文章
Louis Lu · 十一月 2, 2021 阅读大约需 11 分钟

IRIS 2021 技术文档 First Look 25 -- 数据库加密

本文档向您介绍 InterSystems IRIS®数据平台如何处理数据库加密，这是所有企业安全战略的重要组成部分。

本文档介绍了数据库加密的情况，并引导您完成一些与创建加密数据库有关的初始任务。一旦您完成了本指南，您将创建一个密钥文件，激活该密钥文件，然后用它来加密一个数据库。这些活动被设计成只使用默认的设置和功能，这样您就可以熟悉该功能的基本原理，而不必处理那些离题的细节（尽管这些细节在执行实现时可能很重要）。有关数据库加密的完整文档，请参见 *Encryption Guide（《加密指南》）*。

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》）。

1. 为什么数据库加密很重要

虽然加密并不能防止对机密或个人信息的所有不当或未经授权的使用或披露，但确保静止数据的加密为信息安全提供了一个重要的防御层。在数据库级别实施加密为您的信息保护控制提供了一个额外的维度。

此外，许多有关敏感信息或个人信息的法律和法规建议或要求处理数据的组织采用加密作为第一道防线。这些包括法律和法规，如：

- 《健康保险携带和责任法案》（Health Insurance Portability and Accountability Act，HIPAA ）——要求安全保护健康（Secure Protected Health）信息是不可读、不可破译和不可恢复的
- 马萨诸塞州 201 《马萨诸塞州法规法典》(Code of Massachusetts Regulations，CMR) 17.00——要求个人信息在传输和静止时进行加密
- 纽约州 23 《纽约法典、规则和条例》 (NewYork Codes, Rules and Regulations，NYCRR) 500 部分——处理非公开信息的金融和其他涉及的组织必须利用加密作为保护数据的一种手段。
- 欧盟《通用数据保护条例》（General Data Protection Regulation，GDPR）——安全保障要求将加密作为一种保护控制考虑在内
- 意大利《个人数据保护法》（Personal Data Protection Code，PDPC）——《最低数据安全措施技术规范》（Technical Specifications on Minimum Data Security Measures）第 24 条要求对披露健康和性生活的数据进行加密处理
- 澳大利亚隐私原则（Australian Privacy Principles，APP）原则 4——强有力的加密实现解决了必要的隐私增强技术，以确保个人信息的安全
- 日本经济产业省（Ministry of Economy, Trade, and Industry，METI ）指南——如果未加密的个人或机密信息遭到泄露，必须进行监管调查，因为根据《个人信息保护法》（Act on the Protection of Personal Information，APPI）第 20 条，个人信息的处理者有义务防止信息的泄漏、丢失或损坏

请注意，这些法律要求中有许多集中在数据泄露上，因为这是一种越来越普遍的现象，但目前的框架要求组织有义务通过适当的安全控制来解决风险，如基于角色的访问、密码保护、入侵检测、数据丢失预防和日志/审计——以及加密。加密本身并不能满足所有的强制性要求，但提供了一个安全的基础。数据库级别的加密

通过要求攻击者不仅要获得对系统或文件空间的访问权限，而且要有访问数据库的权限，从而加强了保护。这一附加层为组织、其客户和任何利益相关者提供了保证。

2. InterSystems IRIS 如何使用数据库加密

对于与数据库操作相关的活动，InterSystems IRIS
的
加密
和解密过
程对用户是透明的
。从终端用户或应用程序开发人员的
角度来看，应用程序只需执行其常规活动（activity
），数据就会自动在磁盘上加密。从系统管理员的角度来看，有几个简单的任务可以确保数据加密的发生；在执行这些任务后，加密的过程又是在背后执行的。

更重要的是，这些活动使用最少的处理器时间，所以它们对您的应用程序没有明显的影响。此外，由于我们数据库的构建方式，这些活动被高度优化。

加密和解密在密码块链接（Cipher Block Chaining，CBC）模式中使用美国政府高级加密标准（United States Government Advanced Encryption Standard，AES），通常简称为 AES CBC。InterSystems IRIS 支持 AES CBC 的所有合法密钥大小：128–、192–和 256–位密钥。

