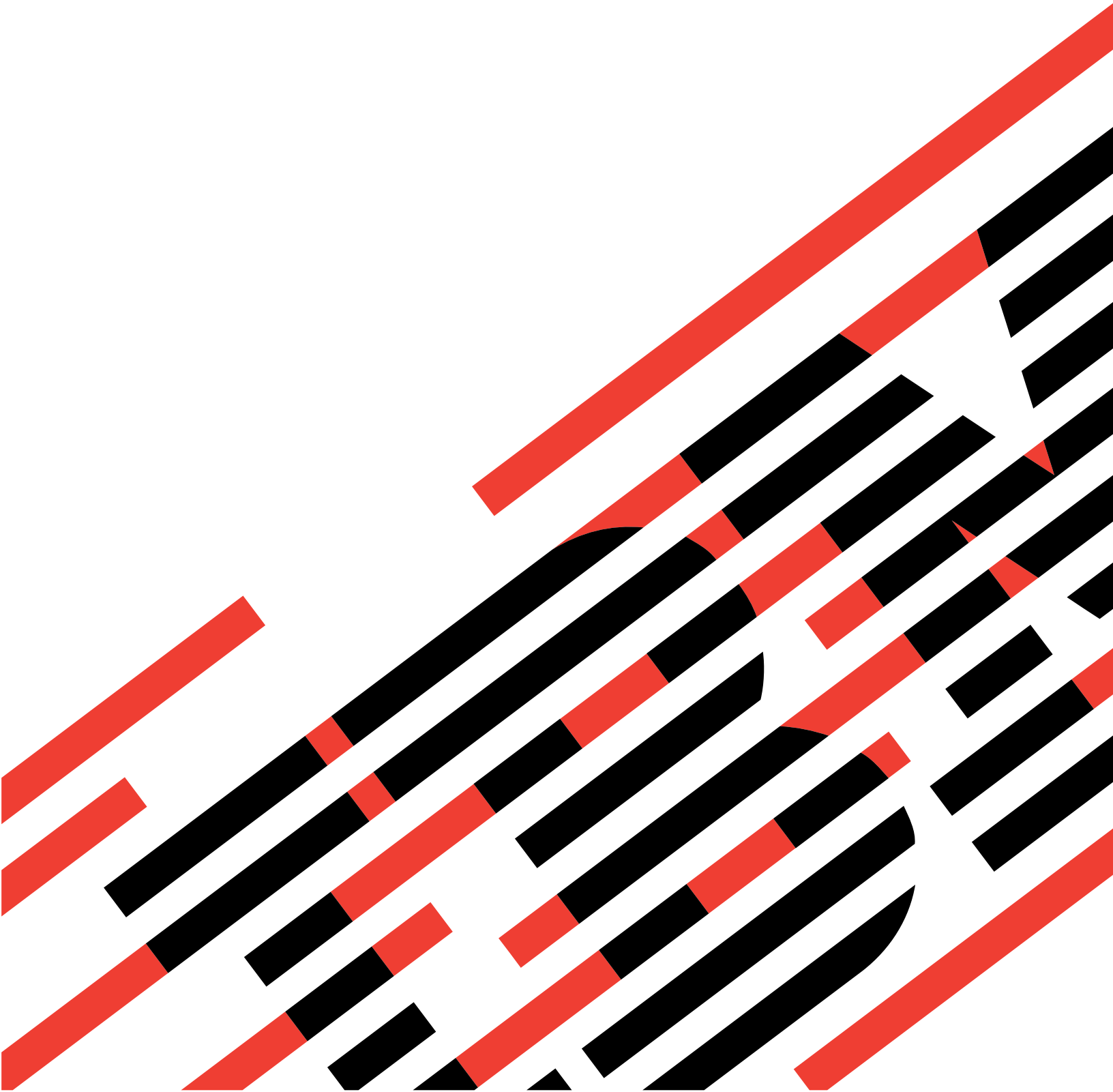
IBM

eserver

iSeries

安全套接字层（SSL）

版本 5 发行版 3



IBM

@server

iSeries

安全套接字层（SSL）

版本 5 发行版 3

注意

在使用本资料及其支持的产品之前，请务必阅读第 19 页的『声明』中的信息。

第五版（2005 年 8 月）

本版本适用于 IBM Operating System/400 V5.3.0（程序号 5722–SS1）及所有后续发行版和修订版，直到在新版本中另有声明为止。本版本不能在所有精简指令集计算机（RISC）机型上运行，也不能在 CISC 机型上运行。

目录

安全套接字层（SSL）

“安全套接字层”（SSL）已经成为使应用程序能够在不受保护的网络（如因特网）上进行安全通信会话的业界标准。使用以下链接来查找关于 SSL 和 iSeries™ 服务器应用程序的更多信息:

- **V5R3 的新增内容**
  记录了关于 SSL 的可用的新功能或新信息。
- **SSL 方案**
  是对 SSL 信息的新补充，且设计用来通过提供 SSL 如何工作的可能示例来提高您对 iSeries 服务器上的 SSL 的理解。
- **SSL 概念**
  包括补充信息，为“安全套接字层”（SSL）协议提供一些基本构建块。
- **SSL 启用计划**
  包括在 iSeries 服务器上启用 SSL 的先决条件，以及一些有用的技巧。
- **用 SSL 保护应用程序**
  包括一个应用程序的列表，您可以用 iSeries 服务器上的 SSL 来保护这些应用程序。
- **SSL 故障诊断**
  提供有关如何开始进行 iSeries 服务器上的 SSL 故障诊断过程的基本指南。
- **SSL 的相关信息**
  包括附加信息资源的链接以供您使用。

V5R3 的新增内容

关于“安全套接字层”（SSL），本发行版有两项新增内容需要注意:

1. 方案: 用 SSL 保护与“中央管理”服务器的客户机连接

   这是一种新方案，它说明如何使用 SSL 来保护远程客户机与 iSeries 服务器上的“中央管理”服务器之间的连接，该 iSeries 服务器是“局域网”（LAN）的指定中央系统。

2. GSKit API 的 GSKit 6B 版本

   从 V5R3 开始，GSKit API 以 GSKit 6B 版本为基础。在前发行版中，它们以 GSKit 4D 版本为基础。有关 GSKit API 的更多信息，请单击此处。

要查找关于本发行版的新增内容或已更改内容的其它信息，请参阅用户备忘录 

如何查看新增内容或更改内容:

为了帮助您查看技术更改，本信息使用:

- » 图像来标记新的或更改的信息的开始位置。
- « 图像来标记新的或更改的信息的结束位置。

打印本主题

可以查看或下载此信息的 PDF 版本。要执行此操作，请选择安全套接字层（SSL）（大约 243 KB）。

其它信息:

还可以查看或打印本主题的任何相关信息。

保存 PDF 文件:

要将 PDF 保存在工作站上以便进行查看或打印:

1. 在浏览器中右键单击 PDF。
2. 单击**目标另存为**。
3. 浏览至要保存 PDF 的目录。
4. 单击**保存**。

下载 Adobe Acrobat Reader:

