LDAP Authentication

 › [Administration](https://grafana.com/docs/grafana/latest/administration/) › [Authentication](https://grafana.com/docs/grafana/latest/auth/) › LDAP

The LDAP integration in Grafana allows your Grafana users to login with their LDAP credentials. You can also specify mappings between LDAP group memberships and Grafana Organization user roles.

在Grafana中的LDAP集成允许你的Grafana的用户使用他们的LDAP证书去登录。你也可以在LDAP组关系和Grafana组织用户角色之间指定映射。

[Enhanced LDAP authentication](https://grafana.com/docs/grafana/latest/enterprise/enhanced_ldap/) is available in [Grafana Enterprise](https://grafana.com/docs/grafana/latest/enterprise/).

增强版的LDAP认证在Grafana企业版中可用。

Supported LDAP Servers

支持LDAP的服务

Grafana uses a [third-party LDAP library](https://github.com/go-ldap/ldap) under the hood that supports basic LDAP v3 functionality. This means that you should be able to configure LDAP integration using any compliant LDAPv3 server, for example [OpenLDAP](https://grafana.com/docs/grafana/latest/auth/ldap/" \l "openldap) or [Active Directory](https://grafana.com/docs/grafana/latest/auth/ldap/#active-directory) among [others](https://en.wikipedia.org/wiki/Directory_service#LDAP_implementations).

Grafana在底层使用了一个支持基本LDAP v3功能的第三方LDAP库。这意味着你可以使用任何兼容的LDAPv3去配置LDAP集成，例子有OpenLDAP或Active Directory或Others。

Enable LDAP

In order to use LDAP integration you’ll first need to enable LDAP in the [main config file](https://grafana.com/docs/grafana/latest/administration/configuration/) as well as specify the path to the LDAP specific configuration file (default: /etc/grafana/ldap.toml).

为了去使用LDAP集成，你需要先在主配置文件中启用LDAP，指定LDAP配置文件的路径（默认为:/etc/grafana/ldap.toml）

[auth.ldap]

# Set to `true` to enable LDAP integration (default: `false`)

enabled = true

# Path to the LDAP specific configuration file (default: `/etc/grafana/ldap.toml`)

config\_file = /etc/grafana/ldap.toml

# Allow sign up should almost always be true (default) to allow new Grafana users to be created (if LDAP authentication is ok). If set to

# false only pre-existing Grafana users will be able to login (if LDAP authentication is ok).

allow\_sign\_up = true

Bash

Grafana LDAP Configuration

Depending on which LDAP server you’re using and how that’s configured your Grafana LDAP configuration may vary. See [configuration examples](https://grafana.com/docs/grafana/latest/auth/ldap/#configuration-examples) for more information.

根据你使用的LDAP服务，然后配置相应的Grafana的LDAP配置。查看配置例子来查看更多信息。

**LDAP specific configuration file (ldap.toml) example:**

**LDAP详细配置文件（ldap.toml）例子：**

[[servers]]

# Ldap server host (specify multiple hosts space separated)

# LDAP服务主机（使用空格分隔可指定多个主机）

host = "127.0.0.1"

# Default port is 389 or 636 if use\_ssl = true

# 默认端口为389，如果use\_ssl=true的话为636

port = 389

# Set to true if LDAP server supports TLS

# 如要LDAP服务支持TLS的话设置为true

use\_ssl = false

# Set to true if connect LDAP server with STARTTLS pattern (create connection in insecure, then upgrade to secure connection with TLS)

# 如果使用STARTTLS模式连接LDAP的话设置为true(创建非安全性连接，那么升级到使用TLS的安全连接)

start\_tls = false

# set to true if you want to skip SSL cert validation

# 如果你想要跳过SSL证书检验的话设置为true

ssl\_skip\_verify = false

# set to the path to your root CA certificate or leave unset to use system defaults

# 设置你的CA证书的路径，或者使用系统默认的

# root\_ca\_cert = "/path/to/certificate.crt"

# Authentication against LDAP servers requiring client certificates

# 针对需要客户端证书的LDAP服务器进行身份验证

# client\_cert = "/path/to/client.crt"

# client\_key = "/path/to/client.key"

# Search user bind dn

# 搜索用户绑定可识别名

bind\_dn = "cn=admin,dc=grafana,dc=org"

