

سامانه یکبار ورود

SSO 5.2



شرکت متن باز سامان

(سهامی خاص)



فهرست

- ۱- معرفی محصول ۳
- ۲- معماری ۴
- ۳- پنل مدیریت ۵
- ۴- صفحه ورود کاربران ۱۱
- ۵- محل ذخیره کاربران و اطلاعات آنها ۱۲



۱- معرفی محصول

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. به بیان دیگر SSO پروسه احراز هویت کاربر می‌باشد که به او اجازه می‌دهد تا برای دستیابی به چندین برنامه نرم‌افزاری مستقل ولی مرتبط، از یک نام کاربری و کلمه عبور یکسان استفاده نماید. این روش با یک سامانه پستی مبتنی بر LDAP (سامانه اخذ و احراز هویت مرکزی) پیاده‌سازی می‌شود که مسئولیت احراز هویت کاربران را برعهده دارد. البته شایان ذکر است 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.

استفاده از این سرویس در بسیاری از سرویس‌های معروف دنیا نظیر Gmail و Facebook نیز وجود دارد و شما با نام کاربری و در واقع ایمیلی که دارید (همیشه یکتا^۱ است) می‌توانید در سرویس‌های دیگر نیز ورود کنید و از همان نام کاربری و گذرواژه برای سایر خدمات نیز بهره ببرید. شرکت متن‌باز سامان با بهره‌گیری از پروتکل‌های LDAP^۲ و CAS^۳ این سرویس را در بسیاری از سازمان‌های کشور راه‌اندازی کرده است.

زیر سامانه‌های این سرویس عبارتند از:

