文章
Qiao Peng · 四月 11, 2022 阅读大约需 8 分钟

InterSystems 数据平台与三级等保 - 第一篇

数据平台不仅要安全，还要合规，三级等保是我们要符合的主要安全规范。InterSystems的数据平台和集成平台产品都和三级等保有关。如果没有正确配置它们的安全选项，就会影响到整个系统的安全，影响到合规性。

在生产环境上，如何配置安全的InterSystems的数据平台，并达到三级等保的要求？

这个系列文章，针对InterSystems数据平台的安全架构，围绕对三级等保的合规性展开，介绍如何配置出一个安全、合规的数据平台。

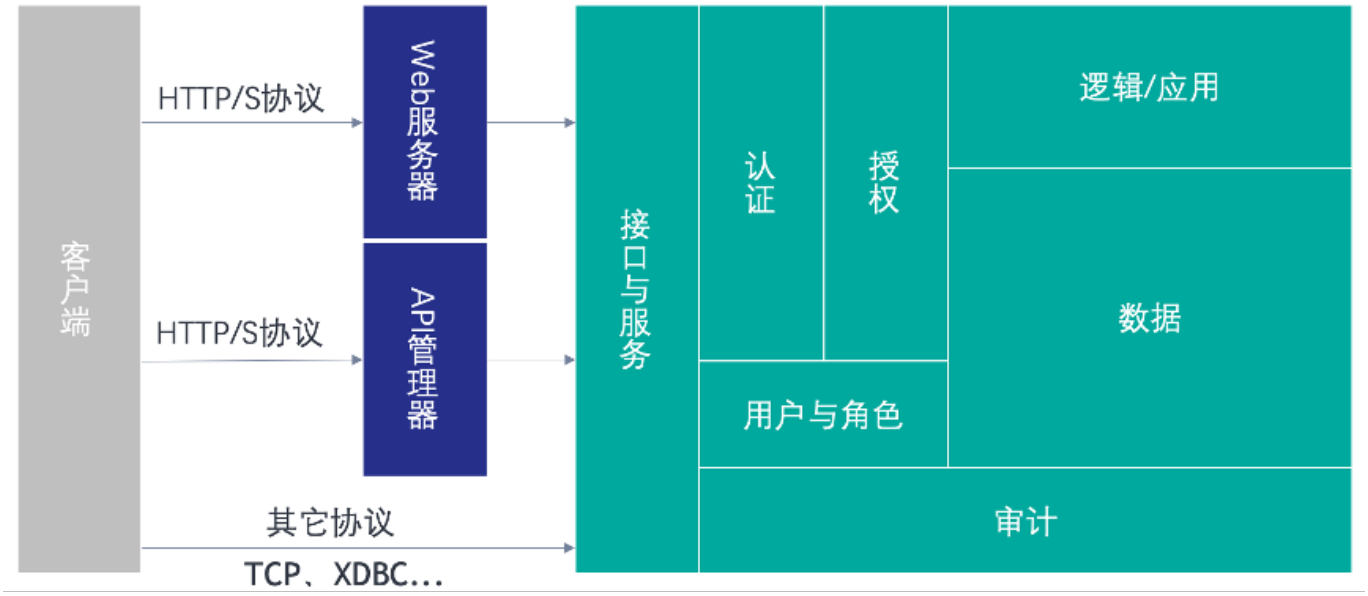
注：本文提到的InterSystems的数据平台，包括*Caché数据库*、*Ensemble集成平台*、*HealthConnect医疗版集成平台*和*InterSystems IRIS数据平台*。