# Search user bind password

# 搜索用户绑定密码

# If the password contains # or ; you have to wrap it with triple quotes. Ex """#password;"""

# 如果密码中包含了 # 或者 ；你应该使用三引号括起来。例如"""#password;"""

bind\_password = 'grafana'

# User search filter, for example "(cn=%s)" or "(sAMAccountName=%s)" or "(uid=%s)"

# 使用搜索过滤，例如"(cn=%s)"或"(sAMAccountName=%s)"或"(uid=%s)"

# Allow login from email or username, example "(|(sAMAccountName=%s)(userPrincipalName=%s))"

# 允许从邮箱或用户名登录，例如"(|(sAMAccountName=%s)(userPrincipalName=%s))"

search\_filter = "(cn=%s)"

# An array of base dns to search through

# 以dns为基础用于搜索的数组

search\_base\_dns = ["dc=grafana,dc=org"]

# group\_search\_filter = "(&(objectClass=posixGroup)(memberUid=%s))"

# group\_search\_filter\_user\_attribute = "distinguishedName"

# group\_search\_base\_dns = ["ou=groups,dc=grafana,dc=org"]

# Specify names of the LDAP attributes your LDAP uses

# 指定LDAP属性的名字为你使用的LADP

[servers.attributes]

name = "givenName"

surname = "sn"

username = "cn"

member\_of = "memberOf"

email = "email"

Bash

Using environment variables

使用环境变量

You can interpolate variables in the TOML config from environment variables. For instance, you could externalize your bind\_password that way:

你可以从环境变量中插入变量到TOML配置中。例如，你可以将你的bind\_password外部化：

bind\_password = "${LDAP\_ADMIN\_PASSWORD}"

Bash

LDAP Debug View

LDAP的调试视图

Only available in Grafana v6.4+

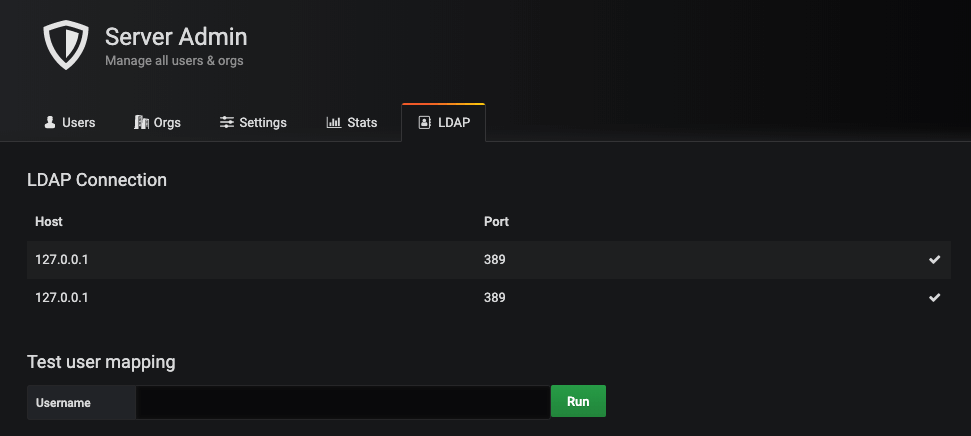
只在Grafana6.4版本之后可用

Grafana has an LDAP debug view built-in which allows you to test your LDAP configuration directly within Grafana. At the moment of writing, only Grafana admins can use the LDAP debug view.

Grafana有一个LDAP的内置调试视图，允许你直接在Grafana中去测试你的LDAP配置。目前为止，只有Grafana的管理者能够使用LDAP调试视图。

Within this view, you’ll be able to see which LDAP servers are currently reachable and test your current configuration.