- پنل مدیریت
- صفحه ورود کاربران

۱ Unique

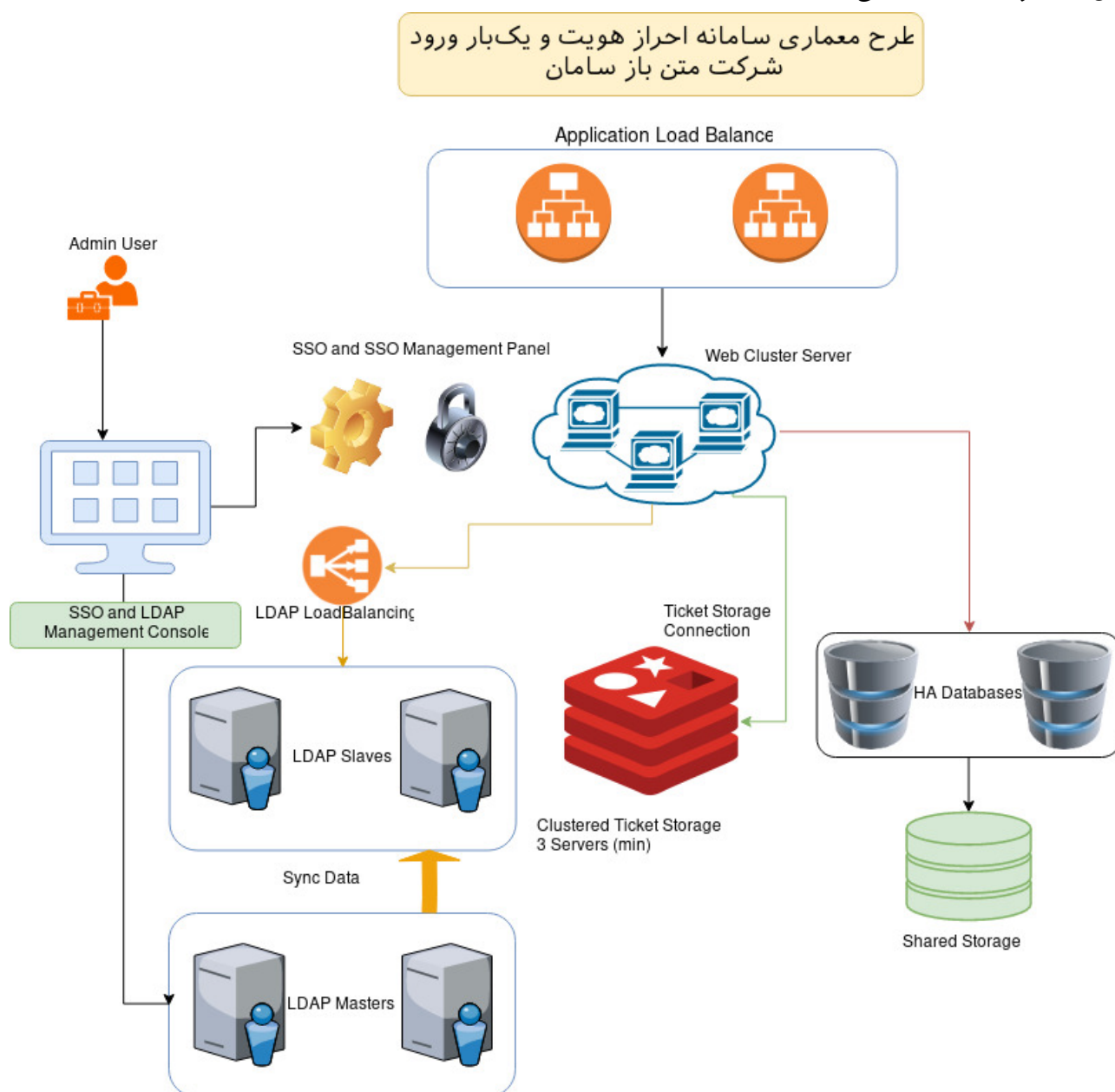
۲ Lightweight Directory Access Protocol

۳ Central Authentication Service



۲- معماری

سرویس متن باز سامان از یک معماری بسیار پیشرفته و پیچیده جهت حفظ کیفیت و پایداری و گسترش پذیری سرویس در تمام لایه‌ها استفاده می‌کند. این معماری علی‌رغم پیچیده بودن به سهولت و با برنامه‌های خودکاری که تولید شده است، نصب و راه‌اندازی می‌گردد. در تصویر ذیل معماری مفهومی و منطقی این محصول را مشاهده می‌کنید.





۳- پنل مدیریت

این سامانه تحت وب در نسخه‌های جدید به عنوان یک سرویس مستقل از CAS پیاده‌سازی شده است و به منظور مدیریت، حذف و اضافه کردن تمام خدمات CAS استفاده می‌شود. پنل مدیریت، همراه با سایر ویژگی‌های سرویس، به مدیر سیستم امکان کنترل سرویس‌هایی که اجازه دارند از طریق CAS احراز هویت کنند، را می‌دهد.

قابلیت‌های این سامانه به شرح زیر است.

- ✓ امکان حذف، اضافه و مدیریت ارتباط سایر سامانه‌ها با SSO
- ✓ مدیریت دسترسی کاربران به هر سامانه بر اساس مقدار فیلدهای مشخص شده (این امکان در تعامل با LDAP می‌تواند دسترسی کاربر را به سامانه‌های مشخصی برقرار یا قطع کند).
- ✓ امکان تعریف ورود با فیلدهای مختلف کاربر که یکتا هست (نام کاربر، ایمیل، کد ملی و غیره)
- ✓ امکان ارسال مقادیر Attribute‌های تعریف شده به ازای هر سامانه و تعیین نحوه آن بصورت کاملاً متنوع
- ✓ توانایی کاربر در کنترل اینکه چه Attribute‌هایی تحویل سامانه مورد نظر شود. این قابلیت مشابه عمل کرد گوگل در زمان احراز هویت یک سامانه جانبی هست که قبل از ارسال اطلاعات درخواستی سامانه، به کاربر صفحه‌ای را نمایش می‌دهد و کاربر می‌بایست این مسأله را تأیید کند. تنظیمی که کاربر مشخص می‌کند ذخیره شده و در دفعات بعدی ورود استفاده می‌شود.
- ✓ امکان فعال و غیرفعال نمودن سامانه‌ها بصورت دستی و یا خودکار بر اساس تاریخ (expiration)
- ✓ امکان کنترل دسترسی کاربران به سامانه‌ها بر اساس تاریخ، مقادیر مشخصه‌های کاربری و همچنین جلوگیری از دسترسی بر اساس مقادیر مشخصه‌های کاربری. این قابلیت باعث کنترل دسترسی کاربران به سامانه‌های مختلف بر اساس هویت و مقادیر اطلاعاتی آنها می‌شود و نیازی به پیاده‌سازی در سمت سرویس گیرنده نیست.
- ✓ امکان سفارشی‌سازی Logo و Theme برای هر سامانه
- ✓ امکان تعریف نمودن URL مربوط به Logout برای هر سامانه
- ✓ امکان تعریف URL دیگری جهت انتقال کاربرانی که احراز هویت آنها موفق نبوده است
- ✓ امکان تعریف تاریخ انقضاء برای هر سامانه و اطلاع‌رسانی آن به کاربران



