



# casbin<sup>★</sup>社区线上宣讲会

主办单位：



# 项目简介

- Casbin: 开源的统一访问控制（权限管理）框架库

- 领域: 网络安全


- 支持多种访问控制模型:

- 访问控制列表（ACL）
- 基于角色的访问控制（RBAC）
- 基于属性的访问控制（ABAC）


- 适用场景

- 网站后台管理界面: 角色管理、权限管理
- RESTful、GraphQL等API网关、微服务的访问控制
- 云计算、大数据系统的管理平面（Control Plane）的访问控制

- 支持八种语言，涵盖市面上主流服务器端语言

 Go	 Java	 node	 php
Casbin	jCasbin	node-Casbin	PHP-Casbin
production-ready	production-ready	production-ready	production-ready

 python™	 Microsoft® .NET	 PASCAL	 Rust
PyCasbin	Casbin.NET	Casbin4D	Casbin-RS
production-ready	production-ready	experimental	production-ready

## ■ Go、Java: hsluoyz

- 2019 Q3谷歌开源贡献奖获得者, 前GSoC学生, Casbin、Npcap作者, Nmap开源社区成员
- 北京大学工学博士, 《计算机学报》审稿人, CCF会员, 发表计算机相关学术论文27篇(一作14篇)

## ■ 核心成员

- nodece (Node.js)
- techone (Python, PHP)
- GopherJ (Rust)
- huazhikui (.NET)
- Joey (C++)
- John Kouraklis (Delphi)
- BetaCat0 (React)
- ...

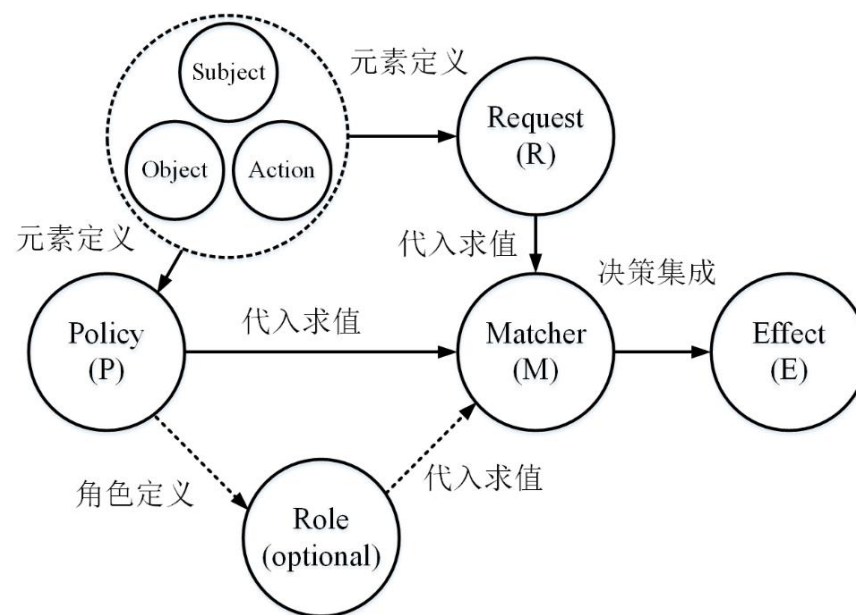
## ■ Casbin的主要特性包括：

- 支持自定义请求的格式，默认的请求格式为 {subject, object, action}；
- 具有访问控制模型（Model）和策略规则（Policy）两个核心概念；
- 支持RBAC中的多层角色继承，不止主体可以有角色，资源也可以具有角色；
- 支持超级用户，如root或Administrator，超级用户可以不受授权策略的约束访问任意资源；
- 支持多种内置辅助函数，如keyMatch，方便对路径式的资源进行管理，如 /foo/bar 可以映射到 /foo\*，ipMatch则可以对IP地址合规情况进行校验。

