文章
Nicky Zhu · 二月 3, 2021 阅读大约需 分钟

IRIS中的权限管理

下一篇:
案例: 建立只能使用SQL的用户

IRIS通过认证(Authentication)与授权(Authorization)两项机制控制外部用户对系统及应用、数据资源的访问
此。如需进行权限控制，则需通过配置认证和授进行。

IRIS中的认证

认证可以验证任的试图连接到InterSystems IRIS®的用户的身份。一旦通过认证，用户就与IRIS建立了通信，从而可
以使用其数据和工具。有许多不同的方法可以验证用户的身份；每种方法都称为验证机制。IRIS
通常被配置为只使用其中一种方式。
支持的认证方式
* 实例认证：通过用户名/密码对登录平台，即密码认证
* LDAP：通过第三方LDAP服务器(如Windows Active Directory)完成证
* 操系统认证：建立操系统用户-平台用户映射，使用操系统用户登录平台
* Kerberos：使用Kerberos协议进行认证
* 代理认证：使用自定义的代码实现认证过程

系统服务与认证

在安装时，IRIS会启动一系列系统级的服务用与控制与外部用户或系统的交互，这些服务都绑定了默认的认证机制

Services are the primary means by which users and computers connect to InterSystems IRIS. The following services are currently available:

页面大小: 0 最大行数: 1000 结果: 16 页面: 1 的 1

名称	已启用	公用	身份验证方法	允许的连接	描述
%Service_Bindings	是	无	密码,委托	未受限	控制 SQL 或对象
%Service_CacheDirect	否	是	密码	未受限	控制 Cache 引导
%Service_CallIn	否	是	密码	未受限	控制调入接口
%Service_ComPort	否	是	密码	未受限	控制连接到Windows系统的COM端口
%Service_Console	是	是	密码,委托	未受限	控制 CTERM (TRM:pid) 和 Windows 控制台
%Service_DataCheck	否	无		未受限	控制此系统作为 DataCheck 源
%Service_DocDB	否	否		未受限	Controls Doc DB applications
%Service_ECP	是	无		未受限	控制 Enterprise Cache Protocol (ECP)
%Service_Login	是	否	密码	未受限	控制 SYSTEM.Security.Login
%Service_Mirror	否	无		未受限	控制镜像
%Service_Monitor	否	无		未受限	控制 SNMP 和远程监视命令
%Service_Shadow	否	无		未受限	控制此系统是否可以是shadow来源
%Service_Sharding	否	无		未受限	Controls this system as a Shard Server
%Service_Telnet	否	是	密码	未受限	控制 Windows 服务器上的 Telnet 会话
» %Service_WebGateway	是	是	密码	未受限	控制CSP网关访问
%Service_Weblink	否	无	未验证	未受限	控制网络链接

图中红框标出的即为系统安装后会自动启用并需认证才可使用的系统服务，认证手段可配置。
例如，如果变更%Service_Console的身份验证方法，取消密码方法，用户就不能通过输入用户名密码登入Terminal
。
通过Portal的菜单 系统管理 > 安全 > 服务 可访问该设置。

账户控制参数

通过系统管理 > 安全 > 系统安全 >
系统范围的安全参数中的选项可对于用户名/密码认证手段的行为进行更加约束。

- 非活动限制 - 指定用户账户不活跃的最大天数，它被定义为成功登录之间的时间。当达到此限制时，该帐户将被禁用。值为0（0）表示对登录之间的天数没有限制。[对于最低安全级别的安装，默认为0，对于正常和锁定的安装，默认为90]。
- 无效登录限制 (0-64) - 指定连续不成功的登录尝试的最大次数。在达到此限制后，要么禁用账户，要么对每次尝试进行递增的时间延迟；行动取决于如果达到登录限制字段则禁用账户的值。值为0（零）表示对无效登

录的次数没有限制。[默认为5]
- 如果达到登录限制，则禁用账户 -
  如果选中，则指定达到无效登录次数（在前一字段中指定）将导致用户账户被禁用。
- 密码有效期天数(0-99999) - 指定密码过期的频率以及用户更改密码的频率(天数)。当初始设置时，指定密码过期的天数。0（0）表示密码永远不会过期。不会影响已设置了下次登录时更改密码字段的用户。[默认为0]