三级等保的要求

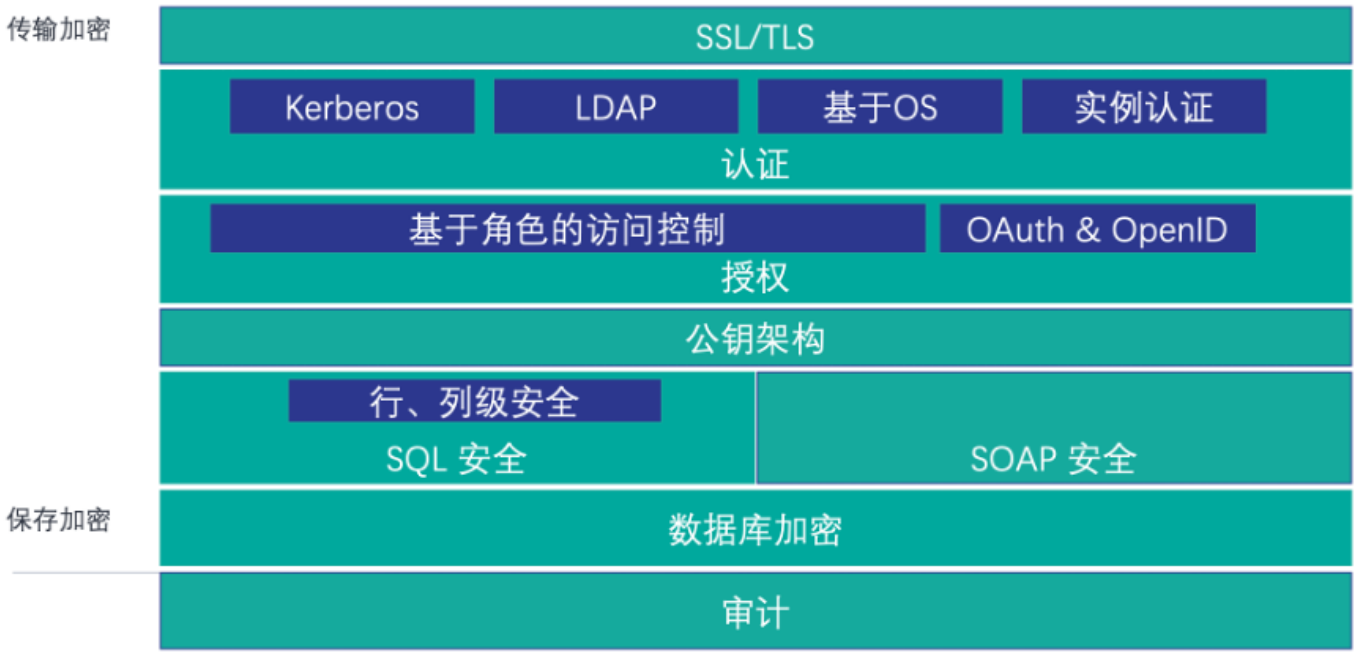
三级等保要求	对数据平台的要求
身份鉴别	确保用户身份是真实、准确的
访问控制	控制：谁、以什么方式、从什么设备可以访问什么数据和功
入侵防范	防范静态数据、传输中的数据、日志和备份中的数据被入侵
恶意代码防范	防止恶意代码被植入和执行，例如SQL注入
可信验证	
数据完整性	保证数据完整性和一致性的能力
数据备份恢复	对数据的备份与恢复能力和策略