## ■ Casbin不做的事情：

- 身份认证（即Authentication，验证用户的用户名、密码），Casbin只负责访问控制。应该有其他专门的组件负责身份认证，然后由Casbin进行访问控制，二者是相互配合的关系；
- 管理用户表或角色表。Casbin认为由项目自身来管理用户、角色表更为合适，Casbin假设所有策略和请求中出现的用户、角色、资源都是合法有效的。

## PERM模型



- PERM模型：基于策略、效果、请求、匹配器

Policy Effect Request Matcher

- 与ACL、BLP、RBAC、ABAC等模型相比，具有较强的表达能力

# 原语含义

- Request原语：表示请求
  - 例子：r = sub, obj, act
- Policy原语：表示策略
  - 例子：p = sub, obj, act
- Matcher原语：请求与策略之间的匹配逻辑
  - 例子：m = r.sub == p.sub && r.obj == p.obj && r.act == p.act
- Effect原语：表达决策集成的效果
  - 例子：e = some(where (p.eft == allow))

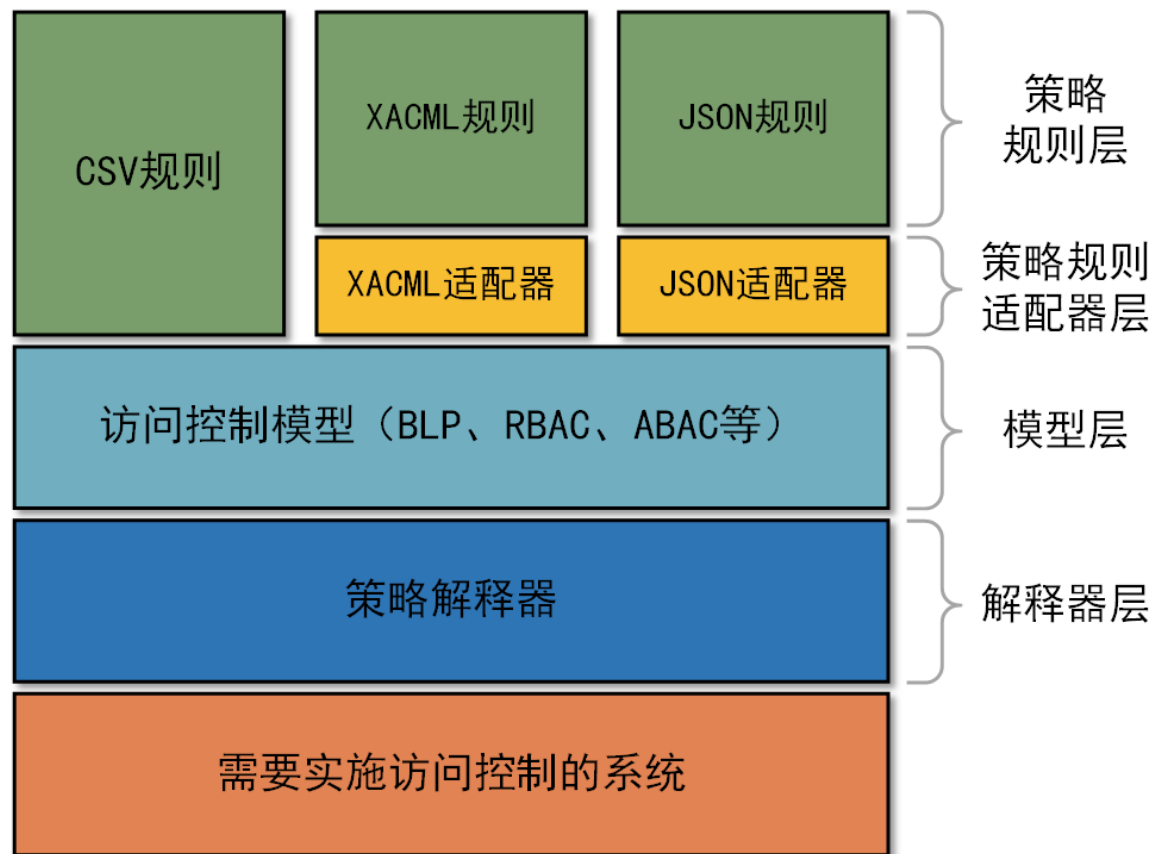
```
1 [request_definition]
2 r = sub, obj, act
3
4 [policy_definition]
5 p = sub, obj, act
6
7 [role_definition]
8 g = _, _
9
10 [policy_effect]
11 e = some(where (p.eft == allow))
12
13 [matchers]
14 m = g(r.sub, p.sub) && r.obj == p.obj && r.act == p.act
```

```
1 p, alice, data1, read
2 p, bob, data2, write
3 p, data2_admin, data2, read
4 p, data2_admin, data2, write
5
6 g, alice, data2_admin
```