如果需要 Adobe Acrobat Reader 来查看或打印本信息，则可以从 Adobe Web 站点（www.adobe.com/products/acrobat/readstep.html）  下载副本。

方案

以下方案设计用来帮助您最大程度地获得在 iSeries 服务器上启用 SSL 的好处:

- 方案: 用 SSL 保护与“中央管理”服务器的客户机连接

  此方案说明如何使用 SSL 来保护远程客户机与 iSeries 服务器之间的连接，此服务器通过使用“iSeries 导航器中央管理”服务器来充当中央系统。
- 方案: 用 SSL 保护与“中央管理”服务器的所有连接

  本方案说明如何使用 SSL 来保护与 iSeries 服务器的**所有**连接，此服务器通过使用“iSeries 导航器中央管理”服务器来充当中央系统。
- 方案: 用 SSL 保护 FTP

  本方案说明如何为 FTP 应用程序启用 SSL。
- 方案: 用 SSL 保护 Telnet

  本方案说明如何为 Telnet 应用程序启用 SSL。
- 方案: 增强 iSeries SSL 性能

  本方案说明如何利用密码硬件来增强 iSeries 服务器上的 SSL 性能。
- 方案: 用密码硬件保护专用密钥

  本方案说明如何使用密码硬件来保护与 iSeries 服务器上的 SSL 事务相关联的专用密钥。

方案: 用 SSL 保护与“中央管理”服务器的客户机连接

情况:

公司拥有一个包括其办公室中的几台 iSeries 服务器的局域网（LAN）。该公司的系统管理员 Bob 已将其中一台 iSeries 服务器指定为 LAN 的中央系统（以下称为“系统 A”）。Bob 使用“系统 A”上的“中央管理”服务器来管理其 LAN 上的所有其它端点。

Bob 很关心从公司 LAN 外部的网络连接至“系统 A”上的“中央管理”服务器的连接。Bob 经常出差，在他外出时，需要安全地连接到“中央管理”服务器。当他不在公司办公室时，他想要确保他的 PC 与“中央管理”服务器之间的连接是安全的。Bob 决定在他的 PC 和“系统 A”的“中央管理”服务器上启用 SSL。以此种方式启用 SSL 后，Bob 能够确定出差期间他与“中央管理”服务器的连接是安全的。

目标:

Bob 想要保护他的 PC 与“中央管理”服务器之间的连接。对于“系统 A”上的“中央管理”服务器与 LAN 上的端点之间的连接，Bob 不需要附加的安全性。对于其他在公司办公室工作的职员，他们在与“中央管理”服务器连接时，也不需要附加的安全性。Bob 的计划是配置他的 PC 和“系统 A”上的“中央管理”服务器，以便他的客户机连接使用服务器认证。从 LAN 上的其它 PC 或 iSeries 服务器到“中央管理”服务器的连接不使用 SSL 保护。

详细信息:

下表根据在 PC 客户机上启用或禁用 SSL 来说明所使用的认证类型:

表 1. 客户机与“中央管理”服务器之间受 SSL 保护的连接的必需元素

Bob 的 PC 上的 SSL 状态	“系统 A”上的“中央管理”服务器的指定认证级别	是否启用了 SSL 连接?
SSL 关闭	任何	否
SSL 打开	任何	是（服务器认证）

服务器认证意味着 Bob 的 PC 对“中央管理”服务器的证书进行认证。当与“中央管理”服务器连接时，Bob 的 PC 充当 SSL 客户机。“中央管理”服务器充当 SSL 服务器，并且必须证明其身份。“中央管理”服务器通过提供由 Bob 的 PC 信任的“认证中心”（CA）发布的证书来执行此项操作。

先决条件和假设:

为了保护他的 PC 与“系统 A”上的“中央管理”服务器之间的连接，Bob 必须执行下列管理和配置任务:

1. “系统 A”满足 SSL 的先决条件（请参阅 SSL 先决条件）。
2. 在“系统 A”上安装了 OS/400® V5R3（或更新版本）。如果“系统 A”正在运行 OS/400 V5R1，则为 OS/400（5722-SS1）安装下列修订（PTF）:
   a. SI01375
   b. SI01376
   c. SI01377
   d. SI01378
   e. SI01838
3. “iSeries 导航器”PC 客户机运行 iSeries Access for Windows® V5R3 或更新版本。
4. 获取 iSeries 服务器的“认证中心”（CA）。
5. 为“系统 A”创建由 CA 签署的证书。
6. 将 CA 和证书发送给“系统 A”，并将其导入密钥数据库。
7. 使用“中央管理”服务器标识指定证书。

a. 在“系统 A”上，启动 IBM® 数字证书管理器。现在，Bob 获取或创建证书，或另外设置或更改他的证书系统。有关如何设置证书系统的信息，请参阅使用数字证书管理器。

b. 单击**选择证书库**。

c. 选择 ***SYSTEM** 并单击**继续**。

d. 输入 *SYSTEM **证书库密码**，并单击**继续**。当重新装入菜单时，展开**管理应用程序**。

e. 单击**更新证书指定**。

f. 选择**服务器**并单击**继续**。

g. 选择**中央管理服务器**并单击**更新证书指定**。这将证书指定给“中央管理”服务器使用，以便建立 iSeries Access for Windows 客户机的身份。

h. 单击**指定新证书**。得到确认消息后，DCM 重新装入到**更新证书指定**页面。

i. 单击**完成**。

8. 设置“iSeries 导航器”：

a. 在 PC 客户机上选择性地安装“iSeries 导航器”的 SSL 组件。

b. 将 CA 下载至 PC 客户机。

配置步骤:

为了使用 SSL 保护其 PC 客户机与“系统 A”上的“中央管理”服务器的连接，Bob 需要完成下列步骤:

1. 步骤 1: 取消激活“iSeries 导航器”客户机的 SSL
2. 步骤 2: 设置“中央管理”服务器的认证级别
3. 步骤 3: 重新启动“系统 A”上的“中央管理”服务器
4. 步骤 4: 激活“iSeries 导航器”客户机的 SSL
5. 可选步骤: 取消激活“iSeries 导航器”客户机的 SSL

要查看扩展的配置步骤，请参阅: 用 SSL 保护与“中央管理”服务器的客户机连接。

配置详细信息: 用 SSL 保护与“中央管理”服务器的客户机连接

下列信息假定您已经通篇阅读了方案: 用 SSL 保护与“中央管理”服务器的客户机连接。在本方案中，iSeries 服务器被指定为公司的局域网（LAN）中的中央系统。Bob 使用中央系统（此处称为“系统 A”）上的“中央管理”服务器来管理公司网络上的端点。以下信息说明如何执行保护与“中央管理”服务器的外部客户机连接所需的步骤。跟随 Bob 一起完成方案配置步骤。

Bob 可以在“中央管理”服务器上启用 SSL 之前，他必须安装必备软件程序并在 iSeries 服务器上安装数字证书。继续执行下一步之前，请参阅本方案的先决条件和假设。一旦满足了这些先决条件，他就可以完成下列过程来为“中央管理”服务器启用 SSL。

