文章
jieliang liu · 十月 26, 2021 阅读大约需 13 分钟

IRIS 2021 技术文档 First Look 29 技术概要：LDAP 和 InterSystems 产品

技术概要：LDAP 和 InterSystems 产品

目录

技术概要：LDAP 和 InterSystems 产品

InterSystems IRIS®数据平台可以与 LDAP（轻量级目录访问协议，Lightweight Directory Access Protocol）服务器集成，从而可以无缝地使用这种流行技术对用户进行身份验证。通过 LDAP 提供授权也很容易。

当用户尝试登录 InterSystems IRIS 时，用户名和密码会被发送到 LDAP 服务器，以验证该用户是否存在。一旦用户的身份得到验证，LDAP 服务器就会向 InterSystems IRIS 发送关于用户属于哪些组的信息。这些组与 InterSystems IRIS 中的角色相对应，这些角色控制用户被授权执行什么操作，以及是否可以读取或写入内容。通过这种方式，InterSystems IRIS 在其安全策略的身份验证和授权方面都使用了 LDAP 技术。

按照本指南中的步骤，您可以连接到 LDAP 服务器，并探索它如何影响 InterSystems IRIS 中的安全。在这些练习中，您将配置 InterSystems IRIS 以与 Windows 活动目录（Active Directory）服务器集成。虽然也支持其他的 LDAP 服务器，但本文主要介绍如何使用活动目录（Active Directory）进行 LDAP 身份验证和授权。

要浏览所有的技术概要（First Look），包括下面描述的可以在免费的社区版（Community Edition）实例上执行的其他内容，请参见 InterSystems First Looks（《InterSystems 技术概要》）。

设置 LDAP 身份验证

在以 LDAP 用户登录并在 InterSystems IRIS 中探索基于 LDAP 的安全之前，需要完成以下操作：

- 选择 InterSystems IRIS 实例
- 定义 LDAP 配置
- 选择 LDAP 域作为默认值
- 在 InterSystems IRIS 中启用 LDAP 身份验证
- 为 LDAP 服务器安装安全证书

0. 选择 InterSystems IRIS 实例

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）。

定义 LDAP 配置

InterSystems IRIS 使用 LDAP 配置来定义连接到 LDAP 服务器和搜索用户所需的信息。要创建和定义新的 LDAP 配置：

设置 LDAP 身份验证

0. 在浏览器中打开您的实例的管理门户（Management Portal）。要使用的 URL 取决于您选择的实例类型；有关确定正确的 URL 的信息，请参见 *InterSystems IRIS Basics:Connecting an IDE*（《*InterSystems IRIS 基础：连接一个 IDE*》）中的 InterSystems IRIS Connection Information（InterSystems IRIS 连接信息）。
1. 进入 **Security LDAP Configurations（安全 LDAP 配置）** 页面 (**System Administration（系统管理） > Security（安全） > System Security（系统安全） > LDAP Configurations（LDAP 配置）**)。
2. 点击 **Create New LDAP configuration（创建新 LDAP 配置）**。
3. 在 **Name（名称）**字段中，输入 irisldap.com。
4. 选择 **Enabled（已启用）** 复选框。
5. 选择 **LDAP server is a Windows Active Directory server（LDAP 服务器是一个 Windows 活动目录（Active Directory） 服务器）** 复选框。
6. 定义以下字段：