- 
- Role原语：表达RBAC角色之间的继承关系
    - 例子：g = \_, \_
    - m = g(r.sub, p.sub) && r.obj == p.obj && r.act == p.act
  - 属性原语：表达属性
    - 例子：m = r.sub.domain == r.obj.domain

# PERM模型解析流程

- Casbin采用基于解释器的设计思想，**将PERM模型语句看作脚本语言进行动态解析**，从而大大增强了模型表达的灵活性。



## ■ 为什么实现插件机制？

- Go是一种静态编译语言，所有直接依赖都必须以源代码形式编译到可执行文件中。为了防止Casbin下游项目代码过于膨胀，Casbin主库只保留核心功能，而将扩展的功能以插件的形式提供，通过依赖注入实现插件的动态调用。

## ■ Casbin插件包含以下几种类型：

- **策略存储插件（Adapter）**：将Casbin策略规则存储到何种数据库中，包括ORM, NoSQL, KV, AWS S3等22个插件；
- **策略同步插件（Watcher）**：当Casbin采用分布式部署时，不同节点的Casbin策略之间如何同步，包括etcd, ZooKeeper, Redis等5个插件；
- **角色管理插件（Role Manager）**：RBAC模型中的角色继承关系如何存储，包括Okta, Auth0等4个插件。



# 策略存储插件 (Adapter)

Go	Java	Node.js	PHP	Python	.NET	Rust
Adapter	Type	Author	AutoSave	Description		
File Adapter (built-in)	File	Casbin	✗	For .CSV (Comma-Separated Values) files		
Filtered File Adapter (built-in)	File	@faceless-saint	✗	For .CSV (Comma-Separated Values) files with policy subset loading support		
Xorm Adapter	ORM	Casbin	✓	MySQL, PostgreSQL, TiDB, SQLite, SQL Server, Oracle are supported by Xorm		
Gorm Adapter	ORM	Casbin	✓	MySQL, PostgreSQL, SQLite3, SQL Server are supported by Gorm		
Beego ORM Adapter	ORM	Casbin	✓	MySQL, PostgreSQL, SQLite3 are supported by Beego ORM		
SQLX Adapter	ORM	@memwey	✓	MySQL, PostgreSQL, SQLite, Oracle are supported by SQLX		
GF ORM Adapter	ORM	@vance-liu	✓	MySQL, SQLite, PostgreSQL, Oracle, SQL Server are supported by GF ORM		
Filtered PostgreSQL Adapter	SQL	Casbin	✓	For PostgreSQL		
PostgreSQL Adapter	SQL	@cychiuae	✓	For PostgreSQL		