InterSystems数据平台安全架构

InterSystems数据平台提供了一个完善的安全架构，用以保护从接入到数据保存的各个层面的数据安全：

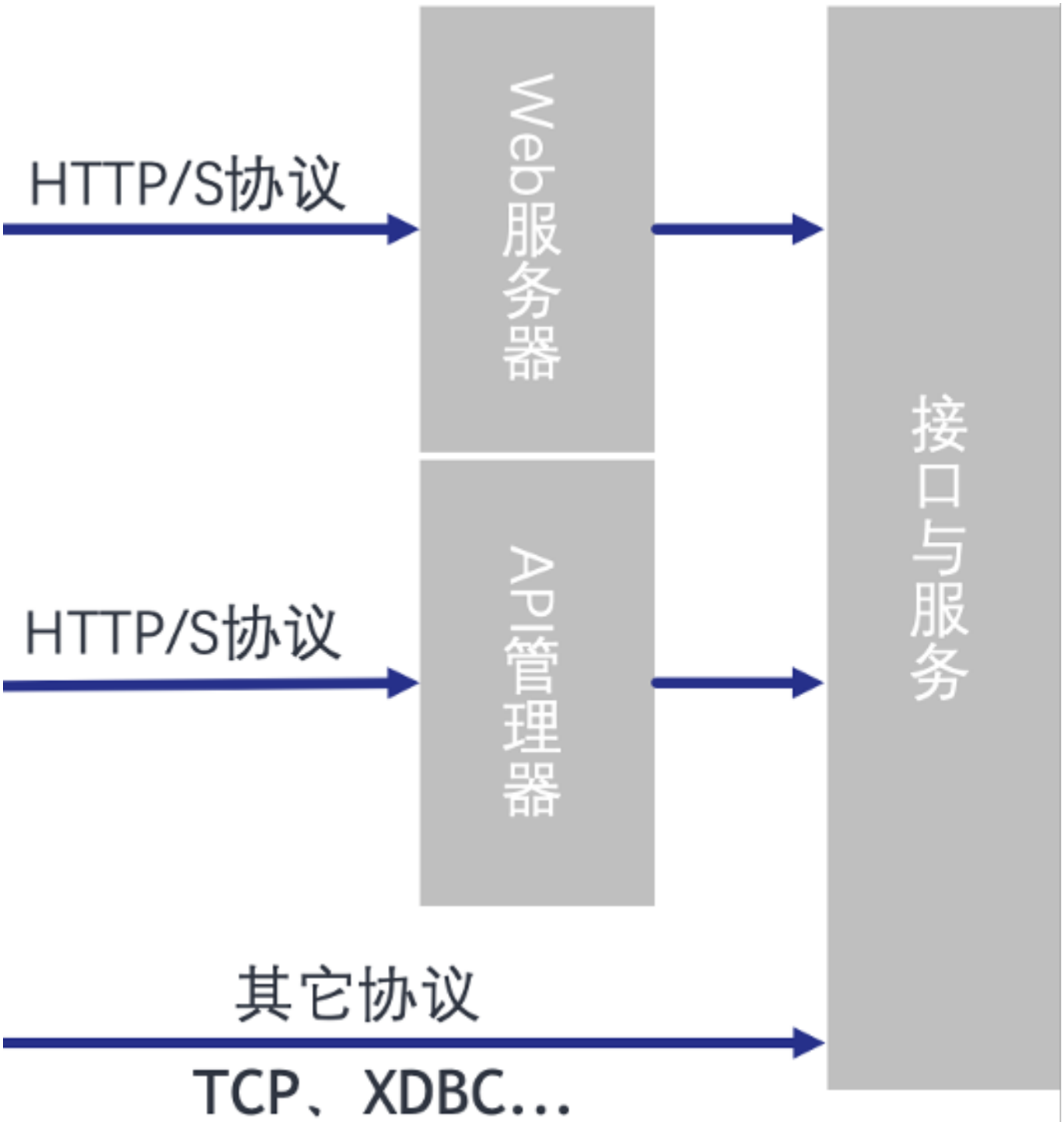


InterSystems数据平台提供丰富的安全相关特性，用以保障系统安全性和合规性：



我们按数据的流向逐一展开，看看应该如何加强InterSystems数据平台的安全。

1. InterSystems数据平台连接通道安全



客户端可以使用多种技术连接到InterSystems数据平台，包括ODBC/JDBC、Java、.net、TCP、Telnet、HTTP、SOAP、REST等。除了客户端的连接，InterSystems数据平台之间也有很多连接通道，例如高可用镜像成员之间、数据平台和Web网关之间…
这些连接通道都应该考虑使用SSL/TLS进行通讯加密，从而保护数据的安全和一致性。

1.1配置InterSystems数据平台的超级服务器接入通道加密

除了通过HTTP、SOAP、REST之外的客户端，其它的客户端都连接到InterSystems数据平台的超级服务器。InterSystems数据平台在系统范围内使用SSL/TLS协议为超级服务器端口通道加密。

配置步骤如下：

1. 在管理门户中，通过路径 ***系统 > 安全管理 > SSL/TLS 配置***，建立名为**%SuperServer**的SSL/TLS配置项。参考文档
2. 在管理门户中，通过路径 ***系统 > 安全管理 > SSL/TLS 配置***，在***超级服务器SSL/TLS支持***选项上选中“ 要求 ”。它的三个选项分别为：