步骤 1: 取消激活“iSeries 导航器”客户机的 SSL

1. 在“iSeries 导航器”中，展开**我的连接**。
2. 右键单击“系统 A”，然后选择**属性**。
3. 单击**安全套接字**选项卡，并取消选择**将安全套接字层（SSL）用于连接**。
4. 退出“iSeries 导航器”并重新启动它。

挂锁从“iSeries 导航器”中的“中央管理”容器消失，指示连接未受保护。这向 Bob 指示在他的客户机与其公司的中央系统之间不再具有受 SSL 保护的连接。

步骤 2: 设置“中央管理”服务器的认证级别

1. 在“iSeries 导航器”中，右键单击**中央管理**，然后选择**属性**。

2. 单击**安全性**选项卡，然后选择**使用安全套接字层（SSL）**。
3. 为认证级别选择**任何**（在 iSeries Access for Windows V5R3 或更新版本上可用）。
4. 单击**确定**以在中央系统上设置此值。

步骤 3: 在中央系统上重新启动“中央管理”服务器

1. 在“iSeries 导航器”中，展开**我的连接**。
2. 在**系统 A** 上，展开**网络 --> 服务器**，然后选择 **TCP/IP**。
3. 右键单击**中央管理**并选择**停止**。中央系统视图折叠且显示一条消息，说明您没有与服务器连接。
4. 一旦“中央管理”服务器已停止，单击**启动**以重新启动它。

步骤 4: 激活“iSeries 导航器”客户机的 SSL

1. 在“iSeries 导航器”中，展开**我的连接**。
2. 右键单击“系统 A”，然后选择**属性**。
3. 单击**安全套接字**选项卡，并选择**将安全套接字层（SSL）用于连接**。
4. 退出“iSeries 导航器”并重新启动它。

挂锁出现在“iSeries 导航器”中的“中央管理”服务器旁边，指示受 SSL 保护的连接。这向 Bob 指示他已经在其客户机与其公司的中央系统之间成功激活了受 SSL 保护的连接。

注: 此过程仅保护一台 PC 与“中央管理”服务器之间的连接。其它与“中央管理”服务器的客户机连接以及从端点到“中央管理”服务器的连接都将是不安全的。要保护其它客户机，确保它们满足先决条件并重复步骤 4。要保护与“中央管理”服务器的其它连接，请参阅方案: 用 SSL 保护与“中央管理”服务器的所有连接。

可选步骤: 取消激活“iSeries 导航器”客户机的 SSL

如果 Bob 想在公司办公室工作，而且不想 SSL 连接影响其 PC 的性能，则可以通过执行下列步骤来轻松地取消激活 SSL 连接:

1. 在“iSeries 导航器”中，展开**我的连接**。
2. 右键单击**中央管理**，然后选择**属性**。
3. 单击**安全套接字**选项卡，并取消选择**将安全套接字层（SSL）用于连接**。
4. 退出“iSeries 导航器”并重新启动它。

挂锁从“iSeries 导航器”中的“中央管理”服务器消失，指示连接未受保护。这向 Bob 指示在他的 PC 客户机和“系统 A”上的“中央管理”服务器之间不再具有受 SSL 保护的连接。

有关与其它 SSL 方案的链接，请参阅方案。

方案: 用 SSL 保护与“中央管理”服务器的所有连接

情况:

公司刚刚建立了一个广域网（WAN），它包括几个处于远程位置（端点）的 iSeries 服务器。端点由位于总公司的一台 iSeries 服务器（中央系统）集中管理。Tom 是公司的安全专家。Tom 想使用“安全套接字层”（SSL）来保护公司的中央系统上的“中央管理”服务器与所有端点服务器和客户机之间的全部连接。

详细信息:

Tom 可以使用 SSL 来**安全地**管理与“中央管理”服务器的所有连接。要将 SSL 与“中央管理”服务器配合使用，Tom 需要保护 iSeries Access for Windows 和他用来访问中央系统的 PC 上的“iSeries 导航器”。

Tom 从两个认证级别中进行选择:

服务器认证

提供端点系统服务器证书的认证。当连接至端点系统时，中央系统充当 SSL 客户机。端点系统充当 SSL 服务器，并且必须通过提供由中央系统信任的“认证中心”发布的证书来证明其身份。对于每个端点系统，必须具有由可信的 CA 发布的有效证书。

