گزارش در مورد نحوه پیاده سازی LDAP برای SSO – قسمت عملی

تهیه و تنظیم: مبین خیری

شماره دانشجویی: 994421017

استاد راهنما: دکتر میرسامان تاجبخش

چکیده:

در این گزارش‌کار قصد داریم به توصیفِ نحوه‌ی پیاده‌سازیِ تکنولوژیِ LDAP برای سیستم‌های احراز هویت SSO بپردازیم. این گزارش‌کار صرفا به توضیحِ پیچیدگی‌های عملیاتیِ چنین فرآیندی خواهد پرداخت. پیش از این در قسمتِ تئوریِ این گزارش‌کار به طور مفصل به ویژگی‌های مختلفِ تکنولوژی‌هایی از قبیلِ LDAP و SSO پرداختیم.

برای پیاده‌سازیِ این فرآیند ابزارها و زیرساخت‌های فراوانی را می‌توان انتخاب کرد.

جهتِ تفهیمِ بهتر مطلب و نشان دادن کاربردِ عملیِ این سیستم، ما در اینجا استفاده از ابزارِ Metabase را برگزیدیم. در ادامه‌ی این گزارش‌کار به‌طور مفصل به دلایل این انتخاب خواهیم پرداخت.

Metabase چیست؟

متابیس در واقع یک سرویسِ آنلاینِ ارائه‌ی خدمات هوش تجاری است که اغلب مشتریانش را شرکت‌ها و موسساتِ داده‌محور تشکیل می‌دهند.

فرض کنید در شرکتِ کوچک یا استارتاپِ تازه‌تاسیسِ شما چند تیمِ مختلف مشغولِ بررسی داده‌ها و استخراج بینش‌های گوناگون برای گسترش کسب‌وکار فعلی‌تان هستند. به طور مثال تیم فروش یا Sales مشغولِ بررسی میزانِ فروش محصولاتِ مختلف شرکت شما در ماه‌های گذشته است. و یا تیم مارکتینگ و بازاریابی مشغول جمع‌آوریِ دیتا از گروه‌های مختلفِ مشتریانِ شماست. در این صورت یکی از مشکلاتِ متعددی که می‌تواند روند تصمیم‌گیری برای مدیران را چند مرتبه دشوارتر سازد، استناد هر تیم به داده‌های مختلف و توضیحاتِ متنوع برای آن‌هاست.

برای حل این مشکل راه حل‌های گوناگونی وجود دارد که یکی از آن‌ها استفاده از یک پلترم ارائه‌دهنده سرویس‌های هوش تجاری و تحلیل داده است. این سرویس‌ها به شما این امکان را می‌دهند که داده‌های یکسانی را با همه‌ی تیم‌ها به اشتراک گذاشته و نمودارها و تحلیل‌های درون هر گروه را با گروه‌های دیگر مقایسه و تنظیم کنید. ضمن اینکه استفاده از هوش مصنوعی در توسعه‌ی چنین محصولاتی موجب شده که تصمیم‌گیری‌های اقتصادی و فنی، برای اعضای تیم‌ها از پیچیدگی‌های کمتری برخوردار باشند.

فرض کنید تیم شما همین امروز به توافق رسیده که استفاده از چنین سرویس‌هایی را در دستور کار خود قرار دهد. هر کدام از اعضای تیم شما، یک ایمیل رسمی دارد که پیش از این در پروفایلِ آن‌ها در وبسایت شرکت ثبت شده. استفاده از سرویس SSO بر روی وبسایت Metabase می‌تواند به کمک اطلاعاتِ ثبت‌شده در حسابِ Gmail اعضا، مشخصاتِ عمومی افراد را دریافت کرده و برای مهاجرت کارکنان شما به این سیستم زمان زیادی را صرفه‌جویی کند.

همین کار را می‌شد با پیاده‌سازی روی یک سرور شخصی و به کمک هاست‌ها و ابزارآلاتِ Open Source نظیر GitHub و GitLab نیز انجام داد. اما ما در اینجا به دلیلِ کاستن از پیچیدگی‌ها و استفاده‌ی مفیدتر از زمان، تصمیم به استفاده از زیرساخت‌ها آماده و قدرتمندِ سرویس Metabase استفاده کنیم.

در ادامه مراحل مختلف پیاده‌سازیِ این شیوه از احراز هویت را به طور مفصل مرور می‌کنیم. لازم به ذکر است که در آموزش زیر برای تفهیمِ بهتر مطلب، احراز هویت به کمک حساب‌های کاربری Gmail را بررسی کردیم. اما پیاده‌سازیِ همین مطلب برای سرویس‌های دیگر نیز دنبال کردن روند مشابهی را می‌طلبد.

جهت وفاداریِ به متونِ منبعِ اصلی، راهنمایی‌های ذیل به زبان انگلیسی تهیه شده‌اند.

Google Sign-In or LDAP

Enabling Google Sign-In or LDAP for single sign-on (SSO) lets your team log in with a click instead of using email and password. SSO can also be used to let people create Metabase accounts without asking an admin to add each person manually. You can find SSO options under **Settings** > **Admin settings** > **Authentication**.