特别 注 意的是，密码有效性过期和禁用账户等设置会影响IRIS实例的所有账户，包括IRIS超级管理员账户。如触发了控制策略，则在更新这些帐户的信息之前，可能无法进行任何操作，这可能导致意外结果。如超级管理员账户被锁定，则需要通过紧急模式启动实例再进行修

对于系统可用的认证手段的配置和其他可用的安全配置，请参见 Security Administration Guide

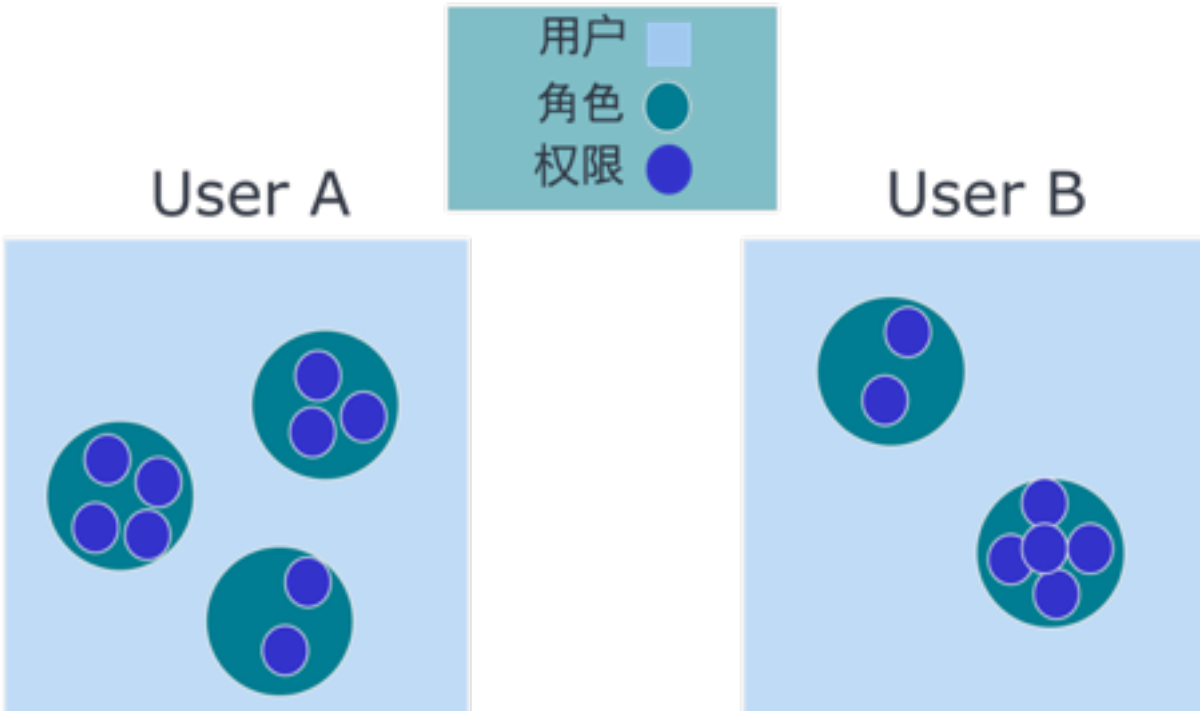
IRIS中的授权

授权模型