InterSystems IRIS 使用最快的可用实现（available
implementation
）执行加密和解密。只要有可能，加密和解密就会利用基于处理器的指令集及其固有的效率。现代英特尔（Modern Intel）和 IBM POWER8 处理器都有这样的指令。InterSystems IRIS
自动检测并使用这些指令，所以您不需
要采取任何行动来实现它。在英特尔（Intel）处理器上，这些是高级加密标准新指令（Advanced Encryption Standard New Instructions，AES-NI）；在 IBM 上，它们是 AES VMX 指令集。

您可以将数据库加密密钥存储在支持密钥管理互通协议（key management interoperability
protocol，KMIP）的密钥管理服务器上，或者存储在包含数据库密钥加密副本的文件中。每个都有自己的优势：

- KMIP 是一个 OASIS
  标准协议，用于客户端与密钥管理系统通信。KMIP
  服务器可以是专门的硬件设备，或是运行密钥管理软件的通用服务器。
- 当数据库加密密钥存储在文件中时，InterSystems 使用多层 AES
  密钥封装算法对密钥进行加密，并使用 PBKDF2
  算法派生出单个管理员密钥加密密钥，从而使字典攻击和暴力破解变得不切实际。

必须记住，虽然数据库加密是安全策略的一个组成部分，但它不能单独解决安全漏洞。其他工具，如动态数据保护，也是至关重要的。这就是为什么数据库加密是 InterSystems IRIS
为保护数据而提供的一整套工具的一部分。这些包括：

- 支持政府标准——您可以将 InterSystems IRIS 配置为使用经过验证符合联邦信息处理标准 140–2（Federal Information Processing Standards 140–2，FIPS 140-2）的库进行数据库加密。这在 Red Hat
  Linux 上是可用的。
- 保护选定的数据元素——被称为数据元素加密，该功能提供了一种编程方法，允许您只对记录的选定部分进行加密，如信用卡或身份识别号码。
- 保护动态数据——InterSystems IRIS 使用最新版本的传输层安全协议（Transport-Layer
  Security，TLS）保护动态数据。TLS 是保护数据通信的行业标准协议。
- 支持第三方授权——InterSystems
  IRIS 支持在第三方网站上使用资源的授权，就像在 web 上经常看到的通过
  QQ 或微信登录以使用一个网站。这是通过开放授权框架（Open Authorization
  Framework）2.0 版（称为 OAuth 2.0）实现的，并可能包括通过另一层，称为 OpenID 连接（OpenID Connect）进行身份验证。

3. 亲自尝试数据库加密

使用 InterSystems IRIS 数据库加密很容易。这个简单的程序将引导您完成设置加密数据库的基本步骤。

用前须知

要使用该程序，您需要一个运行中的 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。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）。

创建加密密钥

首先，创建一个密钥文件，其中自动包含一个数据库加密密钥：

1. 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）。
2. 导航到 **Create Encryption Key File（创建加密密钥文件）** 页面(**System Administration（系统管理）** > **Encryption（加密）** > **Create New Encryption Key File（创建新的加密密钥文件）**)：

3. 在 **Create Encryption Key File（创建加密密钥文件）** 页面上：
   a. 在 **Key File（密钥文件）** 字段中，输入密钥文件的名称和路径。当您点击 **Browse（浏览）** 按钮时，文件选择对话框（File Selection Dialog） 默认在实例的 *install-dir*/mgr 目录中打开（其中 *install-dir* 是 InterSystems IRIS 安装目录），例如，C:\InterSystems\IRIS\mgr\testkeys.key

；您可以在所有类型的实例上使用此目录，或者在主机或容器文件系统中选择另一个位置。

b. 在 **Administrator Name（管理员名称）**、**Password（密码）**和 **Confirm Password（确认密码）**字段中，输入值如 testadmin 和 password。这只是一个示例，所以不要重复使用您在开发环境中使用的密码。

