文章
Nicky Zhu · 十月 18, 2021 阅读大约需 11 分钟

IRIS 2021 技术文档 First Look 27--基于角色的访问控制

目录

技术概要：基于角色的访问控制

本文档向您介绍基于角色的访问控制，解释它在 InterSystems IRIS®数据平台中的工作原理，并帮助您亲自探索。

要浏览所有的技术概要（First Look），包括可以在 InterSystems IRIS 免费的评估实例上执行的那些，请参见 InterSystems First Looks（《InterSystems 技术概要》）。

基于角色的访问控制：为什么它很重要？

当您首次开始使用一个新的数据库平台时，有件事情可能很快就会变得清晰起来：您可能不希望企业中的所有用户都查看和更改系统上的所有内容。

InterSystems IRIS 和所有的数据库平台一样，允许您精细指定 InterSystems IRIS 的每个用户可以执行的操作。我们用来控制用户*授权（authorization）*执行操作的机制被称为*基于角色的访问控制（role-based access control）*。

如果您已经熟悉了基于角色的访问控制，InterSystems IRIS 方案很可能与您以前使用过的一些方案相似。您会在下一节找到有关我们如何处理它的更多细节。

如果您是基于角色的访问控制的新手，这意味着比旧的访问控制方法节省时间，因为旧的访问控制方法没有提供执行系统操作的权限分组。

- 如果没有基于角色的访问控制，为每个用户逐个分配使用 InterSystems IRIS 的各个方面的权限可能需要数小时甚至数天。然后，如果有新员工需要访问，您将不得不重复这个过程。
- 基于角色的访问控制允许您在初始配置 InterSystems IRIS 时将权限分组到角色中。然后，您可以为每个系统用户分配一个或多个现成的角色。您还可以使用或修改一组预定义的角色。

- 此外，通过基于角色的访问控制，如果用户需要使用一组新的权限，则可以将该组权限分组为一个角色，并将该角色分配给用户。而且您可以随时改变角色内的权限列表。

基于角色的访问控制: 如何在 InterSystems IRIS 中工作

InterSystems IRIS
为基于角色的访问控制提供了一个完整的解决方案，我们将在本节中对此进行描述。InterSystems IRIS 支持的每一种认证机制，包括 LDAP、Kerberos 和 OS-based，都可以使用本地 InterSystems 基于角色的访问控制。如果您愿意，您可以使用 LDAP 而不是 InterSystems IRIS 进行角色分配。

简要概念概述

把 InterSystems IRIS 中的信息和功能视为您要保护的*资产*，就像您为属于您的资产投保一样。

基于角色的访问控制：如何在 InterSystems IRIS 内部工作

在 InterSystems IRIS 中被视为资产的项目包括：

- 数据库，将数据和代码作为对象存储。
- 服务，控制用户连接到 InterSystems IRIS 的能力。
- 某些管理权限。
- InterSystems IRIS 应用程序，包括*管理门户（Management Portal）*中的各个页面，它是 InterSystems IRIS 的系统管理用户界面。

在 InterSystems IRIS
中，每项资产（asset）都由一个*资源**（resource）*
来表示，一个资源（resource）可以表示多个资产（asset）。

资源（resource）充当它所代表的资产（asset）的看门人：根据资源类型，它与
"读取"、"写入"（包括读取），和在某些情况下的 "使用"（执行）*权限（permission）*
配对。例如，数据库只存在两种类型的权限：读取，允许查看数据和执行例程；写入，允许修改数据。

资源与权限的配对被称为*权限（privilege）*，权限按*角色（role）*分组。

最后，角色*（role）*被分配给 InterSystems IRIS 中的*用户（user）*。每个用户*（user）*在首次使用 InterSystems IRIS
进行认证时，都会有一个或多个角色*（role）*分配给他们。可以在会话期间向用户添加或删除角色*（role）*。

基于角色*（role）*
的访问控制的具体授权方式取决于您所选择的认证机制。在线文档中完全涵盖了授权的这方面内容。

提示：
对于内部测试和暂存系统，您可能
不希望设置基于密码的认证或基于角色*（role）*的不同级别的访问控制。如果您使用 "最低（minimal）" 安全性来安装您的实例，这个选项是可用的，默认情况下，它给拥有实例的管理门户（Management Portal） URL 的任何人提供完全管理权限。