- ✓ امکان تعریف ورود ۲ مرحله‌ای (Duo Security, FIDO U2F, YubiKey, Google Authenticator, Microsoft)
- ✓ پشتیبانی از سیستم‌های احراز هویت (LDAP, Database, X.509, SPNEGO, JAAS, JWT, RADIUS, M) (MongoDb)
- ✓ پشتیبانی از پروتکل‌های (CAS, SAML, WS-Federation, OAuth2, OpenID, OpenID Connect, REST)
- ✓ امکان محول نمودن احراز هویت به فراهم‌کنندگان خارجی نظیر ADFS, Facebook, Twitter, SAML2 IdPs
- ✓ پشتیبانی از مدیریت رمز عبور، اعلان‌ها، شرایط استفاده و جعل هویت به صورت پیش ساخته
- ✓ پشتیبانی از انتشار attribute از جمله رضایت کاربر
- ✓ نظارت و پیگیری رفتار برنامه، آمار و لاگ‌های مربوط به آن صورت بلادرنگ^۴
- ✓ مدیریت و ثبت برنامه‌های کاربردی و خدمات مشتری با خط مشی مشخص احراز هویت
- ✓ پشتیبانی از کلاینت‌های مربوط به پلت‌فرم‌های مختلف (Java, .Net, PHP, Perl, Apache)
- ✓ قابلیت یکپارچه‌سازی با InCommon, Box, Office365, ServiceNow, Salesforce, (Workday) WebAdvisor, Drupal, Blackboard, Moodle, Google Apps
- ✓ امکان ارسال اطلاعات به صورت رمز شده با استفاده از Public key مربوط به سامانه مشخص



CAS Management Search Services

Save Changes Cancel

Basics Contacts Logout Access Strategy Expiration Multifactor Authentication Proxy Authentication

Basics

Enable Service ⓘ

Service Type

CAS Client

Service URL *
^https://r[redacted]r/auth/cas-auth ⓘ

Service Name *
UAST user profile ⓘ

Description
Access to UAST user profile with SSO login

Theme ⓘ

Reference Links

Logo URL ⓘ

Information URL ⓘ

تصویر شماره ۲

CAS Management Search Services

Manage Services - default

Name	Service Url	Description
CAS Management	^http://a[redacted]management/manage.html	Allow SSO Access for cas management web application
Local UAST	^http://[redacted]/auth/cas-auth	Redirect from local UAST
UAST user profile	^https://[redacted]/auth/cas-auth	Access to UAST user profile with SSO login
Services Management Web Application	^http://[redacted].8080/cas-management/manage.html	Services Management Web Application
Services Management Web Application	^https://c[redacted].8080/cas-management/manage.html	Services Management Web Application

Items per page: 10 1 - 5 of 5 < >

تصویر شماره ۳



Contacts Logout Access Strategy Expiration Multifactor Authentication

Logout Options

Logout URL ?

Logout Type
BACK_CHANNEL ?

تصویر شماره ۴

Contacts Logout Access Strategy Expiration Multifactor Authentication

Expiration

Expiration Date
1397/09/12 ?

Delete service when expired ?

Notify contacts when service is deleted ?

تصویر شماره ۵

Contacts Logout Access Strategy Expiration Multifactor Authentication

Multifactor Policy

Providers ?

Failure Mode
NOT_SET ?

Principal Attribute Name Trigger ?

Principal Attribute Value To Match ?

Enable Bypass ?