禁用（默认选项）- 拒绝使用TLS的客户端连接

启用 - 允许使用TLS的客户端连接，但不必要

要求 – 仅接受使用TLS的客户端连接

如果Telnet也要通过T
LS加密传输，将上面配置的基础上，再建立
一个名为**%TELNET/SSL**的SSL/TLS配置项，然后将上图的***Telnet server SSL/TLS support***
设置为 **要求** ”。具体配置

1.2 配置客户端使用SSL/TLS连接到InterSystems数据平台的超级服务器

不同的客户端技术配置SSL/TLS的方式不同，具体的配置详见：

Java

.net

ODBC/Studio/Windows Terminal

Windows配置

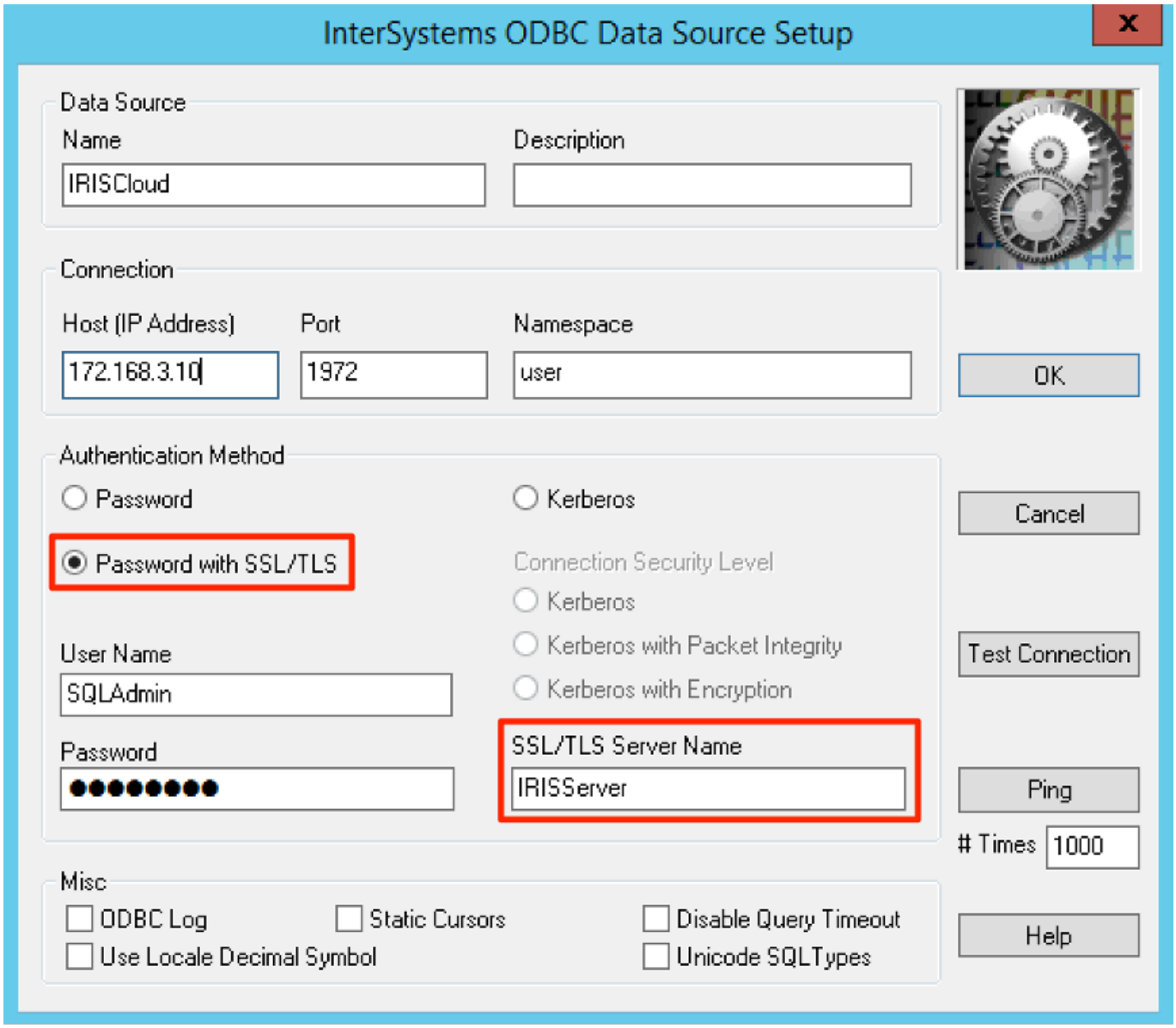
这里以ODBC为例，看看Windows客户端上ODBC设置的步骤：

1. 在Windows客户端上下载IRIS服务器上的CA证书文件，并保存在指定目录。例如：c:\InterSystems\certificates\certificateSQLaaS.pem

2. 在Windows客户端上编辑并保存C:\Program Files (x86)\Common Files\InterSystems\IRIS\SSLDefs.ini，其中***[IRISServer]***是你起的SSL/TLS配置名，后面的***Address***和***Port***是InterSystems数据平台的服务器地址和超级服务器端口号。***[TLSConfig]***是SSL/TLS的配置项，注意其中的***CAfile***是第一步得到的CA证书文件路径。

```
[IRISServer]

Address=172.168.3.10

Port=1972

SSLConfig=TLSConfig

[TLSConfig]

TLSMinVersion=16

TLSMaxVersion=32

CipherList=ALL:!aNULL:!eNULL:!EXP:!SSLv2

Ciphersuites=TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA2
56

KeyType=2

VerifyPeer=1

Password=

CAfile=c:\InterSystems\certificates\certificateSQLaaS.pem
```

3. 配置Windows的ODBC DSN，选中 “ Password with SSL/TLS", 并在 “ SSL/TLS Server Name ” 中填写SSLDefs.ini中特定的配置名，例如 IRISServer