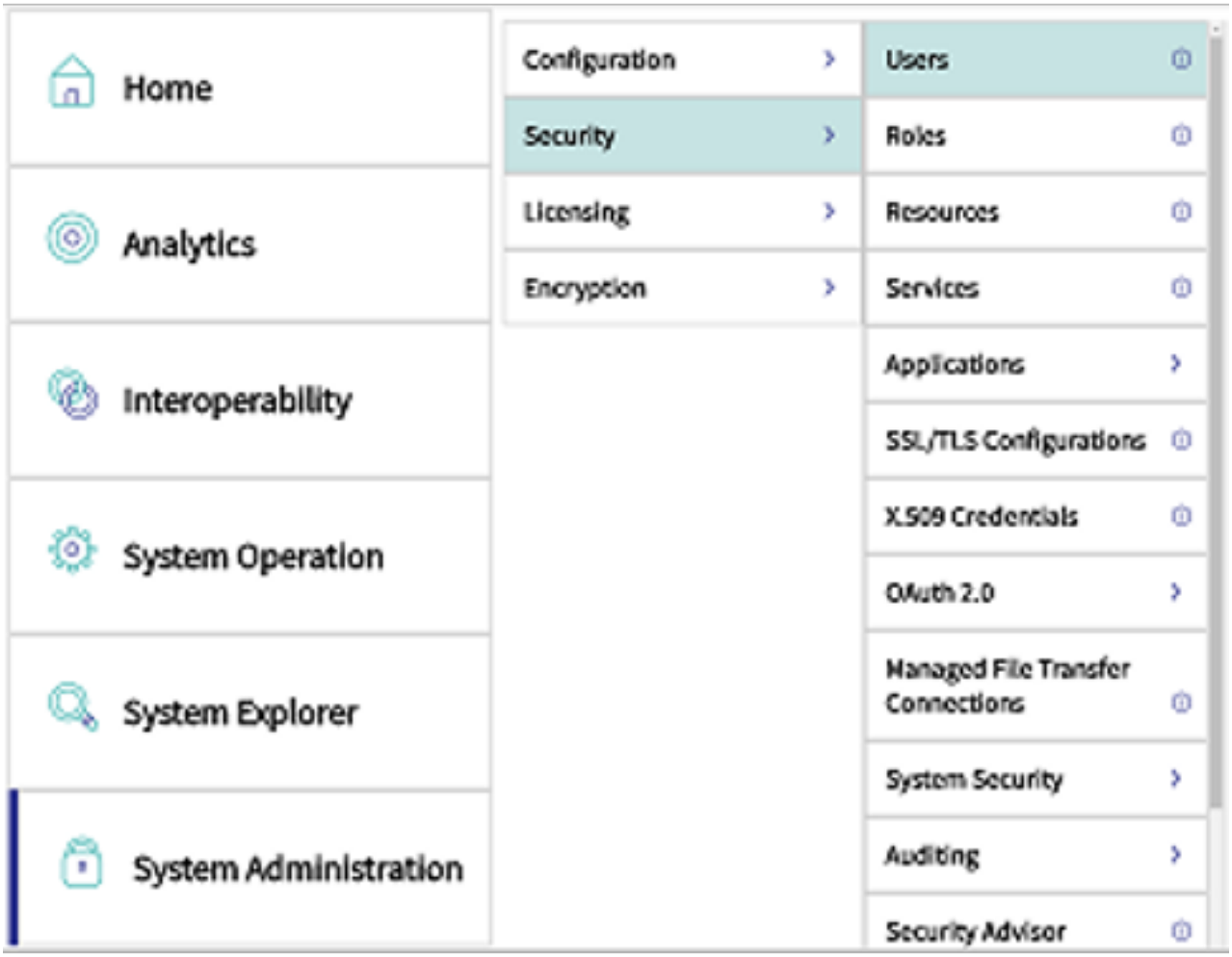
示例用例

如上所述，管理门户（Management Portal）中的各个页面是 InterSystems IRIS
中您可以保护的资产（asset）。管理门户（ Management Portal）允许用户（user）查看和执行 InterSystems IRIS 基本方面的操作，如 globals、命名空间，甚至资源（resource）和角色（role）本身。