If you'd like to have people authenticate with SAML or JWT, Metabase's paid plans let you do just that.

As time goes on we may add other auth providers. If you have a service you'd like to see work with Metabase, please let us know by filing an issue.

Enabling Google Sign-In

Google Sign-In is a good option for SSO if:

- Your team is already using Google Workspace, or
- You'd like to use Google's 2-step or multi-factor authentication (2FA or MFA) to secure your Metabase.

Working in the Google developer console

To let your team start signing in with Google you'll first need to create an application through Google's **developer console**.

Next, you'll have to create authorization credentials for your application by following **the instructions from Google here**. Specify the URI of your Metabase instance in the "Authorized JavaScript origins" section. You should leave the "Authorized Redirect URIs" section blank.

Once you have your `Client ID` (ending in `.apps.googleusercontent.com`), click `Configure` on the "Sign in with Google" section of the Authentication page in the Metabase Admin Panel. Paste your `client_id` into the first box.

Now existing Metabase users signed into a Google account that matches their Metabase account email can sign in with just a click.

Creating Metabase accounts with Google Sign-in

If you've added your Google client ID to your Metabase settings, you can also let users sign up on their own without creating accounts for them.

To enable this, go to the Google Sign-In configuration page, and specify the email domain you want to allow. For example, if you work at WidgetCo you could enter "widgetco.com" in the field to let anyone with a company email sign up on their own.

Note that Metabase accounts created with Google Sign-In do not have passwords and must use Google to sign in to Metabase.

Enabling LDAP authentication

In the **Admin** > **Authentication** tab, go to the LDAP section and click **Configure**. Click the toggle at the top of the form to enable LDAP, then fill out the form with the following information about your LDAP server:

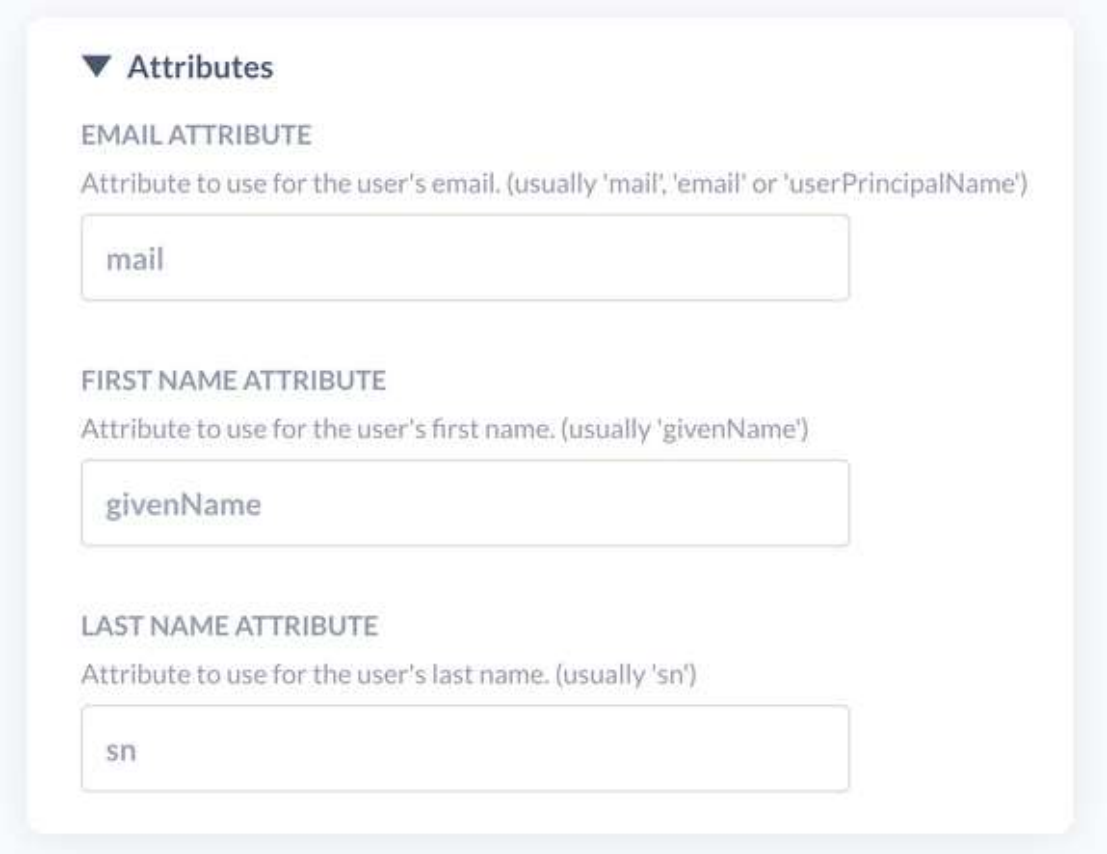
- hostname
- port
- security settings
- LDAP admin username
- LDAP admin password

Then save your changes.

Metabase will pull out three main attributes from your LDAP directory:

- email (defaulting to the `mail` attribute)
- first name (defaulting to the `givenName` attribute)
- last name (defaulting to the `sn` attribute).