在这个视图中，你能够看到可用的LDAP服务，并测试你当前的配置。

[](https://grafana.com/static/img/docs/ldap_debug.png)

[](https://grafana.com/static/img/docs/ldap_debug.png)

To use the debug view:

去使用调试视图：

1. Type the username of a user that exists within any of your LDAP server(s)

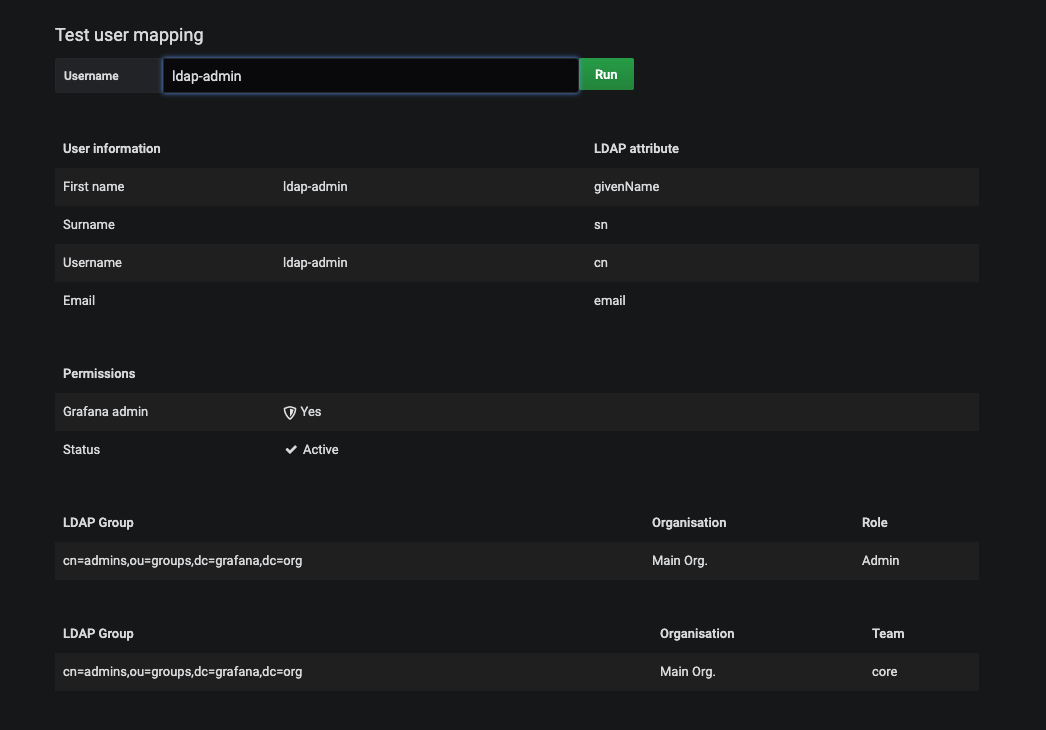
输入任何在你LDAP服务中存在的一个用户的用户名

1. Then, press “Run”

然后点“Run”

1. If the user is found within any of your LDAP instances, the mapping information is displayed

如果发现用户存在于你的LDAP中，那么会映射出相应的信息。

[](https://grafana.com/static/img/docs/ldap_debug_mapping_testing.png)

[](https://grafana.com/static/img/docs/ldap_debug_mapping_testing.png)

Bind

绑定

Bind and Bind Password

绑定和绑定密码

By default the configuration expects you to specify a bind DN and bind password. This should be a read only user that can perform LDAP searches. When the user DN is found a second bind is performed with the user provided username and password (in the normal Grafana login form).

默认配置期望你去指定一个绑定的DN和密码。这应该是一个可以执行LDAP搜索的只读用户。当找到用户DN时，使用用户提供的用户名和密码执行第二次绑定（在正常的Grafana登录表单中）

bind\_dn = "cn=admin,dc=grafana,dc=org"

bind\_password = "grafana"

Bash

Single Bind Example

单个绑定例子

If you can provide a single bind expression that matches all possible users, you can skip the second bind and bind against the user DN directly. This allows you to not specify a bind\_password in the configuration file.