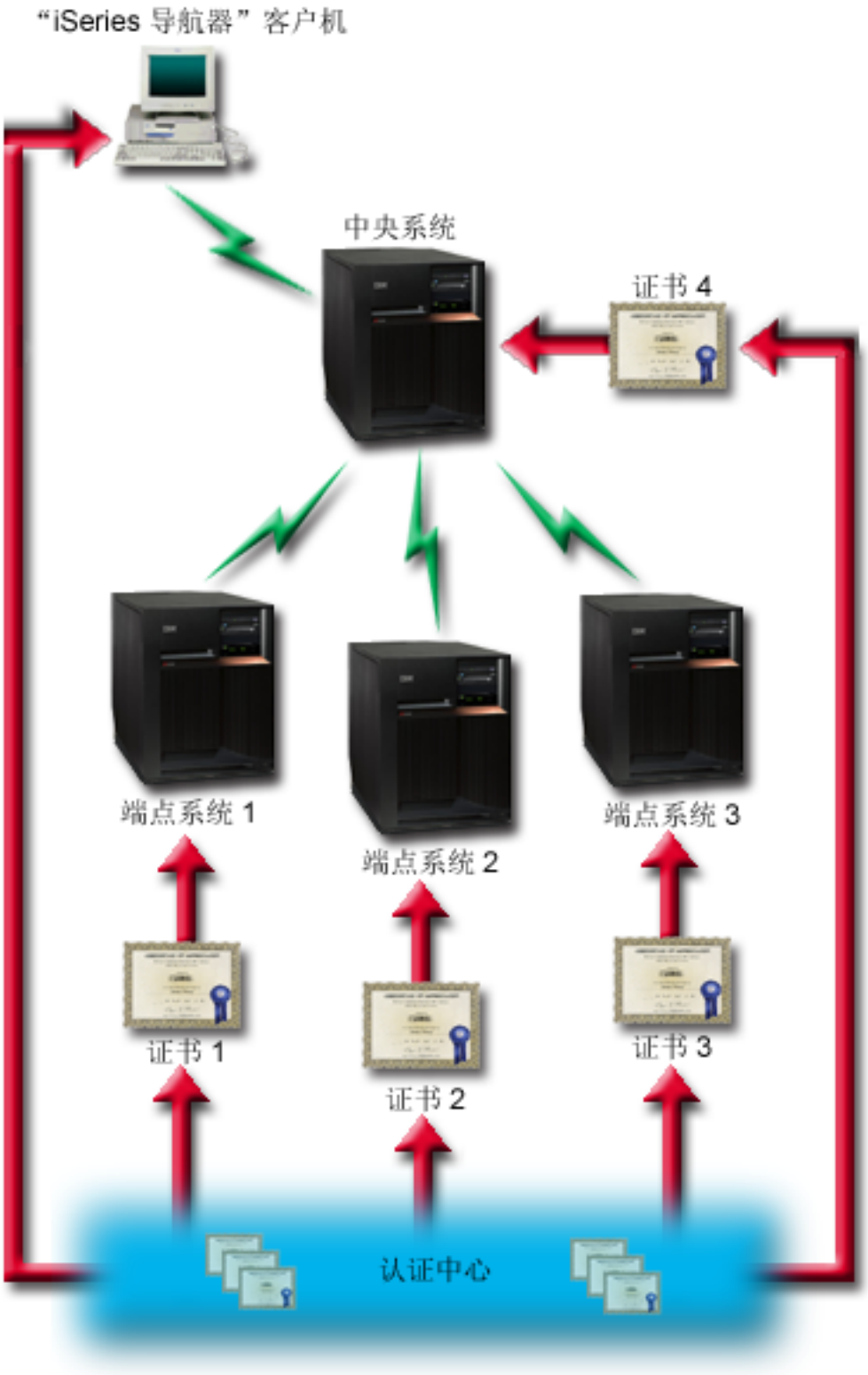
客户机和服务器认证

同时提供中央系统和端点系统证书的认证。这是一种比服务器认证级别更强的安全级别。在其它应用程序中，它被称为客户机认证，其中客户机必须提供有效可信的证书。当中央系统（SSL 客户机）试图与端点系统（SSL 服务器）建立连接时，中央系统和端点系统对彼此的证书进行认证以获取认证中心真实性。

与其它应用程序不同，“中央管理”还通过一份验证列表（称为“可信组”验证列表）来提供认证。通常，验证列表存储标识用户的信息（如用户标识）和认证信息（如密码、个人识别号码或数字证书）。此认证信息是加密的。

通常，大多数应用程序不指定同时启用服务器和客户机认证，因为服务器认证几乎总是发生在 SSL 会话启用期间。许多应用程序具有客户机认证配置选项。由于中央系统在网络中扮演双重角色，因此“中央管理”使用术语“服务器和客户机认证”而不是客户机认证。当 PC 用户连接至中央系统并且启用了 SSL 时，中央系统充当服务器。然而，当中央系统正在连接至端点系统时，它充当客户机。以下图表显示中央系统在网络中是如何同时充当服务器和客户机的。

注: 在此图表中，与“认证中心”关联的证书必须存储在中央系统和所有端点系统上的密钥数据库中。



先决条件和假设:

Tom 必须执行下列管理和配置任务（请参阅图像 受 SSL 保护的中央管理 WAN），以便保护与“中央管理”服务器的所有连接:

1. 中央系统满足 SSL 的先决条件（请参阅 SSL 先决条件）。
2. 中央系统和所有端点 iSeries 服务器运行 OS/400 V5R2 或更新版本。如果中央系统和端点运行 OS/400 V5R1，则为 OS/400（5722-SS1）安装下列修订（PTF）:
   a. SI01375
   b. SI01376
   c. SI01377
   d. SI01378
   e. SI01838
3. “iSeries 导航器”PC 客户机运行 iSeries Access for Windows V5R2 或更新版本。如果客户机在 V5R1 环境下，则安装 V5R1 iSeries Access for Windows（5722-XE1）的 service pack PTF SI01907（或更新版本）。
4. 获取 iSeries 服务器的“认证中心”（CA）。
5. 为每一台由启用了 SSL 的“中央管理”服务器管理的 iSeries 服务器创建由 CA 签署的证书。
6. 将 CA 和证书发送至每一台 iSeries 服务器，并将它们导入密钥数据库。
7. 用“中央管理”应用程序标识和“iSeries 导航器”使用的所有端点服务器的应用程序标识来指定证书:
   a. 启动中央服务器上的 IBM 数字证书管理器。如果 Tom 需要获取或创建证书，或另外设置或更改他的证书系统，则现在就这样做（有关设置证书系统的信息，请参阅使用数字证书管理器）。
   b. 单击**选择证书库**。
   c. 选择 ***SYSTEM** 并单击**继续**。
   d. 输入 *SYSTEM **证书库密码**，并单击**继续**。当重新装入菜单时，展开**管理应用程序**。
   e. 单击**更新证书指定**。
   f. 选择**服务器**并单击**继续**。
   g. 选择**中央管理服务器**并单击**更新证书指定**。这将证书指定给“中央管理”服务器使用。
   h. 单击**指定新证书**。得到确认消息后，DCM 重新装入到**更新证书指定**页面。
   i. 单击**完成**。
   j. 对“iSeries 导航器”使用的所有端点服务器重复此过程。
8. 设置“iSeries 导航器”:
   a. 在 PC 客户机上选择性地安装“iSeries 导航器”的 SSL 组件。
   b. 将 CA 下载至 PC 客户机。

配置步骤:

在 Tom 可以在“中央管理”服务器上启用 SSL 之前，他必须安装必备软件程序并在中央系统上安装数字证书。继续执行下一步之前，请参阅本方案的先决条件和假设。满足了这些先决条件之后，他就可以完成以下过程来保护与“中央管理”服务器的所有连接:

注: 如果已经为“iSeries 导航器”启用了 SSL，则在“中央管理”服务器上启用 SSL 之前，Tom 必须禁用它。如果只是对“iSeries 导航器”启用了 SSL，而没有对“中央管理”服务器启用它，则尝试通过“iSeries 导航器”来连接中央系统将失败。

- 步骤 1: 配置中央系统以进行服务器认证
- 步骤 2: 配置端点系统以进行服务器认证
- 步骤 3: 在中央系统上重新启动“中央管理”服务器

- 步骤 4: 在所有端点系统上重新启动“中央管理”服务器
- 步骤 5: 激活“iSeries 导航器”客户机的 SSL
- 步骤 6: 配置中央系统以进行客户机认证
- 步骤 7: 配置端点系统以进行客户机认证
- 步骤 8: 将验证列表复制到端点系统
- 步骤 9: 在中央系统上重新启动“中央管理”服务器
- 步骤 10: 在所有端点系统上重新启动“中央管理”服务器

要查看扩展的配置步骤，请参阅配置详细信息: 用 SSL 保护与“中央管理”服务器的所有连接。

配置详细信息: 用 SSL 保护与“中央管理”服务器的所有连接

下列信息假定您已经通篇阅读了以下信息: 方案: 用 SSL 保护与“中央管理”服务器的所有连接。现在，您可能想要了解如何执行保护与“中央管理”服务器的所有连接所必需的步骤。跟随 Tom 一起完成此方案。

在 Tom 可以在“中央管理”服务器上启用 SSL 之前，他必须安装必备软件程序并在 iSeries 服务器上安装数字证书。继续执行下一步之前，请参阅本方案的先决条件和假设。满足了这些先决条件之后，他可以完成以下过程来保护与“中央管理”服务器的所有连接。