下面的屏幕截图显示了当实例的管理员使用安装时创建的 **SYSTEM** 帐户登录时，管理门户（Management Portal）的外观和行为。 **SYSTEM** 用户可以访问 **System Administration（系统管理）** > **Security（安全）** >

Users（用户），让他们可以查看和修改任何用户（user）及其角色（role）。

您可能想限制某些管理门户（Management Portal）用户的角色（role）分配，使他们不能查看或修改用户（user）帐户或任何其他对安全至关重要的信息。在下一节，我们将告诉您如何做到这一点。



基于角色的访问控制: 探索它

下面的示例向您展示了如何设置两种类型的"管理者"角色，以便在管理门户（Management Portal）中使用。第一个角色将能够访问允许修改用户和角色定义等安全相关项的页面。第二个角色将没有这个访问权限。

然后您会看到拥有这些角色的用户如何与管理门户（Management Portal）交互。

重要提示： 为了让您体验 InterSystems IRIS，而又不陷入细节的困境，我们保持了简单的探索。例如，我们让您尽可能多地使用默认设置。

但是，当您把 InterSystems IRIS 引入您的生产系统时，您需要做很多不同的事情，特别是（但不限于）安全方面。

所以请确保不要把这种对 InterSystems IRIS 的探索与真实的情况相混淆！本文档末尾提供的参考资料将使您对在生产中使用 InterSystems IRIS 的情况有一个很好的了解。

用前须知

要使用该程序，您需要一个正在运行的 InterSystems IRIS 实例。您的选择包括多种类型的已授权的和免费的

评估实例；该实例不需要由您正在工作的系统托管（尽管它们必须相互具有网络访问权限）。关于如何部署每种类型的实例的信息（如果您还没有可使用的实例），请参见 *InterSystems IRIS Basics: Connecting an IDE*（《*InterSystems IRIS 基础：连接一个 IDE*》）中的 Deploying InterSystems IRIS（部署 InterSystems IRIS）。使用同一文档中的 InterSystems IRIS Connection Information（InterSystems IRIS 连接信息）和 .Net IDE 中的信息将 Visual Studio 连接到您的 InterSystems IRIS 实例。

发现管理门户（Management Portal）页面访问所需的资源

对管理门户（Management
Portal）中的每个页面的访问都受到至少一种资源的保护。您可以通过以下方式发现所需的资源：

0. 使用 *InterSystems IRIS Basics:Connecting an IDE*（《*InterSystems IRIS 基础：连接一个 IDE*》）中URL described for your instance（为您的实例描述的
URL），在浏览器中打开您的实例的管理门户（Management Portal）。
1. 通过点击相应菜单项中的每一个单词，导航至 **System Administration（系统管理）** > **Security（安全）**。

基于角色的访问控制：探索它

提示： 在管理门户（Management Portal）中，带有子页面的菜单项在其名称旁边包含 **>>**
。页面没有这样的标记。

3. 在 **Users（用户）** 菜单项中，点击"用户（Users）"一词右侧的任何位置。这个操作显示查看
Users（用户）页面所需的资源，即 **%AdminSecure** 。(**Security（安全）** 和 **Encryption（加密）**
子菜单中的所有页面都需要 **%AdminSecure** 资源上的使用权限（"U"）。)

4. 导航至 **System Administration（系统管理）** > **Configuration（配置）** > **System Configuration（系统配置）**。
5. 点击"内存和启动（Memory and Startup）"右侧的任何位置。您会看到，查看该页面所需的资源是
%AdminManage 。

0. 创建和分配您自己的管理者角色

对于管理门户（Management Portal）的 **System Administration（系统管理）**菜单内的页面，您需要具有

%AdminSecure 和 **%AdminManage** 资源权限的角色。

鉴于这种结构，您可能希望创建两个反映管理级别的角色，一个是可以访问除安全相关页面以外的所有页面，另一个是可以执行所有操作，包括安全相关的操作。您可以使用预定义的 **%Managerrole** 作为模板。