之后ODBC客户端就可以使用这个DSN通过TLS加密传输连接到InterSystems数据平台了。

1.3 安全建议

虽然不是三级等保必须的，建议配置和开启InterSystems数据平台的超级服务器SSL/TLS连接。

2. Web服务器

InterSystems数据平台在安装时，可以选择安装一个私有的Apache，用于访问管理门户和基于HTTP的开发、测试，例如网页应用、SOAP和RESTful API。

这个私有Apache并不是全功能的，因此不应作为生产环境的Web服务器，尤其是生产环境有基于HTTP的服务、应用或接口时。这时，应该部署独立的Web服务器和InterSystems Web网关，连接到InterSystems的数据平台。并且应该配置HTTPS，而非使用无加密的HTTP。

InterSystems的数据平台支持Apache、IIS和Nginx等Web服务器。

2.1 独立Web服务器的配置

如何配置独立的Web服务器和InterSystems Web网关，如何配置Web服务器的HTTPS？请参考这篇非常棒的社区系列文章：

WebGateway系列

2.2 安全建议

1. 生产环境上，部署独立的Web服务器，而非使用InterSystems 数据平台的私有Web服务器。
2. Web服务器应使用HTTPS，而非HTTP，提供Web服务。

3. 服务与接口

InterSystems 数据平台提供一系列服务和接口，用于各种外部系统和技术的接入，例如常见的ODBC/JDBC的SQL客户端、开发者使用的Studio、管理员常用的Telnet。另外，InterSystems数据平台组件和实例之间的连接也是通过服务实现的，例如Web网关和InterSystems数据平台之间的连接、配置为镜像高可用的多台InterSystems数据平台之间的连接。

3.1 InterSystems数据平台的服务

下表列出了InterSystems数据平台的服务和它们服务的对象：

服务名称	描述
%ServiceBindings	控制 SQL 或对象访问方式，包括Studio、XDBC客户端、Java、
%ServiceCacheDirect	控制 Caché 直连访问方式
%ServiceCallIn	控制使用CallIn的C/C++应用的访问
%ServiceComPort	控制从Windows系统COM端口的访问
%ServiceConsole	控制Windows本地服务器上 CTERM (TRM:pid) 和 Windows 控制