如果你能提供一个能匹配所有可能用户的绑定表达式，你可以跳过第二次绑定，直接使用DN绑定用户。这样允许你不在配置文件中指定bind\_password。

bind\_dn = "cn=%s,o=users,dc=grafana,dc=org"

Bash

In this case you skip providing a bind\_password and instead provide a bind\_dn value with a %s somewhere. This will be replaced with the username entered in on the Grafana login page. The search filter and search bases settings are still needed to perform the LDAP search to retrieve the other LDAP information (like LDAP groups and email).

在这个例子中，你可以不提供bind\_password，并使用s%来代替bind\_dn的值。这个会代替为在Grafana登录页面中输入的用户名。搜索过滤和搜索基础设置还需要去执行LDAP搜索，去检索其他的LDAP信息（比如LDAP组和邮箱）

POSIX schema

POSIX模式

If your LDAP server does not support the memberOf attribute add these options:

如果你的LDAP服务器不支持memberOf属性，请添加以下选项:：

## Group search filter, to retrieve the groups of which the user is a member (only set if memberOf attribute is not available)

## 组搜索过滤，检索用户所属的组（只有memberOf属性不可用时设置）

group\_search\_filter = "(&(objectClass=posixGroup)(memberUid=%s))"

## An array of the base DNs to search through for groups. Typically uses ou=groups

## 基于DN的数组去搜索组。通常用于ou=groups

group\_search\_base\_dns = ["ou=groups,dc=grafana,dc=org"]

## the %s in the search filter will be replaced with the attribute defined below

## 在搜索过滤中的s%被会下面的属性定义所代替

group\_search\_filter\_user\_attribute = "uid"

Bash

Group Mappings

组映射

In [[servers.group\_mappings]] you can map an LDAP group to a Grafana organization and role. These will be synced every time the user logs in, with LDAP being the authoritative source. So, if you change a user’s role in the Grafana Org. Users page, this change will be reset the next time the user logs in. If you change the LDAP groups of a user, the change will take effect the next time the user logs in.

在[[servers.group\_mappings]]中你可以映射一个LDAP组到Grafana的团队和角色。它们每次会在用户登录的时候，使用LDAP作为认证源来同步。所以，如果你在Grafana团队用户页面修改了用户的角色，这次修改会在用户下次登录的时候更新。

The first group mapping that an LDAP user is matched to will be used for the sync. If you have LDAP users that fit multiple mappings, the topmost mapping in the TOML config will be used.

LDAP用户第一个被匹配的组映射会被用于同步。如果你的LDAP用户匹配到了多个映射，在TOML配置中最上面的一个映射会被使用。

**LDAP specific configuration file (ldap.toml) example:**

**LDAP详细的配置文件（ldap.toml）例子：**

[[servers]]

# other settings omitted for clarity

# 这里省略了其他的设置

[[servers.group\_mappings]]

group\_dn = "cn=superadmins,dc=grafana,dc=org"

org\_role = "Admin"

grafana\_admin = true # Available in Grafana v5.3 and above 只在Grafana5.3及以后版本可用

[[servers.group\_mappings]]

group\_dn = "cn=admins,dc=grafana,dc=org"

org\_role = "Admin"

[[servers.group\_mappings]]

group\_dn = "cn=users,dc=grafana,dc=org"

org\_role = "Editor"

[[servers.group\_mappings]]

group\_dn = "\*"

org\_role = "Viewer"