تصویر شماره ۶



Service Access Strategy

Allow Single Sign-On [?] Require All Attributes [?]

Unauthorized Redirect Url [?]

Required Attributes

Name	Value
<input type="checkbox"/> Case Insensitive [?]	<input data-bbox="1029 638 1077 705" type="button" value="+"/>

Type

Select Type

DEFAULT [?]

Rejected Attributes

Name	Value
mbscoAccountStatus	deActive <input type="checkbox"/>

تصویر شماره ۷



Multifactor Authentication Proxy Authentication Username Attribute Attribute Release Properties

Username Options

Default Anonymous Principle Attribute

Username Attribute * ?

Encrypt Username ?
Canonicalization Mode
NONE ▼

تصویر شماره ۸

Attribute Release Policy

Policy
Return Restful ▼

REST Endpoint ?

Attribute Release Options

Exclude default bundle of attributes for release ?
 Authorized to release to credential password ?
 Authorized to release proxy granting ticket ID ?
 Authorized to release authentication attributes ?

Attribute Release Consent

User Consent Enabled ?

Excluded Attributes ▼ ?

Include Only Attributes ▼ ?

تصویر شماره ۹



Attribute Value Filters

Scripted

Script

+

Principal Attribute Repository

Default Cached

ادامه تصویر شماره ۹

Authentication Proxy Authentication Username Attribute Attribute Release Properties

Properties

Name	Value
wsfed.relyingPartyIdentifier	
jwtAsResponse	
jwtAsServiceTicket	
jwtSigningSecret	
jwtSigningSecretAlg	

+

تصویر شماره ۱۰



Multifactor Authentication Proxy Authentication Username Attribute Attribute Release Properties **Advanced**

Advanced

Evaluation Order
-1

Required Handlers

Public Key Options

Location *

Algorithm
RSA

تصویر شماره ۱۱

۴- صفحه ورود کاربران

این سامانه به منظور ورود کاربران و انجام روند احراز هویت آنها است. کاربر با نام کاربری و گذرواژه خود که قبلاً در LDAP ایجاد شده است، یکبار در سیستم احراز هویت می‌شود و سپس با توجه به سرویس‌هایی که در پنل مدیریت تعیین شده‌اند، دیگر نیازی به انجام این رویه برای آن سرویس‌ها نیست. کاربر پس از اتمام کار خود با خروج از این سامانه، تمام نشست‌های مربوط به خود را می‌بندد و عملاً single logout کرده است.

قابلیت‌های این سامانه به شرح زیر است.

- ✓ استفاده از زبان برنامه‌نویسی جاوا و توسعه بصورت MVC بر روی فریم ورک Spring
- ✓ احراز هویت ماژولار از طریق LDAP. Database. X.509 و احراز هویت ۲ فاکتوری
- ✓ پشتیبانی از پروتکل‌های استاندارد SSO شامل CAS. SAML. OAuth. OpenID
- ✓ دارا بودن کتابخانه‌های سمت کلاینت جهت اتصال سایر سامانه‌ها برای زبان‌های برنامه‌نویسی Perl. PHP. .NET. Java و غیره
- ✓ یکپارچگی (Integrate) با نرم‌افزارهای Moodle. BlueSocket. Liferay. Drupal. uPortal
- Google Apps و غیره



- ✓ چند زبانه بودن
- ✓ ارائه وب سرویس با استفاده از پروتکل RESTful
- ✓ دارای اجتماع^۵ قوی کاربری و مستندات کامل و دقیق و بروز

تصویر شماره ۱۲

۵- محل ذخیره کاربران و اطلاعات آنها

این سیستم توانایی اتصال به بانکهای اطلاعاتی مختلف مانند LDAP, RDMS Databases, NOSQL Databases را دارد و می‌تواند از روی آنها اطلاعات کاربران را طبق سیاست‌های سازمان جهت ورود کاربر و استفاده سایر سامانه‌های تحت وب، در اختیار بگیرد. پیشنهاد شرکت متن باز سامان استفاده از سرویس LDAP است که توسط همین شرکت به‌مراه پنل مدیریت و با دقت و کیفیت بالا تولید شده است و طبق نیازمندی مشتری پیاده‌سازی می‌شود.

Community ۵