InterSystems公司的授权模式采用基于角色的访问控制。

- Users – 用户
- Roles – 角色
- Privileges – 权限
- Resources – 资源 | Permissions – 许可

在这种模式下，用户拥有与分配给其自用户身份的角色相关的权限。



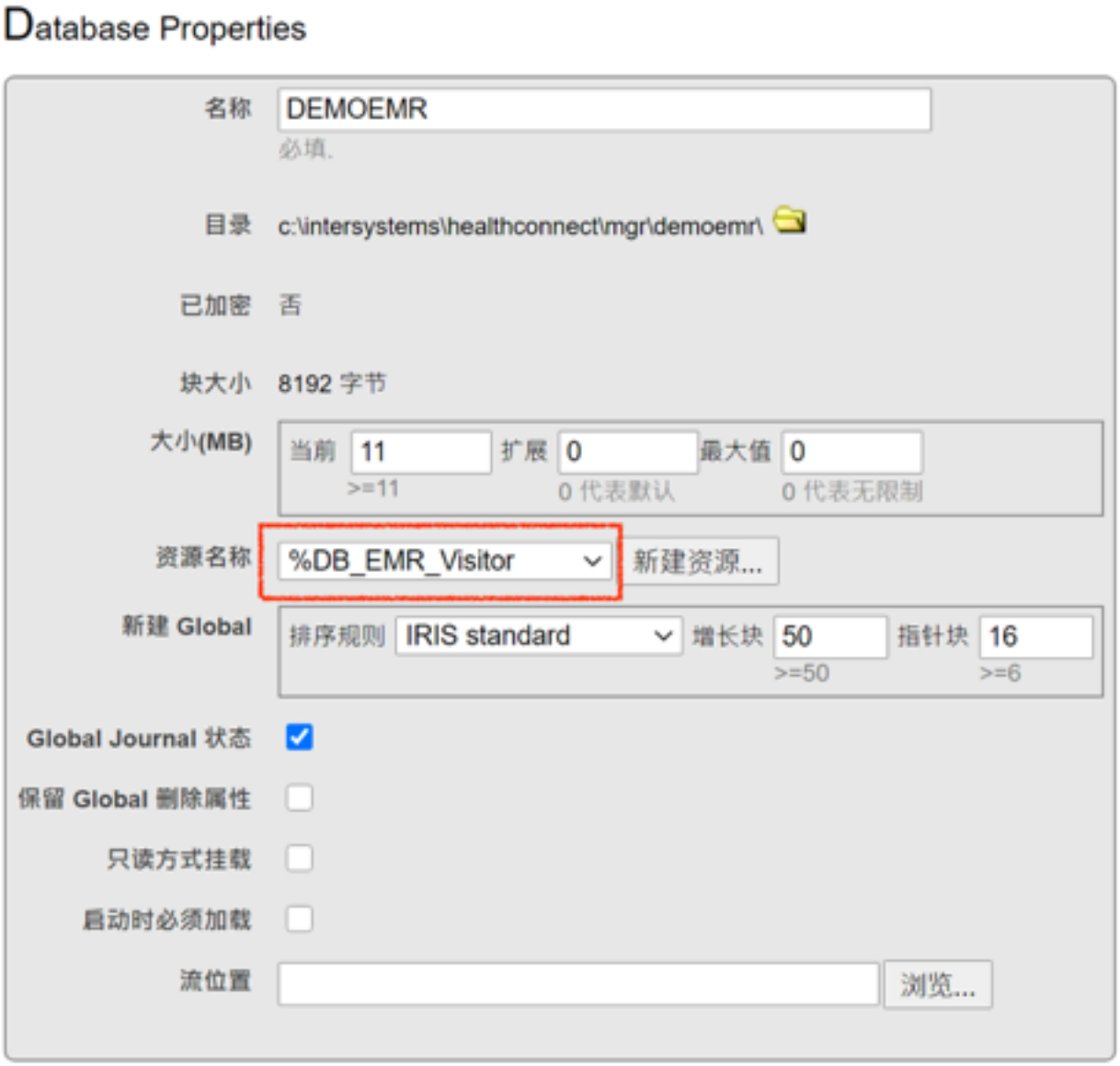
- 一个角色是一个命名的特权集合
- 一个用户可以拥有一个以上的角色
- 权限分配给角色，角色分配给用户

