد نیاز و نرم افزارهای تحت وب سازمان باشد. از ویژگی‌های این واسط کاربری می‌توان به موارد زیر اشاره کرد :

۱- واسط تطبیق‌پذیر ۱ : واسط کاربری ارائه شده قابلیت این را دارد که با توجه به مرورگر و دستگاه استفاده شده برای نمایش خود را مطابقت دهد. این ویژگی بدان معناست که شما می‌توانید به راحتی از این رابط در گوشی‌های هوشمند، دستگاه‌های تبلت و رایانه‌های شخصی استفاده کنید.

۲- مطابقت با استانداردها : صفحات و محیط نرم‌افزار بر روی تمامی مرورگرهایی مطابق با استانداردهای وب ساخته شده‌اند قابل استفاده می‌باشد.

۳- استفاده از بروزترین تکنولوژی‌های تحت وب برای ارائه محیط کاربری ساده و در عین حال کارآمد. (مانند Ajax)

۴- قابل استفاده بر روی مرورگرهای قدیمی : طراحی محیط گرافیکی به صورتی انجام شده که مرورگرهای قدیمی نیز بتوانند اکثر فرآیندهای مهم و ضروری را اجرا کنند. این امکان به کاربران اجازه می‌دهد که در شرایطی که به رایانه خود دسترسی ندارند و یا مجبور به استفاده از مرورگری قدیمی هستند بتوانند فرآیندهای مهم را اجرا کنند.

مشاهده وقایع

این نرم افزار جهت استفاده تیم پشتیبانی سازمان و با هدف سرعت بخشیدن به خدمات و افزایش کیفیت آنها طراحی شده است. این سیستم یک سامانه زیرساختی مجزا است که تمام وقایع سیستم‌ها را جمع‌آوری کرده و در یک سیستم زیرساختی NoSQL ذخیره و index می‌شوند. در زیر لیستی از امکانات پیشنهادی شرکت متن باز سامان قرار گرفته است :

۱- قابلیت خواندن و تجزیه کردن Log نرم‌افزار LDAP

۲- امکان نمایش متن اصلی Log جهت عیب یابی موارد خاص و پیچیده

۳- امکان تفکیک بر اساس نوع فرآیند انجام شده. برای مثال Modify، Search و ...

۴- امکان نمایش در لحظه Log های جدید به مسئولین پشتیبانی جهت عیب یابی تعاملی با کاربران (نسخه‌های آتی)

۵- گروه بندی اطلاعات بر اساس دامنه‌های سازمان و امکان اعطای سطوح دسترسی به کاربران برای مدیریت دامنه‌های خاص

۶- امکان تنظیم میزان بایگانی اطلاعات بر اساس نوع عملیات و دامنه کاربر

مدیریت کاربران

این قسمت نرم‌افزار جهت تایید ثبت نام، ویرایش، مشاهده و گزارش‌گیری از اطلاعات کاربران سازمان که در زیر ساخت یکپارچه LDAP ذخیره می‌شوند طراحی شده است. خروجی این سیستم موارد ذیل خواهد بود:

۱- ایجاد محیط مدیریت غنی با کاربری بالا و در عین حال ساده و کاربر پسند

۲- ساده کردن فرآیندهای چند مرحله ای و شکستن آنها به فرم‌های ساده تر

۳- قابل استفاده بودن نرم‌افزار بر روی دستگاه های مختلف ارتباطی از جمله گوشی‌های تلفن همراه هوشمند، Tablet ها، لپ‌تاپ های با نمایشگر کوچک و رایانه‌های شخصی

۴- قرار دادن امکان ویرایش تنظیمات نرم‌افزار برای مدیران که نیاز به پشتیبانی نرم‌افزار و قابلیت‌های آنرا افزایش می‌دهد.