注: 如果已经为“iSeries 导航器”启用了 SSL，则在“中央管理”服务器上启用 SSL 之前，Tom 必须禁用它。如果只是对“iSeries 导航器”启用 SSL，而不是对“中央管理”服务器启用它，则通过“iSeries 导航器”来连接中央系统的尝试将失败。

步骤 1: 配置中央系统以进行服务器认证

SSL 允许 Tom 保护在中央系统与端点系统之间的传输，以及“iSeries 导航器”客户机与中央系统之间的传输。SSL 提供证书的传输和认证及数据的加密。SSL 连接只可以存在于启用 SSL 的中央系统和启用 SSL 的端点系统之间。在配置客户机认证之前，Tom 需要先配置服务器认证。

1. 在“iSeries 导航器”中，右键单击**中央管理**并选择**特性**。
2. 单击**安全性**选项卡，并选择**使用安全套接字层（SSL）**
3. 选择**服务器**作为认证级别。
4. 单击**确定**以在中央系统上设置此值。

   注: 在完成服务器认证的端点系统配置之前，**切勿**重新启动“中央管理”服务器。
5. 配置端点系统以进行服务器认证。

步骤 2: 配置端点系统以进行服务器认证

在 Tom 为服务器认证配置中央系统之后，需要为服务器认证配置端点系统。完成下列任务:

1. 展开**中央管理**。
2. 比较和更新端点系统的系统值:
   a. 在**端点系统**下，右键单击中央系统并选择**清单 —> 收集**。
   b. 选中收集对话框上的**系统值**选项，以便收集中央系统的系统值清单。取消选择其它任何选项。
   c. 右键单击**系统组 —> 新建系统组**。
   d. 定义包括使用 SSL 要连接的所有端点系统的新系统组。
   e. 要显示新组，展开系统组列表。
   f. 收集完成之后，右键单击新建系统组并选择**系统值 —> 比较和更新**。

g. 验证中央系统显示在**模型系统**字段中。

h. 选择**中央管理**类别并验证以下值，选中各项旁边的框:

- 对**使用安全套接字层**指定**是**。
- 为 SSL 认证级别指定**服务器**。

在配置中央系统以进行服务器认证过程中，在中央系统上设置这些值。

i. 单击**确定**以便在新系统组的端点系统上设置这些值。

j. 等待**比较和更新**进程完成，然后重新启动“中央管理”服务器。这可能要花几分钟时间。

步骤 3: 在中央系统上重新启动“中央管理”服务器

1. 在“iSeries 导航器”中，展开**我的连接**。
2. 展开中央系统视图。
3. 展开**网络 —> 服务器**，并选择 **TCP/IP**。
4. 右键单击**中央管理**并选择**停止**。中央系统视图折叠，且屏幕上显示消息，说明您没有与服务器连接。
5. “中央管理”服务器停止后，单击**启动**以重新启动服务器。

步骤 4: 在所有端点系统上重新启动“中央管理”服务器

1. 展开要重新启动的端点系统。
2. 展开**网络 —> 服务器**，并选择 **TCP/IP**。
3. 右键单击**中央管理**并选择**停止**。
4. “中央管理”服务器停止后，单击**启动**以重新启动服务器。
5. 为每个端点系统重复此过程。

步骤 5: 激活“iSeries 导航器”客户机的 SSL

1. 在“iSeries 导航器”中，展开**我的连接**。
2. 右键单击中央系统，然后选择**特性**。
3. 单击**安全套接字**选项卡，并选择**将安全套接字层（SSL）用于连接**。
4. 退出“iSeries 导航器”并重新启动它。

步骤 6: 配置中央系统以便进行客户机认证（可选步骤）

既然 Tom 完成了服务器认证的配置，他就可以执行下列可选的客户机认证过程。客户机认证为端点系统和中央系统两者提供“认证中心”和可信组的验证。当中央系统（SSL 客户机）尝试使用 SSL 来连接到端点系统（SSL 服务器）时，中央系统和端点系统通过客户机认证来对彼此的证书进行认证。这也称为“认证中心”和“可信组”认证。

注: 直到您已经配置了服务器认证之后才能完成客户机认证配置。

1. 在“iSeries 导航器”中，右键单击**中央管理**并选择**特性**。
2. 单击**安全性**选项卡，并选择**使用安全套接字层（SSL）**。
3. 对认证级别选择**客户机和服务器**。
4. 单击**确定**以在中央系统上设置此值。

   注: 在配置所有端点系统以便将 SSL 与客户机和服务器认证配合使用之前，**切勿**重新启动“中央管理”服务器。

5. 配置端点系统以进行客户机认证。

步骤 7: 配置端点系统以进行客户机认证（可选步骤）

1. 比较和更新端点系统的系统值:

   注: 此任务对任何运行 V4R5 的端点 iSeries 服务器不起作用。

   a. 在**端点系统**下，右键单击中央系统并选择**清单 —> 收集**。

   b. 选中收集对话框上的**系统值**选项，以便收集中央系统的系统值清单。取消选择其它任何选项。

   c. 右键单击**系统组 —> 新建系统组**。

   d. 定义包括使用 SSL 要连接的所有端点系统的新系统组。

   e. 要显示新组，展开系统组列表。

   f. 收集完成之后，右键单击新建系统组并选择**系统值 —> 比较和更新**。

   g. 验证**中央系统**显示在**模型系统**字段中。

   h. 选择**中央管理**类别并验证以下内容:

      - 对**使用安全套接字层**指定**是**。
      - 对 SSL 认证级别指定**客户机和服务器**。

      在配置中央系统以进行客户机认证过程中，在中央系统上设置这些值。选中每个值旁的**更新**框。

   i. 单击**确定**以便在新系统组的端点系统上设置这些值。

步骤 8: 将验证列表复制到端点系统

1. 下列步骤假定您的中央系统是 V5R3 或更高版本: 在“iSeries 导航器”中，展开**中央管理 —> 定义**。
2. 右键单击**数据包**，并选择**新建定义**。
3. 在**新建定义**窗口，进行以下操作:
   - **名称**: 输入定义的名称。
   - **源系统**: 选择中央系统的名称。
   - **选定的文件和文件夹**: 单击字段，并输入 /QSYS.LIB/QMGTC2.LIB/QYPSVLDL.VLDL。
4. 单击**选项**选项卡，并选择**用正在发送的文件替换现有文件**。
5. 单击**高级**。
6. 在**高级选项**窗口中，指定**是**以允许在恢复时存在对象差别。
7. 单击**确定**以刷新定义列表并显示新的数据包。
8. 右键单击新的数据包，然后选择**发送**。
9. 在**发送**对话框中: 展开**可用系统和组**列表中的**系统组 -> 可信组**。将任意系统（V5R3 或更高版本）单独添加到**选择的系统和组**列表。从**选择的系统和组**列表中除去其它任何系统，然后单击**确定**。“可信组”是您在步骤 7: 配置端点系统以进行客户机认证的第 1.c. 部分中定义的系统组。