If your LDAP setup uses other attributes for these, you can edit this under the "Attributes" portion of the form.



Your LDAP directory must have the email field populated for each entry that will become a Metabase user, otherwise Metabase won't be able to create the account, nor will that person be able to log in. If either name field is missing, Metabase will use a default of "Unknown," and the person can change their name in their account settings.

LDAP user schema

The **User Schema** section on this same page is where you can adjust settings related to where and how Metabase connects to your LDAP server to authenticate users.

The **User search base** field should be completed with the *distinguished name* (DN) of the entry in your LDAP server that is the starting point when searching for users.

For example, let's say you're configuring LDAP for your company, WidgetCo, where your base DN is `dc=widgetco,dc=com`. If entries for employees are all stored within an organizational unit in your LDAP server named `People`, you'll want to supply the user search base field with the DN `ou=People,dc=widgetco,dc=com`. This tells Metabase to begin searching for matching entries at that location within the LDAP server.

You'll see the following grayed-out default value in the **User filter** field:

```
(&(objectClass=inetOrgPerson)(|(uid={login})(mail={login})))
```

When a person logs into Metabase, this command confirms that the login they supplied matches either a UID *or* email field in your LDAP server, *and* that the matching entry has an objectClass of `inetOrgPerson`.

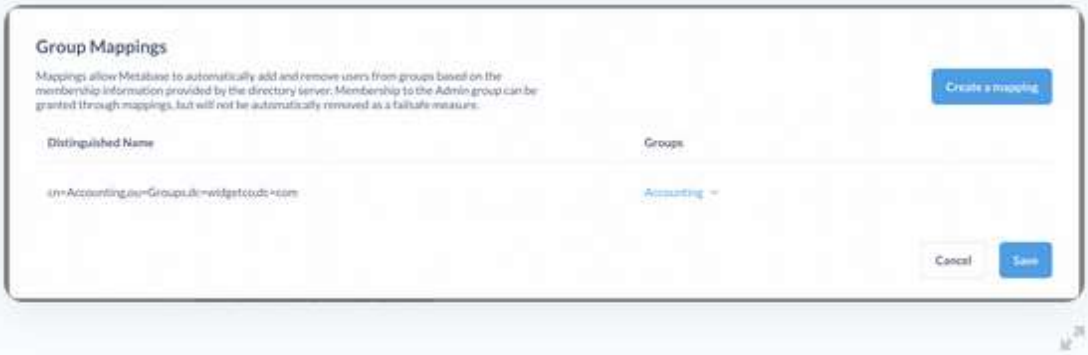
This default command will work for most LDAP servers, since `inetOrgPerson` is a widely-adopted objectClass. But if your company for example uses a different objectClass to categorize employees, this field is where you can set a different command for how Metabase finds and authenticates an LDAP entry upon a person logging in.

LDAP group mapping

Manually assigning people to groups in Metabase after they've logged in via SSO can get tedious. Instead, you can take advantage of the groups that already exist in your LDAP directory by enabling group mappings.

Scroll to **Group Schema** on the same LDAP settings page, and click the toggle to enable group mapping. Selecting **Edit Mapping** will bring up a modal where you can create and edit mappings, specifying which LDAP group corresponds to which Metabase group.

As you can see below, if you have an **Accounting** group in both your LDAP server and Metabase instance, you'll just need to supply the Distinguished Name from your LDAP server (in the example, it's `cn=Accounting,ou=Groups,dc=widgetco,dc=com`) and select its match from the dropdown of your existing Metabase groups.



Notes on group mapping

- The Administrator group works like any other group.
- Updates to a person's group membership based on LDAP mappings are not instantaneous; the changes will take effect only after people log back in.
- People are only ever added to or removed from mapped groups; the sync has no effect on groups in your Metabase that don't have an LDAP mapping.

LDAP group membership filter

> LDAP advanced features is only available on **Pro** and **Enterprise** plans (both self-hosted and on Metabase Cloud).

Group membership lookup filter. The placeholders {dn} and {uid} will be replaced by the user's Distinguished Name and UID, respectively.

Syncing user attributes at login

> Advanced authentication features is only available on **Pro** and **Enterprise** plans (both self-hosted and on Metabase Cloud).

Syncing user attributes with LDAP

You can manage **user attributes** such as names, emails, and roles from your LDAP directory. When you set up **data sandboxing**, your LDAP directory will be able to **pass these attributes** to Metabase.

Syncing user attributes with Google

User attributes can't be synced with regular Google Sign-In. You'll need to set up **Google SAML** or **JWT** instead.

Changing an account's login method from email to SSO

Once a person creates an account, you cannot change the authentication method for that account. However, you can:

- Deactivate password authentication for all users from **Admin settings** > **Authentication**. You'll need to ask people to sign in with Google (if they haven't already).
- Manually update the account's login method in the Metabase application database. This option is not recommended unless you're familiar with making changes to the application database.

Note that you must have at least one account with email and password login. This account safeguards you from getting locked out of your Metabase if there are any problems with your SSO provider.

پایان.