همچنین با توجه به نیازمندیهای یک سازمان موارد ذیل نیز به عنوان امکانات پیشنهادی شرکت به سازمان ارائه می‌گردد که با توجه به سیاستهای هر سازمان می‌بایست تعریف گردد:

۱- امکان ثبت کاربران توسط تیم پشتیبانی سازمان

۲- توسط خود کاربران و منطبق با فرآیند موجود در سازمان

۳- ایجاد کاربران مهمان

۴- برخی مشخصات تعیین شده (برای مثال نام و رمز عبور) توسط خود کاربران (امکان پیشنهادی)

۵- امکان اضافه کردن دامنه‌های جدید به زیرساخت LDAP که در رایانامه سازمان و دیگر نرم‌افزارها قابل استفاده خواهد بود.

۶- امکان نمایش مشخصات کاربران و دامنه‌ها و گزارش گیری از اطلاعات هر دامنه و کاربر.

۷- تعریف سطوح دسترسی گوناگون برای کاربران با حق ویرایش.

۸- تعریف و اجرا فرم‌های ورود اطلاعات گوناگون بسته به نیازهای سازمان. برای مثال فرم‌های گوناگون ثبت کاربر.

SSO به معنی Single sign-on یک روش ورود به سامانه‌های مختلف ولی از طریق یک درگاه ثابت است. با این روش کاربر یک بار به این سامانه SSO متصل می‌شود و سپس به همه سیستمهای دیگر که مجوز داشته باشد، بدون احراز هویت جدید متصل خواهد شد. این با روش با در دست داشتن یک سامانه پشتی مبتنی بر LDAP قابل پیاده‌سازی خواهد بود. البته باید بدانیم که مفهوم Single sign-off یا Single logout نیز وجود دارد که در زمان خروج یک کاربر از یک سیستم از همه سامانه‌ها خارج خواهد شد.

مزایا

موارد زیر را به عنوان مزایای استفاده از SSO می‌توان نام برد.

۱- عدم استفاده از نام‌های کاربری مختلف در سامانه‌های متفاوت

۲- صرفه جویی در زمان به علت عدم نیاز به وارد کردن نام کاربری و رمز برای هر سامانه

۳- صرفه‌جویی در زمان و تعداد افراد پشتیبان در یک سازمان به علت پاسخگویی کمتر بابت نام‌های کاربری متفاوت

۴- احراز هویت مجتمع و متمرکز و ثبت ورود همه افراد در یک سامانه

۵- کنترل دسترسی ورود افراد از یک درگاه

معایب

با توجه به اینکه کاربر می‌تواند با یک بار ورود به همه سامانه‌ها دسترسی داشته باشد، استفاده از SSO دارای اشکالاتی هست که باعث می‌شود سازمان نیاز به این مطلب را احساس کند که داشتن نام کاربری و رمز عبور تنها جهت استفاده از سیستمها اطمینان بخش نیست.مخصوصا برای کسانی که دسترسی های مهمی را به سامانه‌ها دارا هستند.

با توجه به اینکه یک کاربر بعد از ورود به سامانه SSO می‌تواند به همه سامانه‌های دیگر نیز دسترسی داشته باشد، لذا باید اصولا یک سرور احراز هویت دیگر با استفاده از پروتکلی دیگر همیشه در کنار SSO وجود داشته باشد. سامانه‌هایی مانند smart cards یا one-time password یا همان رمز یکبار مصرف.

در کل می‌توان گفت که SSO می‌تواند به همراه مدل احراز هویت ۲ فاکتوری (رمز کاربر بهمراه مثلا رمز یکبار مصرف) به مراتب امن‌تر باشد.

عیب دیگر در مشکلات مربوط به سامانه SSO از دسترس خارج شدن آن هست. در صورتی که سامانه SSO به هر دلیلی کار نکند، کاربران دیگر قادر به ورود در سامانه‌های دیگر نخواهند بود. روش حل این مشکل استفاده از کلاسترینگ و لودبالانسینگ برای این سامانه است. لازم به ذکر است که از لودبالانسرهای در نظر گرفته شده برای سرویس LDAP برای سیستم SSO نیز استفاده خواهد شد.