<https://casbin.org/docs/en/adapters>

PostgreSQL Adapter (Archived)	SQL	Going	✗	For PostgreSQL
RQLite Adapter	SQL	EDOMO Systems	✓	For RQLite
MongoDB Adapter	NoSQL	Casbin	✓	For MongoDB based on MongoDB driver for Go
MongoDB Adapter	NoSQL	Titan DC	✓	For MongoDB based on MongoDB Go driver
RethinkDB Adapter	NoSQL	@adityapandey9	✓	For RethinkDB
Cassandra Adapter	NoSQL	Casbin	✗	For Apache Cassandra DB
DynamoDB Adapter	NoSQL	HOOQ	✗	For Amazon DynamoDB
Dynacasbin	NoSQL	NewbMiao	✓	For Amazon DynamoDB
ArangoDB Adapter	NoSQL	@adamwasila	✓	For ArangoDB
Amazon S3 Adapter	Cloud	Soluto	✗	For Minio and Amazon S3
Azure Cosmos DB Adapter	Cloud	@spacycoder	✓	For Microsoft Azure Cosmos DB
GCP Datastore Adapter	Cloud	LivingPackets	✗	For Google Cloud Platform Datastore
Consul Adapter	KV store	@ankitm123	✗	For HashiCorp Consul
Redis Adapter	KV store	Casbin	✗	For Redis
Etcd Adapter	KV store	@sebastianliu	✗	For etcd
Bolt Adapter	KV store	@wirepair	✗	For Bolt
Protobuf Adapter	Stream	Casbin	✗	For Google Protocol Buffers
JSON Adapter	String	Casbin	✗	For JSON
String Adapter	String	@qiangmzxs	✗	For String

# 策略同步插件（Watcher）

Watcher	Type	Author	Description
<a href="#">Etcd Watcher</a>	KV store	Casbin	Watcher for <a href="#">etcd</a>
<a href="#">NATS Watcher</a>	Messaging system	<a href="#">Solutio</a>	Watcher for <a href="#">NATS</a>
<a href="#">ZooKeeper Watcher</a>	KV store	<a href="#">GrepSr</a>	Watcher for <a href="#">Apache ZooKeeper</a>
<a href="#">Redis Watcher</a>	KV store	<a href="#">@billcobbler</a>	Watcher for <a href="#">Redis</a>
<a href="#">GCP Pub/Sub Watcher</a>	Messaging system	<a href="#">LivingPackets</a>	Watcher for <a href="#">Google Cloud Platform PUB/SUB</a>
<a href="#">NATS, RabbitMQ, GCP Pub/Sub, AWS SNS &amp; SQS, Kafka, InMemory</a>	Messaging System	<a href="#">rusenask</a>	Watcher based on <a href="#">Go Cloud Dev Kit</a> that works with leading cloud providers and self-hosted infrastructure