Bash

| Setting | Required | Description | Default |
| --- | --- | --- | --- |
| group\_dn | Yes | LDAP distinguished name (DN) of LDAP group. If you want to match all (or no LDAP groups) then you can use wildcard ("\*")  LDAP组的可识别名（DN）。如果你想要匹配所有的（或不是LDAP组），那么你应该使用通配符（“\*”） |  |
| org\_role | Yes | Assign users of group\_dn the organization role "Admin", "Editor" or "Viewer"  分配group\_dn用户在组织中的角色："Admin", "Editor"或"Viewer" |  |
| org\_id | No | The Grafana organization database id. Setting this allows for multiple group\_dn’s to be assigned to the same org\_role provided the org\_id differs  Grafana组织的数据库ID。设置这个选项允许多个group\_dn能够被分配到同一个org\_role，但是org\_id是不同的 | 1 (default org id) |
| grafana\_admin | No | When true makes user of group\_dn Grafana server admin. A Grafana server admin has admin access over all organizations and users. Available in Grafana v5.3 and above  如果为true，那么group\_dn的用户会被作为服务的管理者。Grafana服务管理者有组织和用户的所有权限。在Grafana5.3及以后的版本可用。 | false |

Nested/recursive group membership

嵌套/递归的组关系

Users with nested/recursive group membership must have an LDAP server that supports LDAP\_MATCHING\_RULE\_IN\_CHAIN and configure group\_search\_filter in a way that it returns the groups the submitted username is a member of.

要使用嵌套/递归的组关系，必须在LDAP服务中支持LDAP\_MATCHING\_RULE\_IN\_CHAIN并配置group\_search\_filter，然后会返回已提交用户名的组。

To configure group\_search\_filter:

去配置group\_search\_filter:

* You can set group\_search\_base\_dns to specify where the matching groups are defined.

你可以设置group\_search\_base\_dns去指定定义匹配组的位置。

* If you do not use group\_search\_base\_dns, then the previously defined search\_base\_dns is used.

如果你不使用group\_search\_base\_dns，那么会使用上一个定义的search\_base\_dns。

**Active Directory example:**

**动态目录例子：**

Active Directory groups store the Distinguished Names (DNs) of members, so your filter will need to know the DN for the user based only on the submitted username. Multiple DN templates can be searched by combining filters with the LDAP OR-operator. Two examples:

动态目录组存储着成员的可识别名（DN），基于已提交的用户，你的过滤需要知道它的DN。使用LDAP OR-operator可以通过组合过滤来搜索多个DN模板。两个例子如下：

group\_search\_filter = "(member:1.2.840.113556.1.4.1941:=%s)"

group\_search\_base\_dns = ["DC=mycorp,DC=mytld"]

group\_search\_filter\_user\_attribute = "dn"

Bash

group\_search\_filter = "(member:1.2.840.113556.1.4.1941:=CN=%s,[user container/OU])"

group\_search\_filter = "(|(member:1.2.840.113556.1.4.1941:=CN=%s,[user container/OU])(member:1.2.840.113556.1.4.1941:=CN=%s,[another user container/OU]))"

group\_search\_filter\_user\_attribute = "cn"

Bash

For more information on AD searches see [Microsoft’s Search Filter Syntax](https://docs.microsoft.com/en-us/windows/desktop/adsi/search-filter-syntax) documentation.

想要了解更多关于AD搜索的信息，可以查看[Microsoft’s Search Filter Syntax](https://docs.microsoft.com/en-us/windows/desktop/adsi/search-filter-syntax)文档。

For troubleshooting, by changing member\_of in [servers.attributes] to “dn” it will show you more accurate group memberships when [debug is enabled](https://grafana.com/docs/grafana/latest/auth/ldap/#troubleshooting).

为了排除故障，通过修改[servers.attributes]中的member\_of为dn，当调试启用时，它会显示出来更精确的组关系信息。

Configuration examples

配置例子

OpenLDAP

[OpenLDAP](http://www.openldap.org/) is an open source directory service.