c. 选择靠近页面顶部的 **Save（保存）** 按钮。

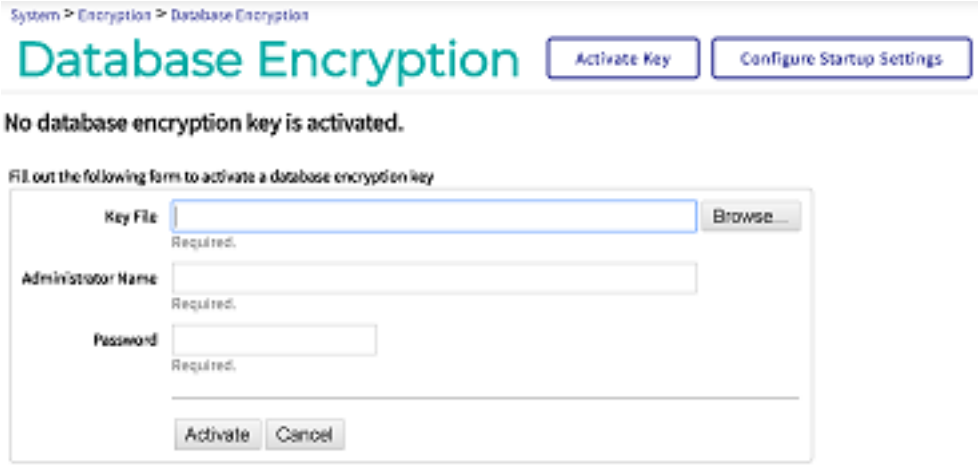
您刚刚在 C:\InterSystems\directory 里创建了 testkeys.key
密钥文件，其中有一个密钥，您可以用它来进行数据库加密。InterSystems IRIS 会显示一条带有密钥的信息，如

有关创建密钥文件及其初始密钥的详细信息，请参见 Create a Key File（《创建密钥文件》）。

激活加密密钥

接下来，激活您刚刚创建的密钥：

1. 在管理门户（Management Portal）中，进入 **Database Encryption（数据库加密）**页面(**System Administration（系统管理）** > **Encryption（加密）** > **Database Encryption（数据库加密）**)。
2. 在数据库加密（Database Encryption）页面，选择 **Activate Key（激活密钥）** 按钮：



3. 在 **Key File（密钥文件）** 字段中，输入您创建的密钥文件的位置，如 C:\InterSystems\IRIS\mgr\testkeys.key。
4. 在 **Administration Name（管理员名称）** 和 **Password（密码）** 字段中，输入您指定的值(testadmin和 password)。
5. 选择 **Activate（激活）** 按钮。

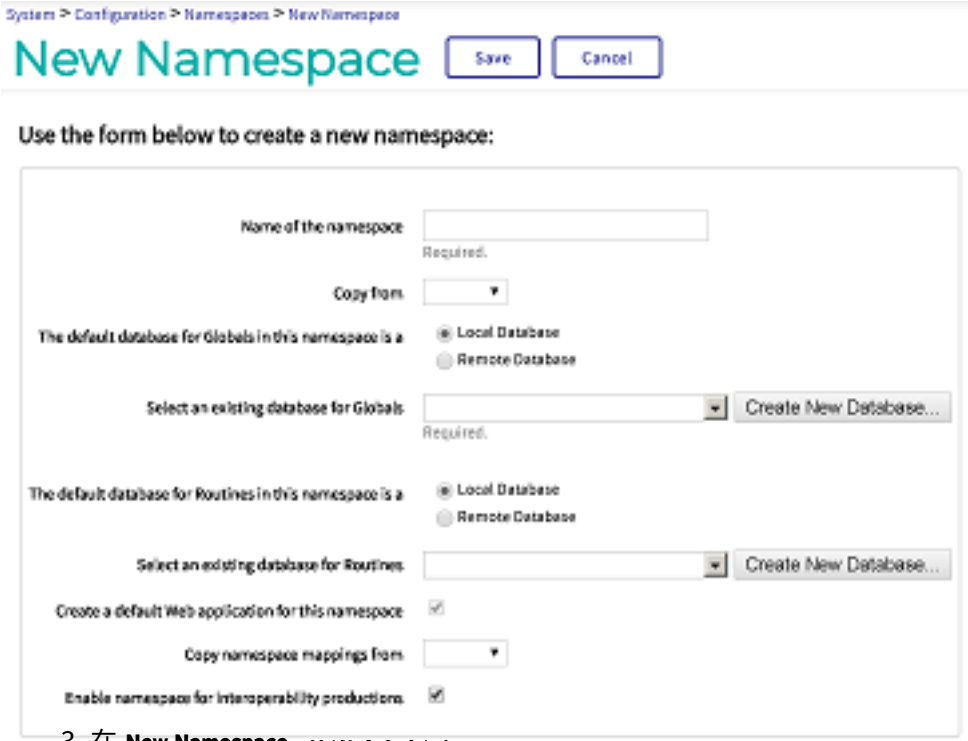
您可以在这个页面上看到密钥 ID：

有关激活密钥的详细信息，请参见 Activate a Database Encryption Key from a Key File（《从密钥文件中激活数据库加密密钥》）。