+----------+----------+ ¦ **字段** ¦ > **内容** ¦ +==========+==========+ ¦ **LDAP domain name（LDAP 域名）** (仅限 Windows) ¦ > irisldap.intersystems.com ¦ +----------+----------+ ¦ **LDAP host names（LDAP 主机名）** ¦ > irisldapdc1.irisldap.intersystems.com ¦ +----------+----------+ ¦ **LDAP username to use for searches（用于搜索的 LDAP 用户名）** ¦ - (Windows) sidLDAPQuery ¦ ¦ ¦ ¦ ¦ ¦ - (UNIX®) ¦ ¦ ¦ ¦ ¦ ¦ > CN=sidLDAPQuery,CN=Users,DC=irisldap,DC=intersystems,DC=com ¦ +----------+----------+ ¦ **LDAP username password（LDAP 用户名密码）** ¦ > 选择 **Enter New Password（输入新密码）**, 然后输入密码为 Cach3L3arning ¦ +----------+----------+ ¦ **LDAP Base DN to use for searches（用于搜索的 LDAP 基础 DN）** ¦ > DC=irisldap,DC=intersystems,DC=com ¦ +----------+----------+ ¦ **LDAP Unique search attribute（LDAP 独特的搜索属性）** ¦ > sAMAccountName ¦ +----------+----------+

8. 选择 **Use TLS/SSL encryption for LDAP sessions（将 TLS/SSL 加密用于 LDAP 会话）**复选框。
9. 选择 **Use LDAP Groups for Roles/Routine/Namespace（将 LDAP 组用于角色/路由/命名空间）**复选框。
10. 选择 **Allow Universal group Authorization（允许通用组授权）**复选框。
11. 点击 **Save（保存）**。

0. 选择新的 LDAP 域作为默认值

一旦定义了 LDAP 服务器的 LDAP 配置，您需要将新的 LDAP 配置设置为默认的 LDAP 域。要将 LDAP 服务器设置为默认服务器：

0. 从管理门户（Management Portal）主页，进入 **System-wide Security Parameters（全系统安全参数）** 页面 (**System Administration（系统管理） >**Security（安全） > System Security（系统安全） > System-wide Security Parameters（全系统安全参数）**)。
1. 从 **Default security domain（默认安全域）**下拉列表中选择 irisldap.com。
2. 点击 **Save（保存）**。

0. 启用 LDAP 身份验证

使用 LDAP 服务器只是 InterSystems IRIS 中可用的一种身份验证方法。不仅必须为 InterSystems IRIS 的整个实例启用 LDAP 身份验证，而且需要由 LDAP 用户访问的 InterSystems IRIS 的每个组件也必须启用 LDAP 身份验证。以下程序为实例和 InterSystems IRIS 安全所需的那些组件启用 LDAP 身份验证：

设置 LDAP 身份验证

0. 从管理门户（Management Portal）主页，进入 **Authentication/Web Session Options（身份验证/Web 会话选项）** 页面(**System Administration（系统管理）> Security（安全） > System Security（系统安全） > Authentication/Web Session Options（身份验证/Web 会话选项）**)。
1. 选择 **Allow LDAP authentication（允许 LDAP 身份验证）**复选框。
2. 点击 **Save（保存）**。
3. 从管理门户（Management Portal）主页，进入 **Web Applications（Web 应用程序）**页面 (**System Administration（系统管理） > Security（安全） > Applications（应用程序） > Web Applications（Web 应用程序）**)。

   在这个页面上，您将为您在 InterSystems IRIS 中将要访问的管理门户（Management Portal）部分启用 LDAP 授权。因为管理门户（Management Portal）的其他部分没有启用 LDAP 授权，如果您试图探索这些其他部分，可能会被要求登录。

5. 点击 **/csp/sys** 来显示用于配置 web 应用程序的页面。
6. 在 **Security Settings（安全设置）** 部分，在 **Allowed Authentication Methods（允许的身份验证方法）**字段中选择 **LDAP** 复选框。
7. 点击 **Save（保存）**。
8. 一旦设置被保存，点击 **Cancel（取消）**以返回到 **Web Applications（Web 应用程序）**页面。
9. 点击 **/csp/sys/sec**。这个 web 应用程序包含管理门户（Management Portal）的安全页面。
10. 在 **Security Settings（安全设置）**部分，在 **Allowed Authentication Methods（允许的身份验证方法）**字段中选择 **LDAP** 复选框。
11. 点击 **Save（保存）**。
12. 一旦设置被保存，点击 **Cancel（取消）**以返回到 **Web Applications（Web 应用程序）** 页面。
13. 点击 **/csp/sys/op**。这个 web 应用程序包含管理门户（Management Portal）的操作页面。
14. 在 **Security Settings（安全设置）** 部分，在 **Allowed Authentication Methods（允许的身份验证方法）**字段中选择 **LDAP** 复选框。