0. 使用 **SYSTEM** 帐户登录管理门户（Management Portal）。
1. 导航至 **System Administration（系统管理）** > **Security（安全）** > **Roles（角色）** ，并点击 **Go**
。您将看到安装了 InterSystems IRIS 的角色列表，包括 **%Manager** 角色。
2. 点击 **%Manager** 链接。 **General（常规）** 标签显示具有此角色的用户可用的权限（与权限配对的资源）。
    - 在权限中，您会看到 **%AdminSecure** 和 **%AdminManage** 上的使用权限。
    - 您也会看到许多其他的权限。这是因为您需要访问许多不同的资源，才能够查看和修改 InterSystems IRIS 设置。既然我们知道只有一种关键资源 **%AdminSecure** ，在 **System Administration（系统管理）**

的安全相关页面的访问方面，对该资源的访问将是我们两个自定义角色之间的唯一区别。

3. 点击 **Cancel（取消）** (在 **Edit %Manager** 下面)，返回到主 **Roles（角色）**页面。

0. **创建 "标准管理者"角色**

0. 在 **Roles（角色）**页面上，点击 **Create New Role（创建新角色）**。将出现一个角色定义页面。

基于角色的访问控制：探索它

2. 在 **Name（名称）** 字段中，输入"**StandardMgr** "。
3. 在 **Copy from（复制自）** 下拉菜单中，选择 **%Manager**。这将复制所有信息，包括权限，从预定义 **%Manager** 角色到新角色。
4. 将描述更改为您所选择的描述，例如："**Role for System Administration without security access（不具有安全访问权限的系统管理角色）**"。
5. 点击 **Save（保存）**。将出现一条 **Role saved（保存角色）** 信息，您将在 **General（常规）** 标签中看到新角色的权限列表。
6. 在 **%AdminSecure** 行中，点击 **Delete（删除）**。这就从角色中删除了权限。
7. 再次点击 **Save（保存）** 来保存更改。

0. **创建"安全管理员"角色**

0. 在 **Roles（角色）**页面上，点击 **Create New Role（创建新角色）**。将出现一个角色定义页面。
1. 在 **Name（名称）** 字段中，输入"**SecurityMgr** "。
2. 在 **Copy from（复制自）**下拉菜单中，选择 **%Manager**。这将复制所有信息，包括权限，从预定义 **%Manager** 角色到新角色。
3. 将描述更改为您所选择的描述，例如："**Role for System Administration with securityaccess（具有安全访问权限的系统管理角色）**"
4. 点击 **Save（保存）**。将出现一条 **Role saved** 信息，您将在 **General（常规）** 标签中看到新角色的权限列表。

0. 创建用户并分配新角色

要查看角色的运行情况，需要创建两个用户，每个用户对应一个新角色。

0. 使用 **SYSTEM** 帐户登录管理门户（Management Portal）。
1. 导航至 **System Administration（系统管理）** > **Security（安全）** > **Users（用户）**，并点击 **Go** 。您将看到安装了 InterSystems IRIS 的用户定义列表。

0. **创建"标准管理员"用户**

0. 在主 **Users（用户）** 页面上，点击 **Create New User（创建新用户）**。将出现一个用户定义页面。

1. 在 **Name（名称）** 字段中，输入"**StdMgr** "。(用户的名称不能与角色的名称一致)。
2. 在 **Password（密码）** 和 **Password (confirm)（确认密码）** 字段中，输入您选择的密码。
3. 点击 **Save（保存）**。将出现一条 **User saved** 信息。
4. 点击 **Roles（角色）**标签。滚动左侧的 **Available** 列表，并高亮显示 **StandardMgr（标准管理员）** 。
5.