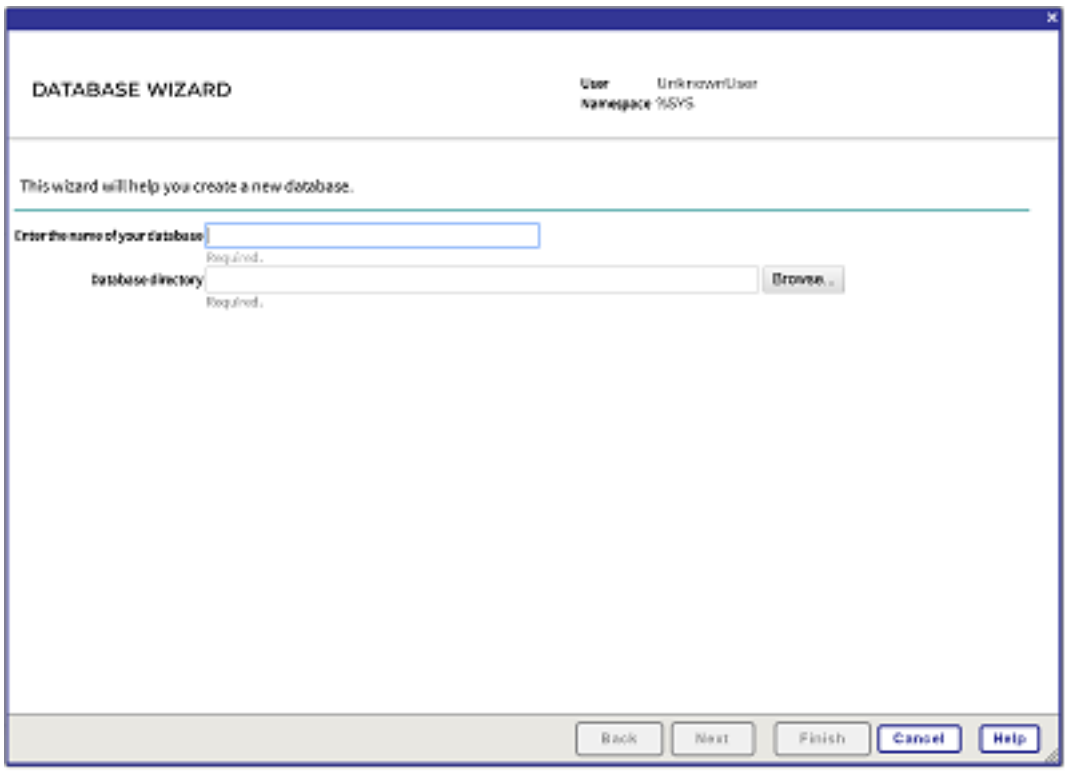
创建加密数据库

现在，您可以创建一个加密数据库：

1. 再次在管理门户（Management Portal）中，进入 **Namespaces（命名空间）** 页面(**System Administration（系统管理）** > **Configuration（配置）** > **System Configuration（系统配置）** > **Namespaces（命名空间）**)。
2. 在 **Namespaces（命名空间）** 页面上，选择 **Create New Namespace（创建新的命名空间）**。这将显示 **New Namespace（新的命名空间）** 页面：



3. 在 **New Namespace（新的命名空间）** 页面，输入您要创建的加密数据库的名称，如 **ENCDB**。
4. 在 **Select an existing database for Globals（为 Globals 选择现有的数据库）** 下拉菜单旁边，选择 **Create New Database（创建新的数据库）** 按钮。这将显示 **Database Wizard（数据库向导）**：



5. 在 **Database Wizard（数据库向导）** 的第一页，在 **Enter the name of your database（输入您的数据库名称）** 字段中，输入您要创建的数据库的名称，如 **ENCDB**。输入一个数据库的目录，如 C:\InterSystems\IRISmgr\ENCDB。在该页面上，选择 **Next（下一步）**。
6. 在下一页，将 **Encrypt database（加密数据库）** 的值从 No 更改为 Yes。在该页面上，选择 **Finish（完成）**。
7. 回到 **New Namespace（新的命名空间）** 页面，在 **Select an existing database for Routines（为例程选择现有的数据库）** 下拉菜单中，选择您刚刚创建的数据库，如 **ENCDB**。
8. 选择靠近页面顶部的 **Save（保存）** 按钮，然后在生成的日志的末尾选择 **Close（关闭）**。