انواع سرویسهای SSO

روشهای مختلفی جهت ارتباط کلاینت با سیستم SSO وجود دارد. در زیر آورده شده است:

۱- مبتنی بر kerberos

۲- مبتنی بر Smart card

۳- مبتنی بر احراز هویت کلاینت ویندوزی

۴- مبتنی بر SAML

سامانه انتخابی

سامانه‌های بسیار زیادی برای پیاده‌سازی SSO در دنیا وجود دارد. چه سامانه‌های متن باز و چه آنها که تجاری هستند و چه مواردی که بصورت سرویسهای رایگان در دنیا وجود دارند مانند سرویس OAuth2 شرکت گوگل. اما یکی از کاملترین سامانه‌ها که سالهاست توسعه داده شده و در سازمانهای بزرگی در دنیا استفاده می‌شود مربوط به گروه Jasig تحت نام CAS هست که کاملا نیز متن باز است.

این نرم‌افزار و نسخه ۴ آن جهت پیاده‌سازی SSO پیشنهاد می‌گردد و قبلا شرکت متن باز در مراکز دیگری نیز این سیستم را پیاده‌سازی نموده است. البته لازم به ذکر است که نرم‌افزارهای دیگری مانند OpenAM و barebones cms نیز وجود دارند که آنها نیز تمام قابلیت‌های Jasig CAS را دارا هستند. اما با توجه به اینکه شرکتهای ایرانی اکثرا نرم‌افزارهای خود را با سامانه Jasig CAS توسعه دادند لذا پیشنهاد می‌شود که از این سامانه استفاده شود.

ویژگیهای سامانه

این نرم‌افزار یک سامانه رده بالا و حرفه‌ای محسوب می‌شود که قابلیت‌های زیادی در آن وجود دارد که شاید مقداری کمی از آنها در یک سازمان استفاده شود.

۱- استفاده از زبان برنامه‌نویسی جاوا و توسعه بصورت MVC بر روی فریم ورک Spring

۲- احراز هویت ماژولار از طریق LDAP. Database. X.509 و احراز هویت ۲ فاکتوری

۳- پشتیبانی از پروتکلهای استاندارد SSO شامل CAS. SAML. OAuth. OpenID

۴- دارا بودن کتابخانه‌های سمت کلاینت جهت اتصال سایر سامانه ها برای زبانهای برنامه‌نویسی Java .NET. PHP. Perl و غیره

۵- یکی‌شدن (Integrateبا نرم‌افزارهای uPortal. Drupal. Liferay. BlueSocket. Moodle. Google Apps و غیره

۶- چند زبانه بودن

۷- ارائه وب سرویس با استفاده از پروتکل RESTful

۸- دارابودن اجتماع قوی کاربری و مستندات کامل و دقیق و بروز

مدلهای اجرا و پیاده سازی

دو روش پیاده‌سازی برای این سامانه وجود دارد که به ترتیب ذیل است:

۱- روش Standalone

۲- روش Clusterشده

به صورت کلی روش دوم پیشنهاد می‌گردد. چرا که از دسترس خارج شدن سرویس SSO می‌تواند نتایج بدی در یک سازمان داشته باشد. و با توجه به اینکه این سرویس عموما برای سازمانهای بزرگ مورد نیاز هست، علیرغم استفاده از زیرساخت‌های مجازی که امکان نگهداری ماشین مجازی را بصورت همیشگی (با ضریب اطمینان بالا) دارا است، می‌بایست قابلیت اطمینان در لایه سرویس نیز الزاما فراهم گردد.

با توجه به نیازهای مختلف سازمانها معماری پیاده‌سازی این سیستم بسته به نیاز یک سازمان پس از ارائه RFP تقدیم خواهد گردید.