   点击右箭头 ，将该角色添加到 **Selected（已选）**列表中。然后点击"**Assign（分配）**"。

   7. 点击 **Cancel（取消）** 以返回到主 **Users（用户）**页面。

创建"安全管理员"用户

0. 在主 **Users（用户）** 页面上，点击 **Create New User（创建新用户）**。将出现一个用户定义页面。
1. 在 **Name（名称）** 字段中，输入"**SecMgr** "。
2. 在 **Password（密码）** 和 **Password (confirm)（确认密码）** 字段中，输入您选择的密码。

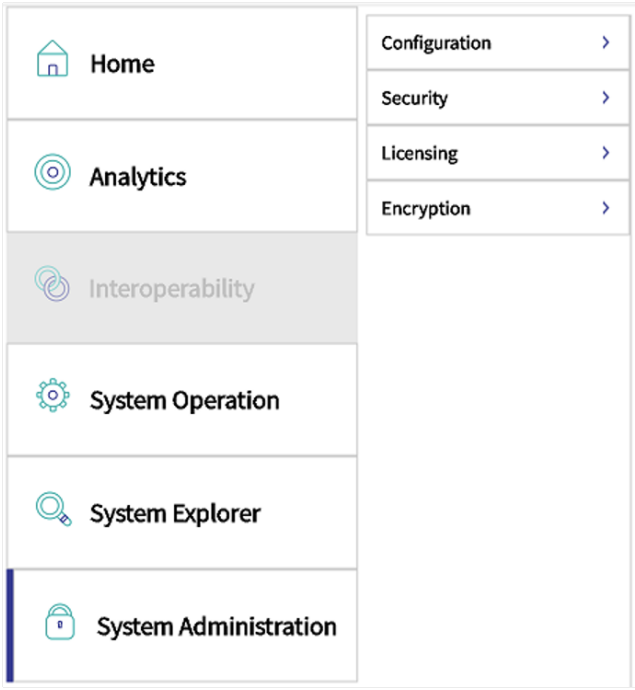
   基于角色的访问控制：探索它

4. 点击 **Save（保存）**。将出现一条 **User saved** 信息。
5. 点击 **Roles（角色）**标签。滚动左侧的 **Available** 列表，并高亮显示 **SecurityMgr（安全管理员）** 。
6. 点击右箭头，将该角色添加到 **Selected（已选）**列表中。然后点击 **Assign（分配）**。
7. 点击 **Cancel（取消）** 以返回到主 **Users（用户）**页面。

0. 尝试管理门户（Management Portal）中的角色

0. 以 **StdMgr** 用户（标准管理员用户）登录管理门户（Management Portal）。您将看到，与安全有关
   的菜单选项是灰色的，正如预期的那样。**Interoperability（互操作性）**
   菜单选项也是灰色的，因为从其中复制两个自定义角色的预定义 **%Manager** 没有访问这些页面所需的权限。

1. 退出，然后以 **SecMgr** 用户（安全管理员用户）重新登录。 正如您所看到的，这个用户具有对 **System Administration（系统管理）** > **Security（安全）**和 **System Administration（系统管理）** > **Encryption（加密）** 子菜单中的页面的完全访问权限。



了解有关基于角色的访问控制的更多信息

要了解有关基于角色的访问控制和 InterSystems IRIS 安全模型的更多信息，请参见：

- *About InterSystems Security*（《*有关 InterSystems 安全*》）中的 "Authorization:Controlling User Access（授权：控制用户访问）"一节
- *InterSystems IRIS Programming Orientation Guide*（《*InterSystems IRIS 编程指南*》）中的 "InterSystems IRIS Security（InterSystems IRIS 安全）"和 "Namespaces and Databases（命名空间和数据库）"部分 --- 为应用程序开发人员提供有关基于角色的访问控制的信息。
- *Security Tutorial*（《*安全教程*》）中的 "Authorization（授权）"部分 --- 创建用户、角色和权限的逐步说明。

#InterSystems IRIS for Health

源 URL: https://cn.community.intersystems.com/post/iris-2021-%E6%8A%80%E6%9C%AF%E6%96%87%E6%A1%A3-first-look-27-%E5%9F%BA%E4%BA%8E%E8%A7%92%E8%89%B2%E7%9A%84%E8%AE%BF%E9%97%AE%E6%8E%A7%E5%88%B6