现在您已经创建了一个名为 **ENCDB** 的加密数据库，它使用 InterSystems IRIS 在您创建密钥文件时创建的密钥。您可以像使用未加密的数据库一样使用这个数据库。由于 InterSystems IRIS 隐藏了所有的加密和解密机制，您可以用通常的方式执行所有的操作，所有数据都会被加密。

有关创建命名空间及其相关数据库的更多详细信息，请参见 *InterSystems IRIS System Administration Guide*（《*InterSystems IRIS 系统管理指南*》）中"Configuring InterSystems IRIS（配置 InterSystems IRIS）"一章中的 "Create/Modify a Namespace（创建/修改命名空间）"。有关背景信息, 请参见 *Orientation Guide for Server-Side Programming*（《*服务器端编程指导手册*》）中的 "Namespaces and Databases（命名空间和数据库）"。

查看加密数据

一旦您创建了加密数据库，您可以像使用其他未加密的数据库一样使用它。唯一的区别是数据的存储方式。要查看存储在加密数据库和未加密数据库中的数据的区别，您可以执行以下简单的测试：

1. 使用 *InterSystems IRIS Basics：Connecting an IDE*（《*InterSystems*

IRIS 基础：连接一个 IDE》）中为您的实例描述的程序，为您的 InterSystems IRIS 实例打开终端（Terminal）。

2. 使用以下命令切换到加密数据库的命名空间：

```
%SYS>set $namespace="ENCDB" ENCDB>
```

3. 在 **ENCDB** 命名空间中，运行以下命令：

```
ENCDB>for i=1:1:1000 set ^x(i)="This is test number "_i
```

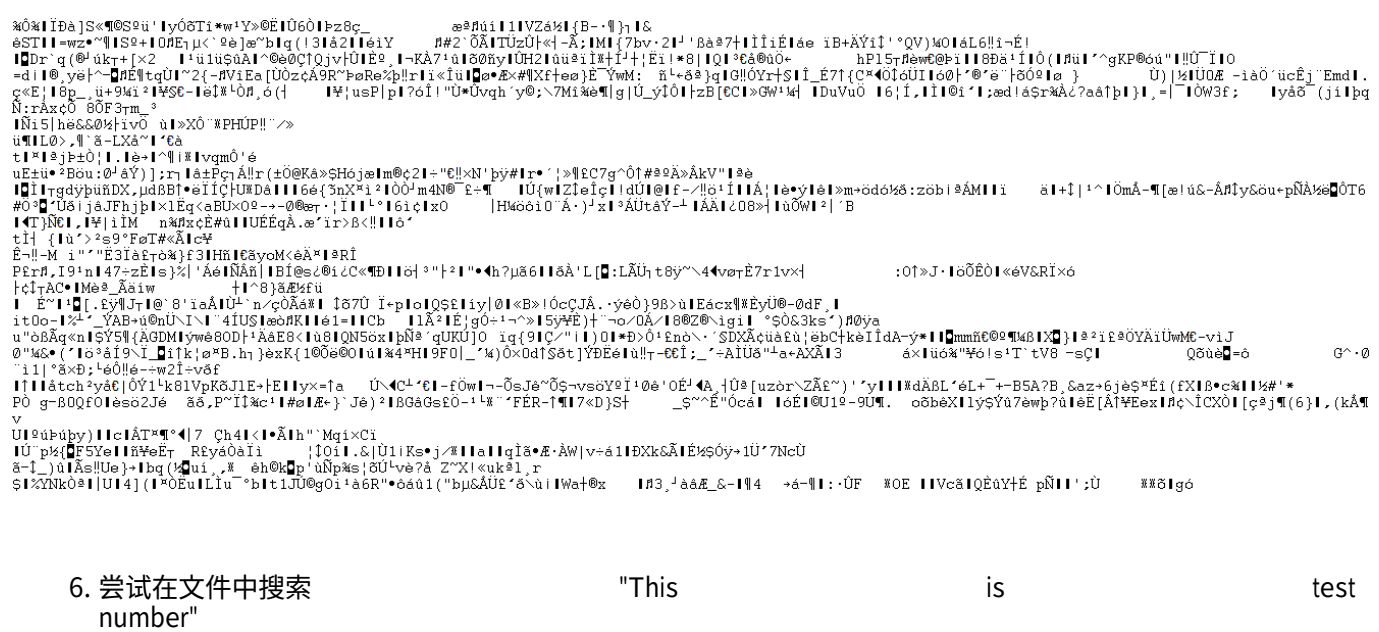
这将创建一千个持久化变量（persistent variable），包含如下内容 This is test number 22。