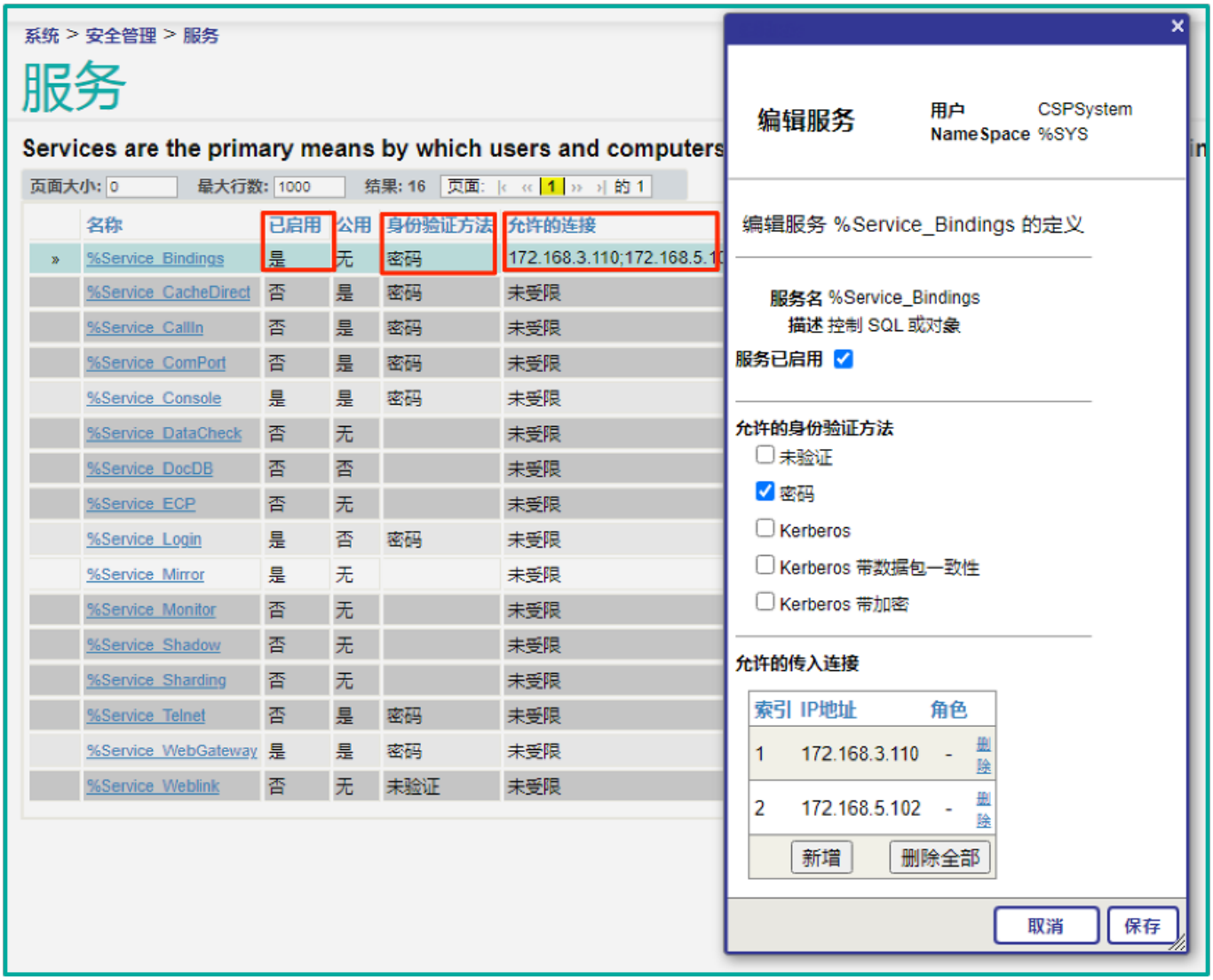
%ServiceTerminal	控制UNIX, Linux, Mac本地服务器上的控制台访问
%ServiceDataCheck	控制实例间数据一致性检查DataCheck时，作为数据源的访问
%ServiceDocDB	控制文档数据库的访问
%ServiceECP	控制是否ECP
%ServiceLogin	控制通过 SYSTEM.Security.Login的登录访问
%ServiceMirror	控制镜像成员访问
%ServiceMonitor	控制 SNMP 和远程监视命令
%ServiceShadow	控制此系统是否可以是shadow来源
%ServiceSharding	控制是否可以作为分片服务器访问
%ServiceTelnet	控制来自于Windows 服务器的本地或远程Telnet 会话访问
%ServiceCSP %ServiceWebGateway	%ServiceCSP （Caché/Ensemble）或%ServiceWebGateway
%ServiceWeblink	控制旧有的WebLink应用访问