   注: 在中央系统中**发送**任务通常会失败，因为中央系统通常是源系统。**发送**任务可在所有端点系统上成功完成。

   在 V5R3 之前版本的 iSeries 系统上，QYPSVLDL.VLDL 位于 QUSRSYS.LIB 中，而不是位于 QMGTC2.LIB 中。因此，如果具有 V5R3 之前版本的系统，您需要将验证列表发送到这些系统，然后将该列表置于 QUSRSYS.LIB（而非 QMGTC2.LIB）中。为此，请执行以下操作:

   a. 右键单击以上创建的数据包定义，然后选择**新建基于**。

   b. 为该定义提供一个新的名称，以将其与第一个定义区分开。

   c. 在该定义的**常规**选项卡上，单击**目标路径**列中的路径 /QSYS.LIB/QMGTC2.LIB/QYPSVLDL.VLDL。这使您可以对其进行编辑。将 QMGTC2 更改为 QUSRSYS。

注: 请确保编辑**目标路径**（而非**源路径**）。

d. 单击**确定**以保存新的数据包定义。

e. 右键单击新的数据包定义，然后选择**发送**。

f. 在**发送**对话框中：展开**可用系统和组**列表中的**系统组 -> 可信组**。将 V5R3 之前版本的任意系统单独添加到**选择的系统和组**列表。从**选择的系统和组**列表中除去其它任何系统，然后单击**确定**。**可信组**是您在步骤 7: 配置端点系统以进行客户机认证的第 1.c. 部分中定义的系统组。

步骤 9: 在中央系统上重新启动“中央管理”服务器

1. 在“iSeries 导航器”中，展开**我的连接**。
2. 展开中央系统。
3. 展开**网络 —> 服务器**，并选择 **TCP/IP**。
4. 右键单击**中央管理**并选择**停止**。中央系统视图折叠，且屏幕上显示消息，说明您没有与服务器连接。
5. “中央管理”服务器停止后，单击**启动**以重新启动服务器。

步骤 10: 在所有端点系统上重新启动“中央管理”服务器

注: 为每个端点系统重复此过程。

1. 展开要重新启动的端点系统。
2. 展开**网络 —> 服务器**，并选择 **TCP/IP**。
3. 右键单击**中央管理**并选择**停止**。
4. “中央管理”服务器停止后，单击**启动**以重新启动服务器。

有关与其它 SSL 方案的链接，请参阅方案。

概念

用 SSL 协议可以建立客户机和服务器应用程序之间的安全连接，这些应用程序提供通信会话的一个或两个端点的认证。SSL 还提供客户机和服务器应用程序所交换的数据的保密性和完整性。

使用以下概念性信息可帮助您更深刻地理解 SSL 和 iSeries 服务器之间的关系:

- SSL 的历史记录
- SSL 如何工作
- 受支持的 SSL 和“传输层安全性”（TLS）协议
- 服务器认证
- 客户机认证

SSL 的历史记录

由于公众越来越关注因特网安全性，为了应付此情况，Netscape 在 1994 年开发了“安全套接字层协议”（SSL）。最初开发 SSL 的目的在于保护 Web 浏览器和服务器通信。该规范以此方式进行设计，从而使其它应用程序（如 TELNET 和 FTP）能够使用 SSL。有关 SSL 和相关协议的更多信息，请参阅受支持的 SSL 和“传输层安全性”（TLS）协议。

SSL 如何工作

SSL 实际上是两个协议，即记录协议和握手协议。记录协议控制在 SSL 会话的两个端点之间的数据流。

握手协议对 SSL 会话的一个或两个端点进行认证，并建立唯一的对称密钥，用来生成对该 SSL 会话的数据进行加密和解密的密钥。SSL 使用非对称密码术、数字证书和 SSL 握手流来对 SSL 会话的一个或两个端点进行认证。通常，SSL 对服务器进行认证。也可以选择 SSL 来对客户机进行认证。一份由“认证中心”发出的数字证书，可以指定给每个端点，或指定给连接的每个端点上使用 SSL 的应用程序。

数字证书包含一个公用密钥和由可信的“认证中心”（CA）数字化签署的一些标识信息。每个公用密钥都具有一个关联的专用密钥。专用密钥不与证书存储在一起，也不作为证书的一部分存储。在服务器认证和客户机认证中，正在被认证的端点必须能够证明其有权访问与数字证书中包含的公用密钥关联的专用密钥。

由于密码操作使用公用密钥和专用密钥，因此 SSL 握手是强调性能的操作。建立了两个端点之间的初始 SSL 会话之后，这两个端点的 SSL 会话信息和应用程序就可以在安全内存中高速缓存，从而加速后续 SSL 会话的启用。恢复 SSL 会话时，这两个端点使用简略的握手流来认证每个端点都有权访问唯一信息，而无需使用公用密钥或专用密钥。如果两个端点都能证明它们有权访问此唯一信息，那么建立新的对称密钥并恢复该 SSL 会话。对于 TLS V1.0 和 SSL V3.0 会话，高速缓存的信息在安全内存中保留的时间不会超过 24 小时。在 V5R2M0 和后续发行版中，可以通过使用密码硬件来将 SSL 握手性能对主 CPU 的影响降至最低。

受支持的 SSL 和“传输层安全性”（TLS）协议

有几个已定义的 SSL 协议版本。最新版本的“传输层安全协议”（TLS）基于 SSL 3.0，并且是“因特网工程任务组织”（IETF）的产品。OS/400 实现支持以下版本的 SSL 和 TLS 协议:

- TLS V1.0
- TLS V1.0 与 SSL V3.0 的兼容性

  注:

  1. 指定 TLS V1.0 与 SSL V3.0 的兼容性意味着如果可能的话将进行 TLS 协商，而如果该协商不可能的话，则将进行 SSL V3.0 协商。如果 SSL V3.0 不能协商，SSL 握手将会失败。
  2. TLS V1.0 与 SSL V3.0 和 SSL V2.0 的兼容性也受支持。这用协议值 **ALL** 指定，这表示如果可能的话，将进行 TLS 协商，而如果不可能的话，则将进行 SSL V3.0 协商。如果 SSL V3.0 不能协商，则将协商 SSL V2.0。如果 SSL V2.0 不能协商，SSL 握手将会失败。
- SSL V3.0
- SSL V2.0
- SSL V3.0 与 SSL V2.0 的兼容性

SSL V3.0 与 SSL V2.0

与 SSL V2.0 相比，SSL V3.0 几乎是一个完全不同的协议。这两个协议之间的一些主要区别包括:

- SSL V3.0 握手协议流与 SSL V2.0 握手流不同。
- SSL V3.0 使用 RSA Data Security,Incorporated 的 BSAFE 3.0 实现。BSAFE 3.0 包括许多计时攻击修正和 SHA-1 散列算法。SHA-1 散列算法被认为是比 MD5 散列算法更安全的算法。SHA-1 使 SSL V3.0 支持使用 SHA-1 而不是 MD5 的其它密码套件。
- SSL V3.0 协议减少了 SSL 握手处理期间发生的 man-in-the-middle（MITM）类型的攻击。在 SSL V2.0 中，MITM 攻击可能会削弱密码规范，虽然这未必会发生，但有这种可能。削弱密码可能会使某个未授权的人破解 SSL 会话密钥。