4. 要确认您已经成功，请看一个变量的值：

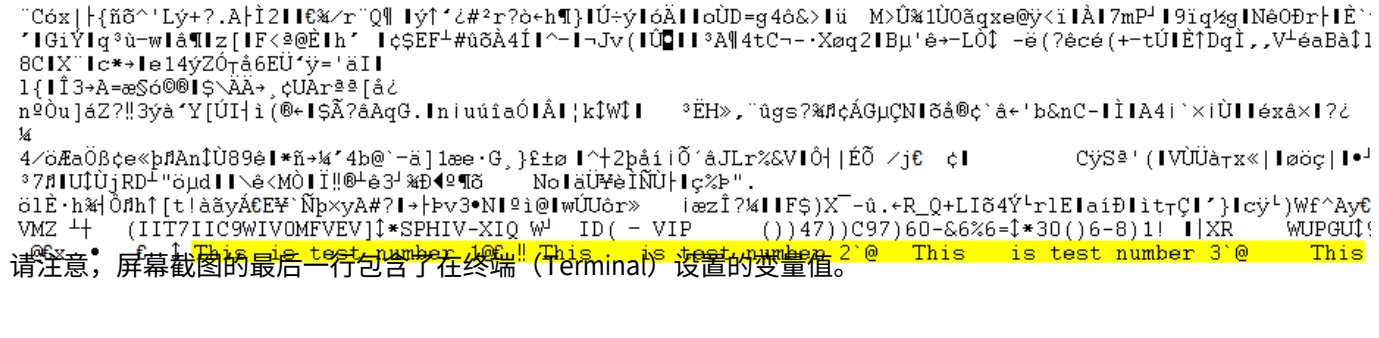
```
ENCDB>w ^x(22)

This is test number 22 ENCDB>
```

5. 要打开数据库文件，进入您在上一节中创建的目录，如 C:\InterSystems\IRIS\mgr\ENCDB，并打开数据库文件 IRIS.DAT。您将会看到如下内容：



6. 尝试在文件中搜索 "This is test number" 这个字符串。您不会找到它——因为数据库是加密的。事实上，您会发现唯一未加密的字符串是数据库的名称或其加密密钥的标识符。
7. 如果您在未加密的数据库上执行同样的测试，产生的文件将包含以下内容：



请注意，屏幕截图的最后一行包含了在终端（Terminal）设置的变量值。

与数据库加密有关的其他功能

InterSystems IRIS 还具有其他值得注意的数据库加密功能，这些功能对您的实现可能很重要：

- KMIP——InterSystems IRIS 允许您在独立于托管实例的服务器上存储密钥。为了与这些服务器通信，InterSystems IRIS 支持密钥管理互通协议（key management interoperability protocol，KMIP）。这使得 InterSystems IRIS 能够从 KMIP 提供的标准化密钥管理方法中获益。
- 更改密钥和添加或删除加密——您可以轻松地更改数据库的加密密钥。如果需要这些操作，加密一个未加密的数据库或制作一个加密数据库的未加密副本也是很简单的。
- 对磁盘上的相关数据进行加密——InterSystems 允许您轻松加密其临时缓存数据库和其他用于保持最近事务记录为当前状态的磁盘内容（即其日志文件）。
- 基于芯片的加密——芯片可以将加密作为其活动的一部分，这为操作提供了更快的速度。InterSystems IRIS 支持使用这种芯片。有关基于芯片的加密的详细信息，请参见下一节。

4. 了解有关数据库加密的更多信息

InterSystems 有很多参考资料可以帮助您了解有关数据库加密的更多信息：

- *Encryption Awareness（《加密意识》）*——InterSystems 在线学习交互式课程，为我们的加密技术提供概念介绍。
- *Encryption Guide（《加密指南》）*——InterSystems 有关数据库加密和相关功能的文档。
- *FIPS 140–2 Compliance for Database Encryption（《FIPS 140-2 数据库加密的遵从性》）*——InterSystems 有关 InterSystems IRIS 支持 FIPS 140-2 标准的文档。

#InterSystems IRIS #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-25-%E6%95%B0%E6%8D%AE%E5%BA%93%E5%8A%A0%E5%AF%86