3.2 InterSystems数据平台服务的安全选项

这些向外开放的服务和接口有多种机制保护安全：

1. 是否启用
2. 是否是公用服务（意味着所有用户都有权限）
3. 身份认证的方式
4. 接入客户端的IP限制
5. 其它特殊限制

在管理门户>系统>安全管理>服务，可以对每一项服务进行单独的安全配置：



3.3 安全建议

1. 关闭不必要的服务。
2. 对开启的服务，应选择安全的认证方式，不应使用“ 未验证 ”方式。
3. 进一步限定允许接入的客户端IP地址。

4. 用户认证

用户认证是保障数据安全的核心之一。

4.1 InterSystems数据平台的用户认证机制

InterSystems数据平台支持多种用户认证机制，包括：

- Kerberos

- 基于操作系统的认证
- IRIS用户名/密码
- LDAP
- 代理认证 – 用户自定义认证
- 无认证 – 无需用户认证，进来的用户自动为UnknownUser
- 二阶段认证

它同时可以开启和使用多种用户认证，允许用户使用不同的认证方式接入数据平台。在启用多种用户认证机制时，InterSystems数据平台会以一定优先顺序来应用用户认证机制：

- Kerberos > 基于操作系统的认证 > IRIS用户名/密码 >无认证
- LDAP > 代理认证 >无认证

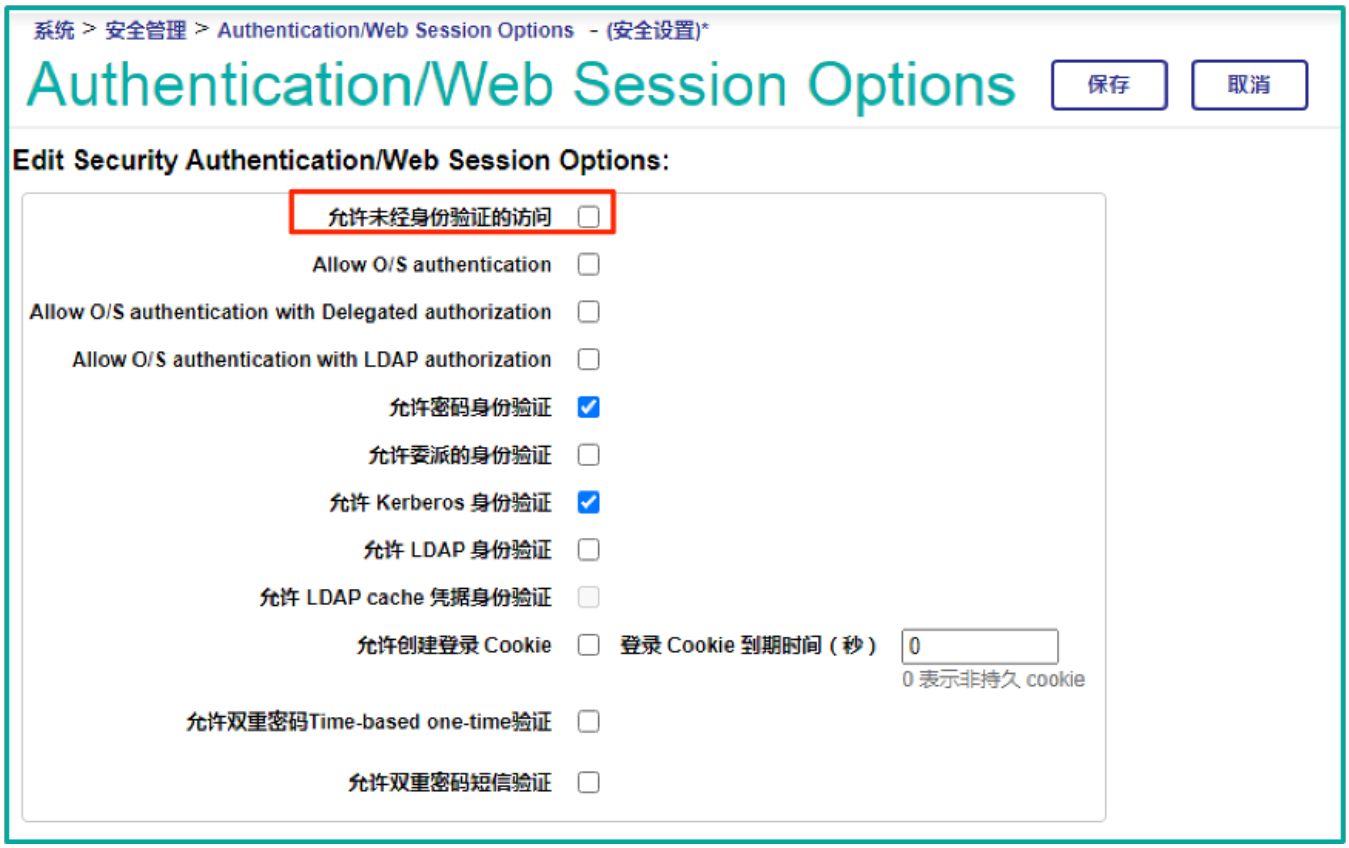
4.2 用户认证方式的设置

这些用户认证方式，可以在系统层面开启或禁用，也可以在服务/接口层面进行选择。对于InterSystems数据平台提供的Web应用，例如网页应用、SOAP服务和RESTful API，还可以在Web应用层面进行用户认证方式的配置。

系统层面的配置，在管理门户>系统>安全管理>Authentication/Web Session Options ；

服务层面的配置，见3.2；

应用层面的配置，将在后面的应用安全章节详细介绍。



4.3 安全建议

1. 系统级禁用“ 无认证 ”，和其它不需要使用的认证方式
2. 系统级，采用更安全的认证方式