其中，Roles就是权限的集合，而权限提供对资源的特定类型的访问的许可。

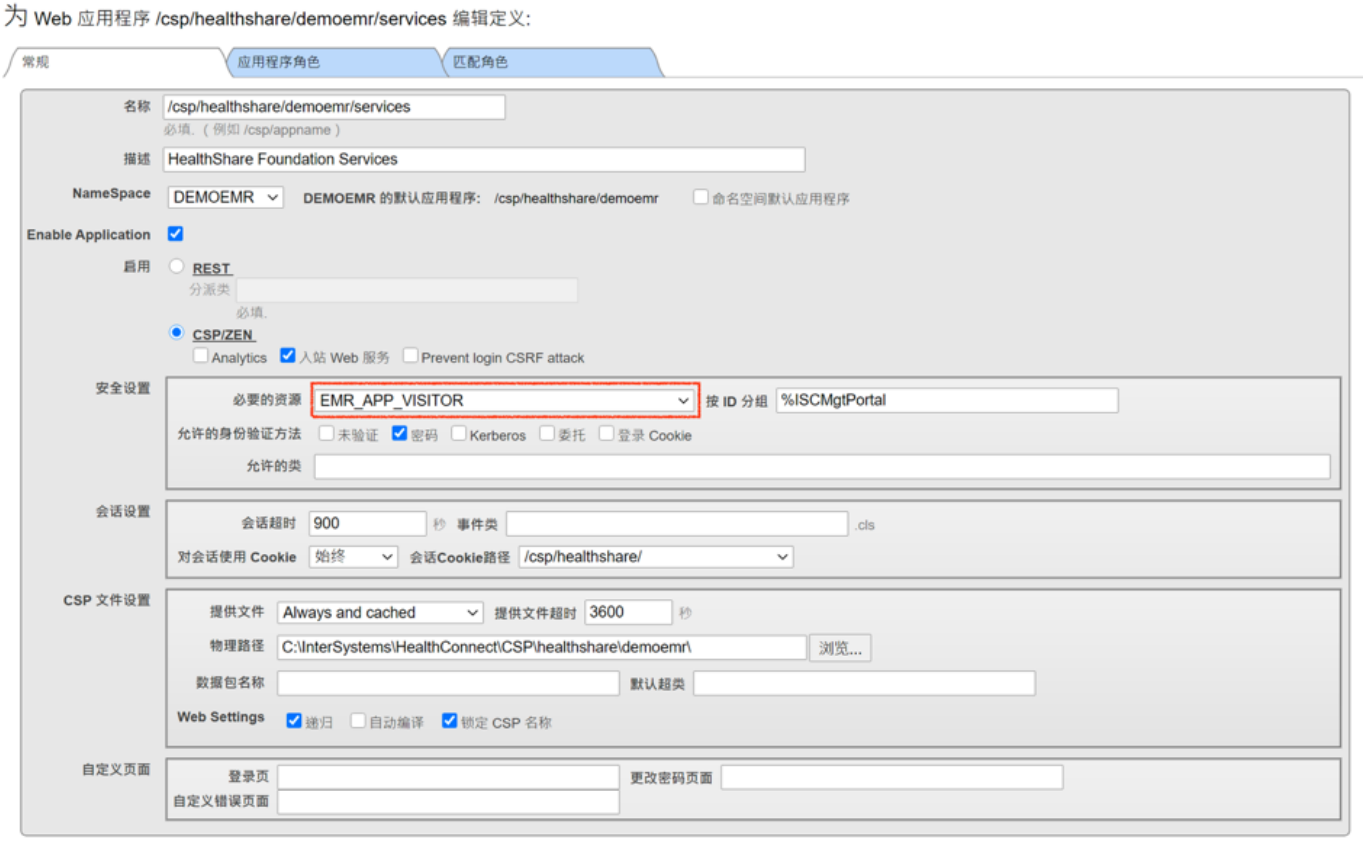
- 可控资源: 数据库，服务，应用（包括Web应用）和其他
- 可选用的许可: Read, Write or Use，其中执行代码需要数据库的读权限

资源的定义

资源是一项相对抽象的概念，用来指代IRIS中的数据库，服务，应用等可被访问的对象。例如，对于数据库，在建立时默认采用%DB_%DEFAULT指代，也可自定义资源（数据库资源必须以%DB_开头）：



对于Web应用，默认不经过资源控制，即所有可登录用户都可访问（但该用户进程不一定能访问到数据，还需参照是否具有对数据库的访问权限）。如通过分配资源进行控制，则登录用户还需有资源才能访问这个Web应用：