15. 点击 **Save（保存）**。

0. 为 LDAP 服务器安装安全证书

LDAP 服务器采用 TLS 进行安全保护，因此您需要安装安全证书才能成功访问服务器。在将其标识为安全证书之前，您将创建一个包含所需证书内容的 .cer 文件。

0. 创建 .cer 文件

要创建将作为安全证书安装的文件：

0. 打开一个文本编辑器，如记事本，并创建一个新文件。
1. 复制以下所有内容并将其粘贴到文本编辑器中的新文件中。新文件应该以

-----BEGIN CERTIFICATE-----开头，并以-----END CERTIFICATE-----结尾。

-----BEGIN CERTIFICATE-----

MIIDuTCCAqGgAwIBAgIQO5hG2uC7G7ZBxcXt/J+z3TANBgkqhkiG9w0BAQsFADBv
MRMwEQYKCZImiZPyLGQBGRYDY29tMRwwGgYKCZImiZPyLGQBGRYMaW50ZXJzeXN0

ZW1zMRgwFgYKCZImiZPyLGQBGRYIaXJpc2xkYXAxIDAeBgNVBAMTF2lyaXNsZGFw
LUlSSVNMREFQREMxLUNBMB4XDTE4MDQwOTE0MDUzMloXDTIzMDQwOTE0MTUzMlow

bzETMBEGCgmSJomT8ixkARkWA2NvbTEcMBoGCgmSJomT8ixkARkWDGludGVyc3lz
dGVtczEYMBYGCgmSJomT8ixkARkWCGlyaXNsZGFwMSAwHgYDVQQDExdpcmlzbGRh
cC1JUklTTERBUERDMS1DQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB

AL/aNDJJNbzGh6tXG8+hmEEplb80UQMcIhLvoanz/RKKZXBBY68rO5pkYUwn/24g
pryGy0OUjA997KKol5rdbXWzK7vUMuVSp0atw1m4vF9hmp1bpKBC60OXmV39Fqar
ej1dkRl0ZXOmCexP8JqTyNwhpOLXvazzzvsNRr4ts9u1m6y9kFYecu4PRqtFCgoC
T6rbgqz1Ew3VrhQHi0HWvq1sR2CngxdyG8AnlSo6nz3X/IrTwrw5lauNLfpsRda5
D5YfUpxYeqpONSUB650u9bC0l5eRWe8kS33Xr+u5Odkhy087I/zN+GK7xMGzxYMR
OWNINIGRvlLuDRshKQl4gP0CAwEAAaNRME8wCwYDVR0PBAQDAgGGMA8GA1UdEwEB

/wQFMAMBAf8wHQYDVR0OBBYEFM3Ofv4R/zkEgHkp4ayvTkAvxJikMBAGCSsGAQQB
gjcVAQQDAgEAMA0GCSqGSIb3DQEBCwUAA4IBAQC8hhvc/+WsDeipNezBo+ovum2z
7q0fStr73Tj84cDGSyCmT2Q/h0qFvkfjtRd8AUBdG0qjhIB4VLVyWmrWDl1jAUcr
3AzygfO6UZjNRT+4c8r8R2xOhE3wJEJWibzXD9bPCtCkhYNJT6bi5PSRgUq+r9GU

探索 LDAP 用户和组

lHnAUmaQa+K+kNEpAvBfIeQ2ox9NPbtUfj/fswKpubWzZZc2udeU8SQLacl6tZMA
tXgZPT6lQfoZU2WmDG1EnoC4Ji1++Sf6Ho2i6kxg1m6geyOPSsGPdsAVjYCqCjuZ
pxjAsfZXV2juLyTBM51rrmV/Rqfougnikh4zhFRBrOHtMP71ZxCptMVz3RHe