5. 用户授权

InterSystems
数据平台提供一套基于角色的权限控制机制，它可以保障细颗粒度的数据与服务安全。

5.1基于角色的权限控制机制

在这套机制下，被保护的数据与服务被称之为***资产***。***资产***
可以是任何具体事物，例如数据库、服务、平台应用、管理工具，甚至可以是抽象的事物，例如工作身份、“ 对患者联系方式的权限 ”。

权限控制机制是：

1. InterSystems数据平台定义***资源***，对应一个或多个***资产***
   ；系统已经定义了一系列系统资源，同时用户可以自定义资源。
2. 对***资源***的许可，例如读、写、使用，就是权限；
3. 将权限分配给InterSystems数据平台定义的角色和/或用户；
4. 用户就具有了相应的资产权限。

5.2资源的权限配置

通过管理门户>系统>安全管理>资源，管理可以创建新资源、配置已有资源的权限。

以%开头的资源是系统已经创建好的资源，例如：

- **%Admin*_** 是工作身份资源
- **%DB*_** 是数据库资源
- **%Service*_** 是服务资源
- **%Ens*_** 是互操作相关的资源

其中，对资源的权限可以被设置为“ 公有权限 ”，即所有用户都有相应的权限。

5.3 安全建议

1. 用户自定义的数据库应该设置自己独立的资源，而非使用%DB%DEFAULT
2. 谨慎使用公共权限
3. 创建自己需要保护的新资源

#安全 #Caché #Ensemble #HealthShare #InterSystems IRIS #InterSystems IRIS for Health

---

源
URL:
https://cn.community.intersystems.com/post/intersystems-%E6%95%B0%E6%8D%AE%E5%B9%B3%E5%8F%B0%E4%B8%8E%E4%B8%89%E7%BA%A7%E7%AD%89%E4%BF%9D-%E7%AC%AC%E4%B8%80%E7%AF%87