<https://casbin.org/docs/en/watchers>

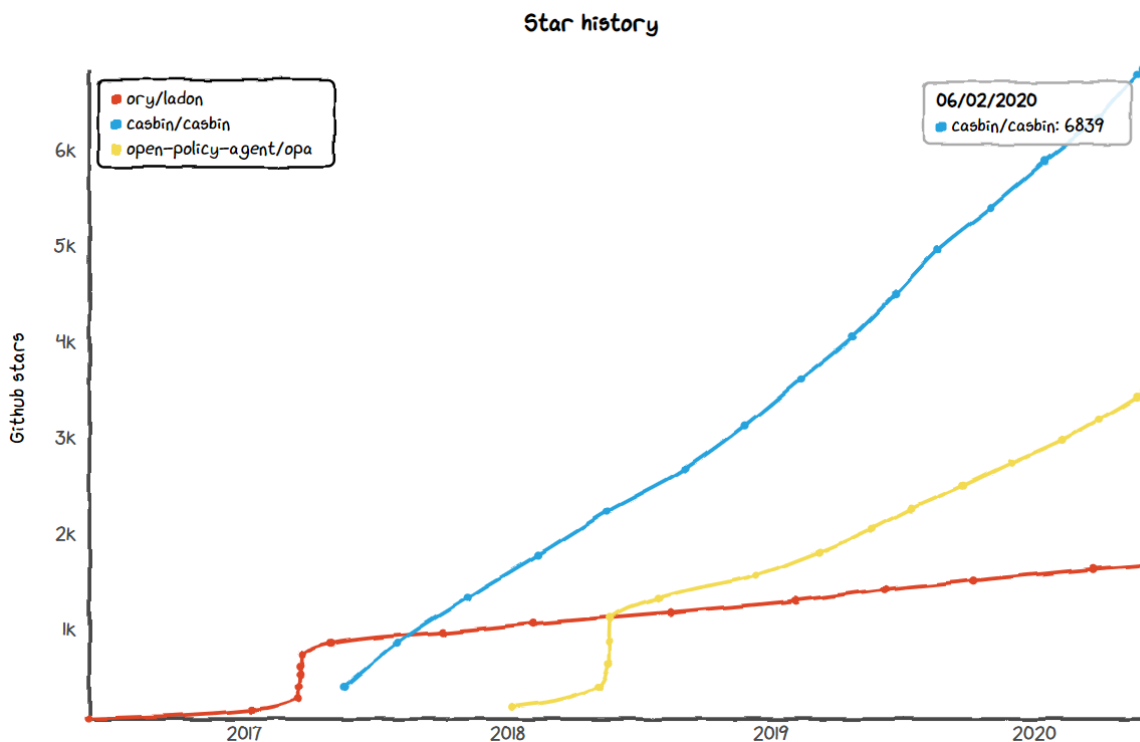
# 角色管理插件（Role Manager）

Role manager	Author	Description
Default Role Manager (built-in)	Casbin	Supports role hierarchy stored in Casbin policy
Session Role Manager	EDOMO Systems	Supports role hierarchy stored in Casbin policy, with time-range-based sessions
Okta Role Manager	Casbin	Supports role hierarchy stored in <a href="#">Okta</a>
Auth0 Role Manager	Casbin	Supports role hierarchy stored in <a href="#">Auth0's Authorization Extension</a>

<https://casbin.org/docs/en/role-managers>

# 项目成长性

- 启动时间：04/25/2017
- Star个数（与OPA、Ladon项目对比）：



☆ Casbin	6,840	☆ jCasbin	1,044
☆ Node-Casbin	992	☆ PHP-Casbin	677
☆ PyCasbin	438	☆ Casbin.NET	282
☆ Casbin4D	16	☆ Casbin-RS	191


数据来自于：<https://star-history.t9t.io/#casbin/casbin&open-policy-agent/opa&ory/ladon>

# 代码贡献情况

- 共55位Contributor，其中国际人士占相当大比例
- 贡献方式：Pull Request



# 项目应用情况

- 在200+个开源项目获得应用，知名的有：
  - Intel的RMD项目：Intel公司的资源管理服务，用来管理Intel CPU相关的硬件资源；
  - VMware的Dispatch项目：部署Serverless服务的应用框架平台；
  - 腾讯的TKE项目：腾讯云容器服务TKE。



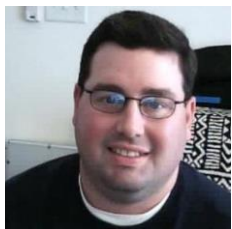
<https://casbin.org/en/users>

- \*在闭源项目中的应用无法直接统计，据了解有Cisco、Verizon、小米、趣头条等在生产环境中采用。



# 来自Cisco（思科）的感谢信

- Cisco美国总部的工程师Kenny Jones对Casbin作出如下评价：



- Casbin在Cisco云基础架构平台服务（Cloud Infrastructure and Platform Services, CIPS）中被应用，CIPS为思科公私有云提供provision和billing服务；
- 该服务包含约5k个用户、18k条策略，采用自行设计的Casbin LDAP角色管理插件支持RBAC的策略；
- Casbin提供了多租户粒度的权限管理，思科云的每一个访问请求都会经过Casbin过滤。目前应用Casbin的挑战主要在多域继承、多节点策略同步、降低决策延迟等方面。总之，Casbin为思科云的访问控制提供了坚实的基础架构。