OpenLDAP是一个开源的目录服务。

**LDAP specific configuration file (ldap.toml):**

**LDAP详细的配置文件（ldap.toml）：**

[[servers]]

host = "127.0.0.1"

port = 389

use\_ssl = false

start\_tls = false

ssl\_skip\_verify = false

bind\_dn = "cn=admin,dc=grafana,dc=org"

bind\_password = 'grafana'

search\_filter = "(cn=%s)"

search\_base\_dns = ["dc=grafana,dc=org"]

[servers.attributes]

name = "givenName"

surname = "sn"

username = "cn"

member\_of = "memberOf"

email = "email"

# [[servers.group\_mappings]] omitted for clarity

Bash

Multiple LDAP servers

多个LDAP服务

Grafana does support receiving information from multiple LDAP servers.

Grafana不支持从多个LDAP服务中接受信息。

**LDAP specific configuration file (ldap.toml):**

**LDAP详细的配置文件（ldap.toml）：**

# --- First LDAP Server ---

[[servers]]

host = "10.0.0.1"

port = 389

use\_ssl = false

start\_tls = false

ssl\_skip\_verify = false

bind\_dn = "cn=admin,dc=grafana,dc=org"

bind\_password = 'grafana'

search\_filter = "(cn=%s)"

search\_base\_dns = ["ou=users,dc=grafana,dc=org"]

[servers.attributes]

name = "givenName"

surname = "sn"

username = "cn"

member\_of = "memberOf"

email = "email"

[[servers.group\_mappings]]

group\_dn = "cn=admins,ou=groups,dc=grafana,dc=org"

org\_role = "Admin"

grafana\_admin = true

# --- Second LDAP Server ---

[[servers]]

host = "10.0.0.2"

port = 389

use\_ssl = false

start\_tls = false

ssl\_skip\_verify = false

bind\_dn = "cn=admin,dc=grafana,dc=org"

bind\_password = 'grafana'

search\_filter = "(cn=%s)"

search\_base\_dns = ["ou=users,dc=grafana,dc=org"]

[servers.attributes]

name = "givenName"

surname = "sn"

username = "cn"

member\_of = "memberOf"

email = "email"

[[servers.group\_mappings]]

group\_dn = "cn=editors,ou=groups,dc=grafana,dc=org"

org\_role = "Editor"

[[servers.group\_mappings]]

group\_dn = "\*"

org\_role = "Viewer"

Bash

Active Directory

动态目录

[Active Directory](https://technet.microsoft.com/en-us/library/hh831484(v=ws.11).aspx) is a directory service which is commonly used in Windows environments.

动态目录是一个目录服务，普遍在Windows环境中使用。

Assuming the following Active Directory server setup:

假定下面是动态目录服务设置：

* IP address: 10.0.0.1
* Domain: CORP
* DNS name: corp.local

**LDAP specific configuration file (ldap.toml):**

LDAP详细配置文件（ldap.toml）：

[[servers]]

host = "10.0.0.1"

port = 3269

use\_ssl = true

start\_tls = false

ssl\_skip\_verify = true

bind\_dn = "CORP\\%s"

search\_filter = "(sAMAccountName=%s)"

search\_base\_dns = ["dc=corp,dc=local"]

[servers.attributes]

name = "givenName"

surname = "sn"

username = "sAMAccountName"

member\_of = "memberOf"

email = "mail"

# [[servers.group\_mappings]] omitted for clarity

Bash

Port requirements

端口要求

In above example SSL is enabled and an encrypted port have been configured. If your Active Directory don’t support SSL please change enable\_ssl = false and port = 389. Please inspect your Active Directory configuration and documentation to find the correct settings. For more information about Active Directory and port requirements see [link](https://technet.microsoft.com/en-us/library/dd772723(v=ws.10)).

在上面的例子中启用了SSL并配置了一个加密端口。如果你的动态目录不支持SSL，请做以下的修改：enable\_ssl=false和port=389。

Troubleshooting

排除故障

To troubleshoot and get more log info enable LDAP debug logging in the [main config file](https://grafana.com/docs/grafana/latest/administration/configuration/).

为了排队故障并获取更多日志信息，在主配置文件中起用LDAP调试记录。

[log]

filters = ldap:debug