-----END CERTIFICATE-----

3. 在您可以访问的目录中将该文件另存为 irisldap.cer。

0. 在 Windows 上安装安全证书

如果您在 Windows 上运行 InterSystems IRIS，请完成以下步骤来完成安装您所创建的安全证书的过程。

0. 使用 Windows 资源管理器（Explorer），双击在您保存文件的目录中的安全文件 irisldap.cer。
1. 点击 **Install Certificate（安装证书）**。
2. 选择 **Local Machine（本地机器）** 并点击 **Next（下一步）**。
3. 点击 **Yes（是）** 以允许对您的设备进行更改。
4. 选择 **Place all certificates in the following store（将所有证书放入以下存储区）**并点击 **Browse（浏览）**。
5. 选择 **Trusted Root Certification Authorities（受信任的根证书颁发机构）**并点击 **OK（确定）**。
6. 点击 **Next（下一步）**。
7. 点击 **Finish（完成）**。

0. **在 UNIX® 上安装安全证书**

如果您在 UNIX® 上运行 InterSystems IRIS，请完成以下步骤来完成安装您所创建的安全证书的过程。

0. 以 system 用户身份登录管理门户（Management Portal）时，进入 **Security LDAP Configurations（安全 LDAP 配置）** 页面 (**System Administration（系统管理） > Security（安全） > System Security（系统安全） > LDAP Configurations（LDAP 配置）**)。
1. 从 LDAP 配置的列表中点击 **irisldap.com**。
2. 在 **TLS/SSL certificate file（TLS/SSL 证书文件）**字段中，输入 irisldap.cer 的路径和文件名，这是您创建并保存的文件。

探索 LDAP 用户和组

现在您已经配置了您的 LDAP 连接并启用了 LDAP 身份验证，您可以使用 LDAP 服务器来登录 InterSystems IRIS。LDAP 服务器包含三个用户：user1、user2 和 user3。user1 属于 intersystems-Role-%Operator 组，user2 属于 intersystems-Role-%Manager 组，user3 属于 intersystems-Role-%Developer 组。每个组都授予属于 InterSystems IRIS 中相应角色的权限。例如，当 user1 通过 LDAP 服务器的身份验证成功时，将为其分配 **%Operator** 角色。

在本教程中，您将以所有三个用户的身份登录到 InterSystems IRIS，并根据与用户关联的角色探索可用的操作。当您作为一个有效的 LDAP 用户登录到 InterSystems IRIS 时，InterSystems IRIS 会自动创建用户，而不需要您事先手动添加用户。

User1: 操作员

要以 user1 的身份登录并探索 InterSystems IRIS：

0. 如果您目前已登录到 InterSystems IRIS，请点击管理门户（Management Portal）左上角的 **Logout（退出）**链接。

探索 LDAP 用户和组

2. 使用以下凭证登录 InterSystems IRIS：

用户名：user1

密码：Password1

user1 是 intersystems-Role-%Operator 组的成员。基于这个组，当 user1 通过身份验证时，他们会被自动授予与 InterSystems IRIS 中 **%Operator** 角色相关的权限。

3. 从管理门户（Management Portal）主页，进入 **Databases（数据库）** 页面 (**System Operation（系统操作）> Databases（数据库）**)。user1 可以访问这个页面，因为他们已经被 LDAP 服务器授权，可以和与 **%Operator** 角色关联的页面进行交互。
4. 在管理门户（Management Portal）主页上，请注意 **System Administration（系统管理）** 菜单已被禁用。user1 不能访问此菜单，因为 **%Operator** 角色不包含适当的权限。

0. User2: 管理者

要以 user2 的身份登录并探索 InterSystems IRIS：

0. 点击管理门户（Management Portal）左上角的 **Logout（退出）** 链接。
1. 使用以下凭证登录 InterSystems IRIS：