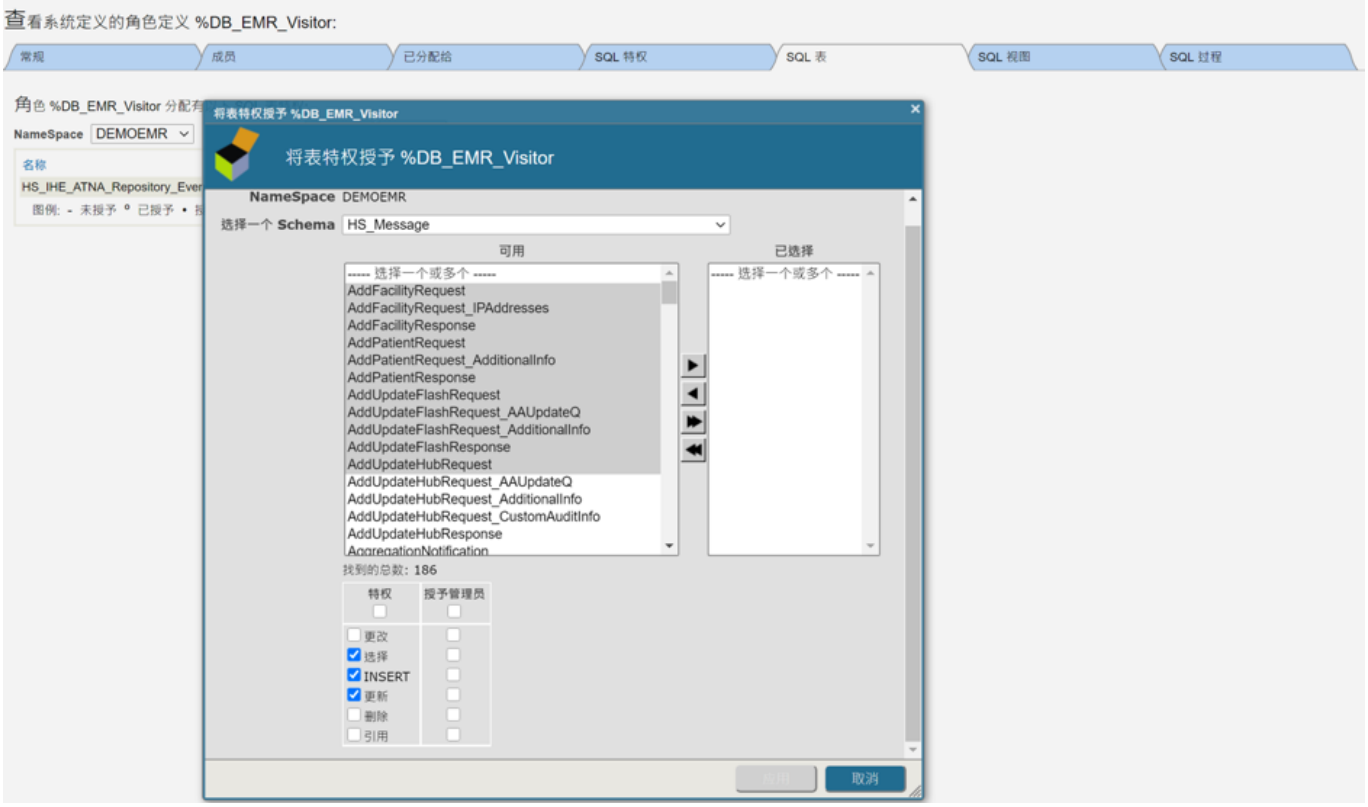


因此，一项权限实际上是指对某个资源的一些特定操的集合。
例如，对于数据库UserDB具有读写操许可的权限A，对于Web应用/csp/sys具有使用操许可的权限B。如果们
将这两项权限都赋给角色RoleA，那么这个角色就同时拥有A权限和B权限，从而能够访问数据库UserDB和访问Web
应用/csp/sys。

SQL授

除了对数据库进行授外，IRIS作为一个数据平台，需对外提供数据访问。因此，IRIS也提供了SQL授对用户可
执行的SQL进行细粒度的权限控制。
SQL的授可以分配给角色或用户。但通常在企业环境中，用户数量会很多，仍然需对SQL用户进行分组，根据分
组规划角色，通过角色进行授的控制，才能有效降低维护授所需工作量。
SQL的授针对SQL类型，可分为库、表级授。
对于Create table、drop view、truncate
table这一类的DDL，使用库级授，即用户可在特定的库中执行建表、删除视图等经过授的操。如下：

对于Select、update等DML，则使用表级**授**，使用户能够通过DML访问特定的表中的数据。如：



除通过Portal操之外，对于SQL的**授**，还可使用IRIS SQL中的额GRANT语句，例如：

GRANT * ON Schema Test TO TestRole

这个SQL即可以将当前操数据库Schema Test中的所有表的所有权限都赋给TestRole这个角色。
关于GRANT语句的用法，可参见 GRANT指令

以上即为IRIS中进行权限控制所需的概念和内容，在后续文章中，我们会结合实例向大家介绍其使用。

下一篇：
案例: 建立只能使用SQL的用户

推荐阅读

Security Administration Guide - https://docs.intersystems.com/irisforhealthlatest/csp/docbook/DocBook.UI...

#SQL #安全 #数据库 #新手 #用户 #系统管理 #角色 #身份验证 #InterSystems IRIS #文档

源 URL: https://cn.community.intersystems.com/post/iris%E4%B8%AD%E7%9A%84%E6%9D%83%E9%99%90%E7%AE%A1%E7%90%86