برخی از پروژه‌های انجام شده

بعضی از پروژه‌های انجام شده در بحث احراز هویت مرکزی و سامانه یکبار ورود موارد ذیل بوده است:

۱- صدا و سیمای جمهوری اسلامی ایران – سال ۸۸ – طراحی و پیاده‌سازی احراز هویت مرکزی و طرح بروزرسانی آن بطوری که ۶ سرور توسط ۲ سرور لودبالانسر پاسخ کلیه نیازهای سازمان است.

۲- دانشگاه تهران – توسعه سیستم‌های الدپ و SSO و بازطراحی فرآیندهای ثبت نام و مدیریت کاربران و سامانه سیک اطلاعات با سامانه‌های مبدا دانشجویی و پرسنلی– سال ۹۴

۳- دانشگاه علوم پزشکی شهید بهشتی-راه‌اندازی و طراحی سامانه احراز هویت مرکزی-سال ۹۲

۴- دانشگاه علوم پزشکی شهید بهشتی – توسعه سرویس الدپ و سیستم سینک دانشجویی و پرسنلی با سامانه‌های مبدا – سال ۹۴

۵- دانشگاه شهید باهنر کرمان – پیاده‌سازی و راه‌اندازی سرویس الدپ و سامانه ثبت نام کاربران و سینک اطلاعات – سال ۹۳ و ۹۵

۶- پژوهشگاه فناوری اطلاعات و ارتباطات (مرکز تحقیقات مخابرات) – پیاده‌سازی سیستم احراز هویت مبتنی بر سامبا۴ و جایگزینی سرویس‌های ویندوزی و پیاده‌سازی سیستم SSO – سال ۹۳

شرکت متن باز سامان

پرسشنامه فنی مرتبط با سامانه احراز هویت مرکزی

کارفرمای گرامی خواهشمند است پس از مطالعه دقیق طرح پیشنهادی نسبت به اعلام نیازمندیهای خود و همچنین ارسال پاسخ کامل و دقیق مربوط به سوالات ذیل اقدام بفرمایید.

فرم پرسشنامه

۱- وضعیت فعلی کاربران به چه صورت بوده و در چه سیستمی نگهداری می‌شود؟ فرمت داده کاربران فعلی به چه صورت هست.

۲- سامانه‌های هویتی مجموعه شامل چه مواردی است؟ (پرسنلی، دانشجویی و غیره)

۳- آیا امکان ارتباط با سایر سامانه‌ها وجود دارد؟ (از چه روشی)

۴- آیا نیازی به مهاجرت کاربران فعلی وجود دارد؟ (با شرح کامل)

چه کسانی به سیستم دسترسی خواهند داشت و چه نوع دسترسی را خواهند داشت؟

۵- نحوه ورود کاربران به سامانه به چه طریق خواهد بود؟ (استفاده از LDAP؟ CAS؟ یا با حساب کاربری تعریف شده در سامانه‌ها؟)

۶- چه سامانه‌هایی به سیستم SSO یا LDAP متصل خواهند شد.؟ این سامانه‌ها از چه زبان برنامه‌نویسی استفاده می‌کنند؟

۷- تعداد تخمینی کاربران چه میزان است؟

۸- ویژگیهای خاص یا مهم سامانه‌های خود را مشخص نموده و هر مورد مهمی که در پیاده‌سازی سیستم جدید اهمیت دارد را ذکر کنید.

۹- آیا اطلاعات کارکنان به صورت ذخیره شده در پایگاه داده و به طور یکپارچه و کامل و یکتا وجود دارد؟

۱۰- چه نوع جستجو و گزارش‌هایی در سطح سامانه مورد نیاز است؟

۱۱- موارد دیگری که جزء نیازمندیهای سازمان بوده و در سوالات بالا قید نشده را در شرح نیازمندیهای خود بصورت نسبتا جامع ذکر کنید.