TLS V1.0 与 SSL V3.0

基于 SSL V3.0 的最新业界标准 SSL 协议是“传输层安全性”（TLS）V1.0。其规范由“因特网工程任务组织”（IETF）在 RFC 2246 ″The TLS Protocol.″  中定义。

TLS 的主要目标是使 SSL 更安全并使协议的规范更精确和完善。TLS 在 SSL V3.0 的基础上，提供了这些增强内容:

- 更安全的 MAC 算法
- 更严密的警报
- “灰色区域”规范的更明确的定义

任何对 SSL 启用的 iSeries 服务器应用程序将自动获取 TLS 支持，除非该应用程序特别要求只能使用 SSL V3.0 或 SSL V2.0。

TLS 提供了以下安全性改进:

- **对于消息认证使用密钥散列法**
  TLS 使用“消息认证代码的密钥散列法”（HMAC），当记录在开放的网络（如因特网）上传送时，该代码确保记录不会被变更。SSL V3.0 还提供键控消息认证，但 HMAC 比 SSL V3.0 使用的（消息认证代码）MAC 功能更安全。
- **增强的伪随机功能（PRF）**
  PRF 生成密钥数据。在 TLS 中，HMAC 定义 PRF。PRF 使用两种散列算法，以这种方式保证其安全性。如果任一算法暴露了，只要第二种算法未暴露，则数据仍然是安全的。
- **改进的已完成消息验证**
  TLS V1.0 和 SSL V3.0 都对两个端点提供已完成的消息，该消息认证交换的消息没有被变更。然而，TLS 将此已完成消息基于 PRF 和 HMAC 值之上，这也比 SSL V3.0 更安全。
- **一致证书处理**
  与 SSL V3.0 不同，TLS 试图指定必须在 TLS 实现之间交换的证书类型。
- **特定警报消息**
  TLS 提供更多的特定和附加警报，以指示任一会话端点检测到的问题。TLS 还对何时应该发送某些警报进行记录。

服务器认证

通过服务器认证，客户机可确保服务器证书是有效的，并确保该证书是由客户机信任的认证中心（CA）签署的。SSL 将使用非对称密码术和握手协议流来生成一个将只用于此唯一 SSL 会话的对称密钥。此密钥用来生成一组密钥，使用这组密钥来对将在 SSL 会话上流动的数据进行加密和解密。随后，在 SSL 握手已经完成时，将已经对通信链路的一端或两端进行了认证。另外，还生成了一个唯一的密钥来对数据进行加密和解密。握手完成之后，应用层数据将在该 SSL 会话中以加密形式流动。

客户机认证

许多应用程序允许启用客户机认证选项。通过客户机认证，服务器将确保客户机证书是有效的，并确保该证书是由服务器所信任的“认证中心”签署的。以下的 iSeries 服务器应用程序支持客户机认证:

- IBM HTTP Server（基于 Apache）
- FTP 服务器
- Telnet 服务器
- “中央管理”端点系统
- 目录服务（LDAP）

SSL 启用计划

当计划在 iSeries 服务器上启用 SSL 时，请考虑以下问题:

- SSL 先决条件
- 想要什么类型的数字证书，从哪里可获取它们

SSL 先决条件:

- IBM 数字证书管理器（DCM），OS/400 的选项 34（5722-SS1）
- TCP/IP Connectivity Utilities for iSeries（5722-TC1）
- IBM HTTP Server for iSeries（5722-DG1）
- 如果您正在尝试用 HTTP Server 来使用 DCM，请确保安装有 IBM Developer Kit for Java™（5722–JV1）。否则，HTTP 管理服务器将不会启动。
- IBM Cryptographic Access Provider 产品，5722-AC3（128 位）。此产品的位大小指示可用于密码操作的对称密钥中的秘密资料的最大大小。对称密钥允许的大小受各个国家或地区的导入和导出规则控制。位大小越大，连接越安全。
- 您可能还希望安装密码硬件来与 SSL 配合使用以加速 SSL 握手处理。有关可用选项，请参阅密码硬件信息。如果希望安装 4758 IBM 加密协处理器或 4764 IBM 加密协处理器，还必须安装“选项 35”，即“密码服务提供者”。

如果要将 SSL 与 iSeries Access for Windows 组件配合使用，还必须安装 iSeries Client Encryption 产品，5722-CE3（128 位）。iSeries Access for Windows 需要此产品以便建立安全连接。

注: 不需要安装 Client Encryption 产品，就可使用随“个人通信”产品附带的 PC5250 仿真器。“个人通信”有其自己的内置加密代码。

数字证书

参阅使用公用证书与发出专用证书以加深理解公用数字证书和专用数字证书之间的差别以及获取它们的选择。

IBM“数字证书管理器”（DCM）是 iSeries 服务器用以管理数字证书的解决方案。要了解有关 DCM 的更多信息，请参阅“信息中心”主题使用数字证书管理器。

用 SSL 保护应用程序

可以用 SSL 保护以下 iSeries 服务器应用程序:

- 企业身份映射（EIM）
- FTP 服务器
- HTTP Server（基于 Apache）
- iSeries Access for Windows
- 目录服务服务器（LDAP）
- 分布式关系数据库体系结构（DRDA®）和分布式数据管理（DDM）服务器
- “中央管理”服务器
- Telnet 服务器
- Websphere Application Server — Express
- 编写入 API（应用程序编程接口）的 iSeries Access for Windows 集合的应用程序
- 使用 iSeries 服务器上支持的安全套接字“应用程序编程接口”（API）开发的应用程序。受支持的 API 是“全局安全工具箱”（GSKit）和 SSL_iSeries 本机 API。参阅安全套接字 API 以获取有关 GSKit 和 SSL_API 的信息。

SSL 故障诊断

这种很基本的故障诊断信息旨在帮助您减少 iSeries 服务器可能遇到的关于 SSL 的问题列表。重要的是要知道它不是故障诊断信息的全部来源，而仅仅是一个指南。

验证以下叙述是真实的:

- 已经满足 iSeries 服务器上 SSL 的先决条件（请参阅 SSL 先决条件）。
- 如果正在使用装有 V5R1 系统的“iSeries 导航器”的“中央管理”技术，则系统上已经安装了以下 PTF:
  - si01375
  - si01376
  - si01377
  - si01378
  - si01838
- 认证中心和证书是有效的且尚未到期。

如果已对系统验证了上述叙述是真实的，但依然存在与 SSL 相关的问题，请尝试以下选项:

- 在错误表中可交叉引用服务器作业记录中的 SSL 错误代码以查找有关该错误的更多信息。参阅安全套接字 API 错误代码消息页面以访问有关安全套接字错误代码消息的信息。例如，此表将可能在服务器作业记录中显示的 -93 映射为常量 SSL_ERROR_SSL_NOT_AVAILABLE。
  - 负返回码（由代码数字前的短划线表示）表示您正在使用 SSL_ API。
  - 正返回码表示您正在使用 GSKit API。程序员可在其程序中编码 gsk_strerror()or SSL_Strerror() API 以获取错误返回码的简短描述。某些应用程序使用此 API，并打印输出包含此语句的作业记录消息。

  如果需要更详细的信息，该表中提供的消息标识可以显示在 iSeries 服务器上以说明此错误的可能原因及恢复。说明这些错误代码的其它文档可能位于返回错误的个别安全套接字 API 中。
- 以下两个头文件包含与该表相同的“系统 SSL”返回码的常量名称，但是没有消息标识交叉引用:
  - QSYSINC/H.GSKSSL
  - 

    QSYSINC/H.QSOSSL

  请记住，虽然在这两个文件中“系统 SSL”返回码的名称保持常量，但可能有多个错误与每个返回码关联。

有关 iSeries 服务器故障诊断的更多信息，请参阅故障诊断和维护页面。

相关信息

可在以下资源查找附加的 SSL 信息:

IBM 源

- SSL 和 Java 安全套接字扩展（JSSE）页面包括 JSSE 的简短描述及其使用方法。
- IBM Toolbox for Java 页面包括可用 Java 类的简短描述及其使用方法。

请求评论

- RFC 2246: ″The TLS Protocol Version 1.0″  详细说明了 TLS 协议。

- RFC2818: ″HTTP Over TLS″  描述了如何在因特网上使用 TLS 保护 HTTP 连接。

其它源

- The SSL Protocol Version 3.0 文档  非常详细地说明了 SSL Protocol V3.0。

附录. 声明

本信息是为在美国提供的产品和服务编写的。

IBM 可能在其他国家或地区不提供本文档中讨论的产品、服务或功能特性。有关您当前所在区域的产品和服务的信息，请向您当地的 IBM 代表咨询。任何对 IBM 产品、程序或服务的引用并非意在明示或暗示只能使用 IBM 的产品、程序或服务。只要不侵犯 IBM 的知识产权，任何同等功能的产品、程序或服务，都可以代替 IBM 产品、程序或服务。但是，评估和验证任何非 IBM 产品、程序或服务，则由用户自行负责。

IBM 公司可能已拥有或正在申请与本文档内容有关的各项专利。提供本文档并未授予用户使用这些专利的任何许可。您可以用书面方式将许可查询寄往:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594-1785
U.S.A.

有关双字节（DBCS）信息的许可查询，请与您所在国家或地区的 IBM 知识产权部门联系，或用书面方式将查询寄往:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

本条款不适用英国或任何这样的条款与当地法律不一致的国家或地区: INTERNATIONAL BUSINESS MACHINES CORPORATION “按现状” 提供本出版物，不附有任何种类的（无论是明示的还是暗含的）保证，包括但不限于暗含的有关非侵权、适销和适用于某种特定用途的保证。某些国家或地区在某些交易中不允许免除明示或暗含的保证。因此本条款可能不适用于您。

本信息中可能包含技术方面不够准确的地方或印刷错误。此处的信息将定期更改；这些更改将编入本出版物的新版本中。IBM 可以随时对本出版物中描述的产品和／或程序进行改进和／或更改，而不另行通知。

本信息中对非 IBM Web 站点的任何引用都只是为了方便起见才提供的，不以任何方式充当对那些 Web 站点的保证。那些 Web 站点中的资料不是 IBM 产品资料的一部分，使用那些 Web 站点带来的风险将由您自行承担。

IBM 可以按它认为适当的任何方式使用或分发您所提供的任何信息而无须对您承担任何责任。

本程序的被许可方如果要了解有关程序的信息以达到如下目的: （i）允许在独立创建的程序和其他程序（包括本程序）之间进行信息交换，以及（ii）允许对已经交换的信息进行相互使用，请与下列地址联系:

IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

只要遵守适当的条件和条款，包括某些情形下的一定数量的付费，都可获得这方面的信息。

本资料中描述的许可程序及其所有可用的许可资料均由 IBM 依据 IBM 客户协议、IBM 国际软件许可协议或任何同等协议中的条款提供。

此处包含的任何性能数据都是在受控环境中测得的。因此，在其他操作环境中获得的数据可能会有明显的不同。有些测量可能是在开发级的系统上进行的，因此不保证与一般可用系统上进行的测量结果相同。此外，有些测量是通过推算而估计的，实际结果可能会有差异。本文档的用户应当验证其特定环境的适用数据。

涉及非 IBM 产品的信息可从这些产品的供应商、其出版说明或其他可公开获得的资料中获取。IBM 没有对这些产品进行测试，也无法确认其性能的精确性、兼容性或任何其他关于非 IBM 产品的声明。有关非 IBM 产品性能的问题应当向这些产品的供应商提出。

所有关于 IBM 未来方向或意向的声明都可随时更改或收回，而不另行通知，它们仅仅表示了目标和意愿而已。

商标

下列各项是 International Business Machines Corporation 在美国和／或其他国家或地区的商标:

DRDA
IBM
iSeries
Operating System/400
OS/400
Windows
Windows NT

Lotus®、Freelance 和 WordPro 是International Business Machines Corporation 和 Lotus Development Corporation 在美国和／或其他国家或地区的商标。

Microsoft®、Windows、Windows NT® 和 Windows 徽标是 Microsoft Corporation 在美国和／或其他国家或地区的商标。

其他公司、产品和服务名称可能是其他公司的商标或服务标记。

用于下载和打印出版物的条款和条件

如果符合以下条款和条件并且由此您表示接受它们，则授予您使用您选择下载的出版物的准用权。

个人使用: 只要保留所有的专有权声明，您就可以为个人、非商业使用复制这些出版物。未经 IBM 明确同意，您不可以分发、展示或制作这些出版物或其中任何部分的演绎作品。

商业使用: 只要保留所有的专有权声明，您就可以仅在企业内复制、分发和展示这些出版物。未经 IBM 明确同意，您不可以制作这些出版物的演绎作品，或者在您的企业外部复制、分发或展示这些出版物或其中的任何部分。

除非本准用权中有明确授权，不得把其他准用权、许可或权利（无论是明示的还是暗含的）授予这些出版物或其中包含的任何信息、数据、软件或其他知识产权。

当使用该出版物损害了 IBM 的利益，或者根据 IBM 的规定，未正确遵守上述指导说明时，则 IBM 保留自主决定撤销本文授予的准用权的权利。

您不可以下载、出口或再出口本信息，除非完全遵守所有适用的法律和法规，包括所有美国出口法律和法规。IBM 对这些出版物的内容不作任何保证。这些出版物“按现状”提供，不附有任何种类的（无论是明示的还是暗含的）保证，包括但不限于暗含的关于适销性和适用于某特定用途的保证。

从此站点下载或打印出版物，即表明您同意这些条款和条件。

中国印刷