附邮件原文：

无脑选择指南:

1. 会前端的, 选绿色;
2. 会Go的, 选橙色;
3. 会其他语言的, 选黄色

# 12个社区项目介绍

项目	难度	导师	需要会什么?	项目特点
1. Casbin核心引擎	高	罗杨 (hsluoyz)	纯Go	核心业务, 算法级改进
2. Casbin官方论坛	高	罗杨 (hsluoyz)	前端React, 后端Go	新业务, 完整项目
3. Casbin分布式插件	高	刘子轩 (nodece)	纯Go	专攻分布式领域
4. Casbin分布式高可用 (Rust)	高	江成 (GopherJ)	Rust	维护Rust版本Casbin
5. Casbin服务化 (C++)	中	谢非 (Joey)	C++	开发、维护C++版本Casbin
6. jCasbin 生态完善 (Java)	中	罗杨 (hsluoyz)	Java	维护Java版本Casbin
7. PyCasbin完善和优化	中	techoner	Python	维护Python版本Casbin
8. PHP-Casbin生态完善	中	techoner	PHP	维护PHP版本Casbin
9. Node-casbin 生态完善	低	刘子轩 (nodece)	Node.js	维护Node.js版本Casbin
10. Casbin.NET生态完善	高	周而易始(huazhikui)	.NET	维护.NET版本Casbin
11. Casbin仪表盘Web界面	中	张合龙 (BetaCat0)	前端React, 后端Go	新业务, 完整项目
12. 基于 Kubernetes 构建云原生分布式访问控制应用	高	张合龙 (BetaCat0)	纯Go, Kubernetes容器技术	专攻容器云技术



## 2. Casbin官方论坛

- Casbin官方论坛项目初衷
  - Casbin需要一个开源免费的、搜索引擎友好的非即时通讯渠道。
  - Slack: 搜索引擎不友好, 10000条以上收费
  - Gitter, Github: 国内访问速度慢
  - 论坛: 国内的discuzX等已经停止维护, 国外的discourse不符合国人习惯, ruby无论运维还是二次开发都比较麻烦
- 该论坛的另一个功能是全方位展示Casbin访问控制的功能, 后台利用Casbin进行权限管理, 前台利用casbin.js控制UI元素, 如按钮的显示。该论坛会成为Casbin技术最强有力的展示。该论坛开源, 因此也欢迎其他开源社区使用。
  - 论坛其实权限可以很复杂, 全局管理, 版主, 用户, 新人能不能发帖等, 这些都是权限, 还有前端权限, 正好测一下我们将要新推出的casbin.js
- 代码仓库:
  - Casbin-forum (<https://github.com/casbin/casbin-forum>)