用户名：user2

密码：Password2

user2 是 intersystems-Role-%Manager 组的成员。基于这个组，当 user2 通过身份验证时，他们会被自动授予与 **%Manager** 角色相关的权限。正如您将看到的，这些权限包括访问 user1 无法看到的页面。

3. 从管理门户（Management Portal）主页，进入 **Users（用户）** 页面 (**System Administration（系统管理）> Security（安全）> Users（用户）**)。请记住，user1 不能访问 **System Administration（系统管理）** 菜单。
4. 从用户列表中点击 user1。
5. 点击 **Roles（角色）** 标签。

请注意，**%Operator** 是分配给 user1 的唯一角色。

6. 点击 **Cancel（取消）** 以返回到 **Users（用户）** 页面。
7. 请注意，在用户列表中没有 user3 的条目。该用户将在 user3 登录时自动创建，此时 InterSystems IRIS 使用 LDAP 服务器对用户进行身份验证。

0. User3: 开发者

要以 user3 的身份登录并探索 InterSystems IRIS：

0. 点击管理门户（Management Portal）左上角的 **Logout（退出）**链接。
1. 使用以下凭证登录 InterSystems IRIS：

用户名：user3

密码：Password3

user3 是 intersystems-Role-%Developer 组的成员。基于这个组，当 user3 通过身份验证时，他们会被自动授予与 **%Developer** 角色相关的权限。

3. 请注意，该用户可以访问 **System Explorer（系统资源管理器）**菜单，而不是 **System Operation（系统操作）**和 **System Administration（系统管理）**菜单。您可以看出，分配给 user3 的 **%Developer** 角色与分配给

   了解有关 LDAP 和安全的更多信息

   user1 和 user2 的角色具有不同的权限。这可以防止 user3 看到自己的用户配置文件，因为 **Users（用户）**页面是在 **System Administration（系统管理）**菜单下。

自动创建用户

您已经登录到 InterSystems IRIS，但没有先创建新用户。当在 LDAP 服务器上发现这些用户时，InterSystems IRIS 会自动创建这些用户。下面的程序演示了这个过程：

0. 点击管理门户（Management Portal）左上角的 **Logout（退出）**链接。
1. 使用以下凭证登录 InterSystems IRIS：

用户名：user2

密码：Password2

请记住，user2 拥有 **%Manager** 角色。

3. 从管理门户（Management Portal）主页，进入 **Users（用户）** 页面 (**System Administration（系统管理） > Security（安全） > Users（用户）**)。
4. 在列表中找到 user3 并点击行中的 **Delete（删除）**。

   此时，拥有 **%Developer** 角色的 user3 在 InterSystems IRIS 中不复存在。

5. 点击管理门户（Management Portal）左上角的 **Logout（退出）**链接。
6. 使用以下凭证登录 InterSystems IRIS：

用户名：user3

密码：Password3

因为 user3 仍然存在于 LDAP 服务器上，所以即使您刚刚在 InterSystems IRIS 中删除了用户帐户，您也能够以 user3 的身份重新登录到 InterSystems IRIS。

7. 如果需要，您可以重新登录 InterSystems IRIS，以确认 user3 现在是一个用户。 a. 点击管理门户（Management Portal）左上角的 **Logout（退出）**链接。 b. 使用以下凭证登录 InterSystems IRIS：

   用户名：user2

   密码：Password2

c. 从管理门户（Management Portal）主页，进入 **System Administration（系统管理） > Security（安全） > Users（用户）**。user3 现在在列表中，尽管您之前删除了该用户账户。

了解有关 LDAP 和安全的更多信息

您可以使用以下参考资料来了解有关 LDAP 和其他安全概念的更多信息。

- 有关在 InterSystems IRIS 中使用 LDAP 的详细信息，请参见 LDAP Guide（《LDAP 指南》）。
- 有关 InterSystems IRIS 中基于角色的安全的介绍，请参见 First Look:Role-Based Access Control（《技术概要：基于角色的访问控制》）。

#新手 #InterSystems IRIS