## 3. Casbin 分布式插件 - Golang

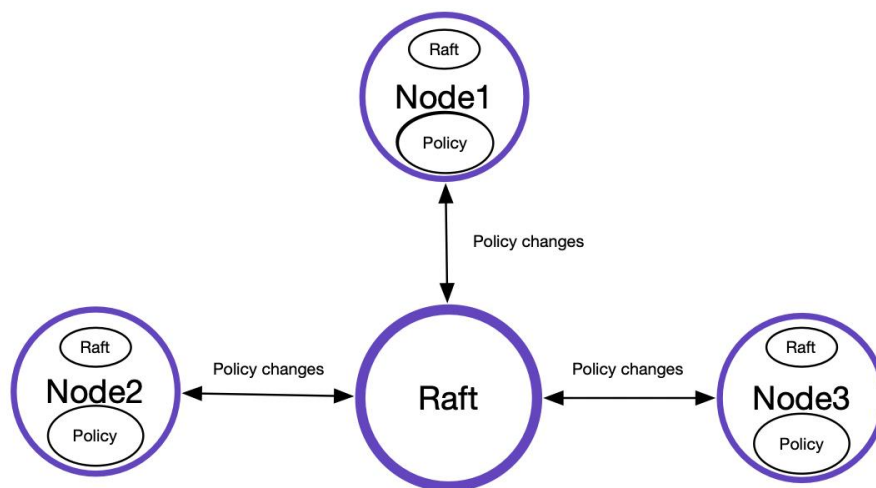
### ■ 项目描述

在分布式系统中，最常见的问题就是如何保证数据一致性。在 Casbin 中提出两个概念 adapter 和 watcher，adapter 用于存储策略，watcher 用于在分布式系统同步多个节点策略，当策略发生变更时将该次变更通过 adapter 持久化到策略到文件或数据库中，然后通过 watcher 去通知其他节点，其他的节点需要通过 adapter 全量拉取策略，但是 watcher 需要依赖提供 Pub/Sub 机制的中间件去实现。为了减少依赖中间件，实现增量同步策略提高性能，因此提出 Casbin 分布式插件。

## 3. Casbin 分布式插件 – Golang

### ■ 项目产出

- 基于 Raft 实现单机、分布式环境中多节点策略同步
- 正确，充足的单元/集成测试，确保 Casbin 在分布式环境下运行的正确性
- 支持动态增、删节点
- 探索如何将策略分组，映射到不同节点，确定策略的增，删以及某个请求的权限计算都在正确的节点进行, 以此减轻单机的内存压力



## 7.8. PHP和Python版Casbin生态建设

### ■ PHP-Casbin生态

- 目前支持Laravel、ThinkPHP、Yii、Codeigniter、CakePHP 等主流框架的扩展（已完成）。
- Symfony框架的扩展（待开发）。
- C级别框架 Phalcon Framework的支持（待开发）。
- 基于Swoole框架的支持，例如： Hyperf、easyswoole等（待开发）。
- PHP的C/C++扩展，基于Casbin-cpp，也可以考虑通过zephir实现（计划中）。

### ■ PyCasbin生态

- 完善PyCasbin，和Casbin（Golang）保持一致，在保证功能、结构不变的情况下调优
- 主流框架的扩展完善，例如： Django、Flask

### ■ 代码仓库：

- PHP-Casbin (<https://github.com/php-casbin>)
- PyCasbin (<https://github.com/casbin/pycasbin>)

## 9. Node-Casbin 生态完善

- 当前发展情况

Node-Casbin 创建于2018年7月，至今16名贡献者，star 将近1k，NPM 下载量 36k/month。

Node-Casbin 在 Node.js 平台上取得了不错的进展，但是我们仍然需要努力工作，以帮助 Casbin 成为世界上最受欢迎的身份授权库。Node-Casbin 已经对koa、egg、express、hapi 等主流框架提供了权限认证中间件，还需要对nest、meteor 提供支持。adapter 是 Casbin 持久化策略的插件，目前我们已经支持TypeORM、Sequelize，这些都是 ORM，因此我们还需要考虑提供纯数据库驱动的 adapter。

- 项目产出

- 实现 nest、meteor 权限认证中间件
- 实现纯数据库驱动的 adapter: PostgreSQL, Mysql, Microsoft SQL Server, Oracle, SQLite, IBM Db2.

- 代码仓库:

- Node-Casbin (<https://github.com/casbin/node-casbin>)

# 问答环节

Casbin 暑期2020主页:

<https://github.com/casbin/Summer2020>

## 如何申请?

### 1. 联系社区（2020年5月15日至6月20日）

1. 发送【中文简历PDF】至Casbin社区官方邮箱: [admin@casbin.org](mailto:admin@casbin.org)
2. 加入《Casbin访问控制社区群》（QQ大群）: [546057381](#)
3. 加入《Casbin软件所点亮计划-暑期2020-官方群》（QQ小群）: [632575275](#)，联系导师，与导师沟通项目细节和方案，完善项目申请书

### 2. 官网投递（2020年6月1日至6月20日）

详见: <https://isrc.iscas.ac.cn/summer2020/help/student.html#学生如何报名>